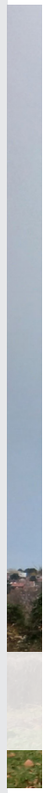


SOVAL

Les intrusions sur les installations d'eau potable étant susceptibles de présenter un risque pour la santé de la population, les exploitants doivent mettre en œuvre les moyens de sécurisation physique permettant de satisfaire aux besoins en eau potable.

ARTICLE INTERACTIF

Eau potable : sécuriser physiquement les ouvrages et la distribution

Arnaud Moign

Abstract

Intrusions into drinking water facilities can pose a risk to public health. Operators must therefore implement physical security measures to ensure they can fulfill their mission and meet drinking water needs. Their tools include a range of technical solutions for detection, deterrence, and access control, all managed through centralized oversight and the implementation of a comprehensive safety and security plan.

Les intrusions sur les installations d'eau potable sont susceptibles de présenter un risque pour la santé de la population. Les exploitants doivent donc mettre en œuvre les moyens de sécurisation physique permettant d'assurer leur mission et de satisfaire aux besoins en eau potable. Leurs armes : un panel de solutions techniques de détection, de dissuasion, de contrôle d'accès, le tout encadré par un pilotage centralisé et la mise en place d'un PGSSE.

L'article L.1321-1 du Code de la santé publique rappelle que « *toute personne qui offre au public de l'eau en vue de l'alimentation humaine, à titre onéreux ou à titre gratuit et sous quelque forme que ce soit, y compris la glace alimentaire, est tenue de s'assurer que cette eau est propre à la consommation* ».

Historiquement, cette obligation de potabilité impliquait une surveillance de la qualité sanitaire de l'eau. Mais depuis 2010[1] la démarche de sécurité sanitaire s'est étendue aux risques intentionnels. L'article R.1321-23 du Code de la santé publique prévoit ainsi une évaluation périodique des vulnérabilités pour les gestionnaires des installations desservant plus de 10 000 personnes (méthode Amdec[2]).

C'est dans ce contexte que le Plan de gestion de la sécurité sanitaire des eaux

1. *Arrêté du 30 décembre 2022 relatif au programme de tests et d'analyses à réaliser dans le cadre de la surveillance exercée par la personne responsable de la production ou de la distribution d'eau < https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046849478 >*

2. *Analyse des modes, des effets et de la criticité des défaillances, ou Failure Modes, Effects and Criticality Analysis (FMECA).*


© Assa Abloy

Dans le monde de l'eau, où de nombreux sites sont isolés, le bloc-porte (ici, un modèle antieffraction d'Assa Abloy) est un levier clé de dissuasion et de résistance, une protection physique immédiatement visible qui retarde l'intrusion et sécurise les points d'accès critiques.

(PGSSE) s'est peu à peu imposé comme stratégie de référence en gestion préventive et anticipation des menaces liées à l'eau potable. Le PGSSE est en effet promu par l'Organisation mondiale de la santé (OMS) depuis 2004. Si sa mise en place relevait jusqu'ici d'une démarche volontaire, la transposition de la nouvelle directive européenne (UE) 2020/2184 le rendra bientôt obligatoire. Deux échéances réglementaires sont ainsi à retenir : juillet 2027, pour les PGSSE liés à la zone de captage, et janvier 2029, pour la production et la distribution de l'eau potable[3]. Les collectivités devront donc être en mesure d'identifier les points sensibles, y compris les vulnérabilités aux malveillances, et de mettre en œuvre des mesures préventives, afin de garantir en permanence la sécurité sanitaire de l'eau pour le consommateur.

DES RISQUES AVÉRÉS

Par ailleurs, au-delà des collectivités, c'est l'ensemble des acteurs de l'eau qui sont mobilisés par la mise en place du PGSSE, dans une dynamique d'amélioration continue : collectivités, exploitants, abonnés et acteurs locaux, ce qui nécessite une collaboration et un accompagnement du changement. L'Astee[4] œuvre dans ce sens, en proposant le guide « *Initier, mettre en place, faire vivre un PGSSE* » et en organisant des temps forts pour accompagner la mise en œuvre de ce dispositif.

Les menaces physiques pesant sur les ouvrages et réseaux d'eau potable sont multiples et peuvent avoir des conséquences immédiates et lourdes pour les exploitants. Selon Aude Rouyer, responsable Management produit chez Alcea (Assa Abloy), on peut classer ces menaces en quatre familles : « *Il y a, d'une part, les menaces liées au contexte territorial, comme l'isolement de certains sites, le vieillissement des infrastructures et la surexposition en zone dense. Il y a, d'autre part, toutes les menaces intentionnelles (intrusion sur sites, vandalisme, sabotage ciblé d'ouvrages, vols de matériel, etc.) et les menaces accidentelles liées à des défaillances d'équipements, des malfaçons, des erreurs humaines ou des collisions. Enfin, il ne faut pas oublier les menaces hybrides, lorsque l'accès physique à un local, une armoire, un capteur ou un automate sert de tremplin pour agir sur le système, neutraliser la détection ou faciliter une attaque numérique.* »

Une intrusion physique peut être une simple intrusion opportuniste sans conséquence ou un acte de malveillance délibéré aux conséquences graves, tels des vols, des dégradations ou une volonté manifeste de nuire à la population (terrorisme).

Les intrusions peuvent se produire par une porte, une trappe, un capot ou même par un point de ventilation des réservoirs, ce dernier constituant une vulnérabilité souvent négligée lors du déploiement de solutions de sûreté physique sur un site. Lorsque les dispositifs de protection sont insuffisamment sécurisés ou inexistants, une personne curieuse ou mal intentionnée peut donc avoir un accès direct à l'eau potable.

Les conséquences d'une intrusion avec accès à l'eau potable sont ainsi particulièrement lourdes pour l'exploitant. Elles entraînent la mise en œuvre immédiate de procédures strictes définies par l'Agence régionale de santé (ARS) : isolement de l'ouvrage concerné, enquêtes internes, analyses spécifiques en laboratoire spécialisé (type biotox) et, le cas échéant, mise en place de solutions de distribution alternatives, comme la fourniture d'eau en bouteille.

Mais, comme le rappelle Sébastien Carré, responsable marché Sécurisation des réseaux sensibles chez EJ France, « *au-delà de l'impact opérationnel, ces situations génèrent également des coûts importants et peuvent affecter durablement la confiance des usagers* ».

METTRE EN ŒUVRE UNE DÉMARCHE DE SÉCURISATION

La détection. L'objectif principal des dispositifs de sûreté est de permettre une détection la plus précoce possible d'une présence non autorisée sur un site


© Pixstart

Grâce aux images satellitaires et au système expert Buildspot de Pixstart, le satellite permet de surveiller rapidement de très grandes zones, avec une mise à jour tous les deux à cinq jours environ.

3. *Article 6 de l'Arrêté du 3 janvier 2023 relatif au PGSSE*
4. *Association scientifique et technique pour l'eau et l'environnement.*

L'EAU POTABLE SOUS HAUTE PROTECTION

La sécurisation physique des ouvrages d'eau potable est une priorité face aux risques de malveillance. Nos systèmes de verrouillage haute sécurité protègent efficacement les accès sensibles, même en environnements contraints.
Des solutions robustes, durables et éprouvées pour protéger les infrastructures critiques.

www.deny-security.com
Plus d'informations :

dény SECURITY

ou un ouvrage, afin de pouvoir réagir rapidement et de limiter les conséquences d'une intrusion. Cette détection peut s'appuyer sur plusieurs niveaux de dispositifs complémentaires. Les premiers d'entre eux sont les moyens de surveillance périmétrique, tels que la vidéosurveillance ou les barrières infrarouges, car ils ont l'avantage d'identifier une intrusion dès l'approche du site. De plus, ces systèmes jouent également un rôle dissuasif non négligeable. Il existe en outre des solutions de surveillance en continu, plus technologiques et spécifiquement dédiées à la protection de la ressource en eau potable. C'est le cas de Buildspot, un outil de surveillance innovant, proposé par Pixstart, qui repose sur l'analyse d'images satellitaires scientifiques[5], après application de corrections géométriques, atmosphériques et radiométriques. Comme l'explique Romane Schnell, ingénieure commerciale chez Pixstart, « *avec sa résolution de 2,5 mètres, Buildspot permet de surveiller les zones sensibles liées aux captages et d'être alerté en cas de changement, qu'il soit d'origine humaine ou naturelle. Si le satellite permet de surveiller de très grandes zones de manière extrêmement rapide et efficace, grâce aux images satellitaires et à notre système expert, les données peuvent être mises à jour à chaque nouveau passage du satellite au-dessus de la zone concernée, soit environ tous les deux à cinq jours, offrant une fréquence de suivi bien supérieure à celle des méthodes de terrain traditionnelles. Grâce à cette approche, notre outil assure un suivi continu des évolutions sur les périmètres de protection, notamment le suivi des constructions, la surveillance environnementale, le contrôle des activités humaines et la détection de travaux non déclarés susceptibles d'impacter les captages d'eau potable* ».

Contrôle d'accès. Concernant les ouvrages eux-mêmes, il est essentiel de mettre en place des dispositifs de détection au niveau des accès. Pour les menaces physiques intentionnelles, il existe des solutions de contrôle d'accès robustes, adaptées à des environnements exigeants, avec une traçabilité complète des entrées/sorties et des droits d'accès évolutifs. Sébastien Carré, d'EJ France, cite plusieurs équipements adaptés aux ouvrages isolés ou non surveillés en permanence : « *Capteurs d'ouverture sur portes, trappes ou capots, mais aussi capteurs de vibration capables de signaler une tentative d'effraction avant même l'ouverture effective.* » Les solutions de gestion des ressources, notamment des clés, sont également des points centraux de la gestion des accès. La solution Netkey d'Alcea permet, par exemple, de structurer la gestion des clés au quotidien, en proposant une traçabilité des emprunts et retours, des droits d'accès maîtrisés et une vision claire des responsabilités de chacun. Pour Aude Rouyer, d'Alcea, « *c'est un levier simple et efficace de renforcer la sûreté opérationnelle, surtout quand le personnel et les prestataires sont toujours en mouvement* ». Par ailleurs, comme l'ajoute Aude Rouyer, cette traçabilité peut encore être améliorée en optant pour un système de clés électroniques : « *Les clés eCliq d'Assa Abloy remplacent les clés mécaniques et permettent une gestion simple et efficace des droits. Il y a la possibilité d'attribuer des droits permanents ou temporaires, de gérer immédiatement une clé perdue ou volée, et d'obtenir une traçabilité complète pour chaque porte, portail, trappe au sol ou armoire électrique.* »

Retarder l'effraction. La détection précoce d'une intrusion doit impérativement être couplée à des solutions de sûreté physique capables de retarder l'effraction. Ces deux dimensions sont indissociables pour assurer une mise en sûreté efficace d'un site ou d'un ouvrage hydraulique. Des acteurs comme EJ et Alcea accompagnent les opérateurs du secteur de l'eau sur l'ensemble de cette chaîne de protection. En tant que fabricant, EJ développe ainsi des trappes de sécurité à double capot et des chapeaux de ventilation, conçus pour offrir une résistance à l'effraction de 30 minutes (certifié par un organisme indépendant). De tels équipements sont déployés aussi bien sur des sites de production, des captages d'eau brute que sur des ouvrages sensibles du réseau de distribution, et bien entendu sur des réservoirs d'eau potable. Pour Aude Rouyer, d'Alcea, qui propose une offre de sûreté complète pour les infrastructures critiques (supervision logicielle, solutions de verrouillage et portes, accompagnement de bout en bout) il ne faut pas non plus négliger l'effet de dissuasion : « *La première barrière, c'est le bloc-porte. Au sein du groupe Assa Abloy, nous fabriquons et installons des blocs-portes antieffraction (CR2 à CR5) pour protéger les ouvrages. Dans le monde de l'eau, où de nombreux sites sont isolés, c'est un levier clé de dissuasion et de résistance, une protection physique immédiatement visible qui retarde l'intrusion*

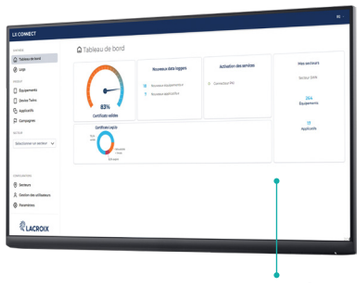
© EJ

Lorsqu'elle est couplée à des équipements à haute résistance mécanique, la solution anti-intrusion complète eDefenso d'EJ, certifiée LPCB et agréée CNPP permet de générer une alerte dès les premiers signes d'effraction, ce qui donne à l'exploitant le temps nécessaire pour réagir et intervenir avant tout accès à l'eau.

5. *Les images sont issues de Sentinel-2, une série de satellites d'observation de la Terre de l'Agence spatiale européenne (ESA)*

SOFREL LogUp

La solution data logger simple, optimale et **cybersécurisée** pour la **surveillance des réseaux d'eau** et des sites isolés



La plateforme de centralisation LX CONNECT
pour la gestion de parc à distance et la cybersécurité automatisée du réseau

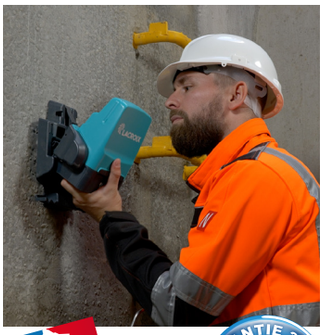
L'application mobile My SOFREL LogUp
pour réduire le temps de mise en œuvre sur le terrain

Le data logger SOFREL LogUp
un modèle hardware unique et évolutif pour tous les usages eaux potable & usées

IEC 62443
Solution contruite suivant les specifications de la norme

De multiples usages

- **Sectorisation**
- **Gestion des réservoirs**
- **Autosurveillance et diagnostic permanent**
- **Surveillance des déversoirs d'orage**
- **Suivi des paramètres de qualité des eaux**



- **Data logger éco-conçu**, robuste et compact
- Logiciel et fonctions métier **évolutifs à distance**
- **Cybersécurité IEC62443** automatisée
- **Gestion centralisée** des équipements et des utilisateurs
- **Modification à distance** des configurations
- Tableaux de bord pour le **suivi du fonctionnement du parc**
- **Étanchéité** renforcée & **pile interne** longue durée

CONÇU ET FABRIQUÉ EN **FRANCE**

GARANTIE 3 ANS 3 Ans

LACROIX

www.lacroix-environment.fr

2 rue du Plessis - 35770 Vern sur Seiche
Tel. 02 99 04 89 00
Email : info.fr.environment@lacroix.group

© Alcea – Assa Abloy

La gestion globale et centralisée des risques physiques peut être confiée à un système de supervision comme Alwin, développé par Alcea. Cette plateforme simplifie le pilotage de la sûreté des sites au quotidien, en particulier pour la gestion multisite.

et sécurise les points d'accès critiques. » En outre, il ne faut pas limiter la sécurisation physique aux accès principaux, mais aussi intégrer les accès considérés comme secondaires dans la stratégie, notamment les points de ventilation des réservoirs, qui constituent pourtant des vulnérabilités potentielles.

Miser sur une approche globale. L'efficacité de ces dispositifs repose néanmoins sur leur intégration dans une approche globale, incluant la transmission des alertes, leur prise en compte par les équipes d'exploitation et la cohérence avec les procédures d'intervention existantes. La dissuasion et la détection ne doivent donc pas être envisagées isolément, mais considérées comme des éléments complémentaires d'une stratégie de sûreté physique adaptée aux enjeux des réseaux d'eau potable. EJ propose ainsi eDefenso, une solution complète certifiée niveau SR4 par le LPCB[6] et intégrant à la fois la trappe sécurisée, le système de détection associé et la surveillance électronique avec EJ Connect. « *Lorsqu'elle est couplée à des équipements à haute résistance mécanique, une telle approche permet de générer une alerte dès les premiers signes d'effraction. Cette alerte précoce donne à l'exploitant le temps nécessaire pour réagir et intervenir avant tout accès à l'eau, ce qui limite les risques sanitaires et opérationnels* », explique Sébastien Carré, d'EJ France. Cette gestion globale et centralisée des risques physiques peut aussi être confiée à un système de supervision comme Alwin, développé par Alcea. Cette plateforme interopérable et évolutive simplifie le pilotage de la sûreté des sites au quotidien, grâce à une interface intuitive, une centralisation des événements et la possibilité de définir des scénarios d'alerte. Un tel outil est donc particulièrement pertinent pour la gestion multisite.

LA SÉCURISATION DES SITES : LES ÉVOLUTIONS À VENIR

En France, la sécurité des infrastructures critiques est encadrée par le dispositif SAIV (Secteurs d'activité d'importance vitale), qui identifie les ouvrages essentiels et impose aux exploitants de mettre en place des mesures de protection physique et organisationnelle. Or, comme le secteur de l'eau potable est considéré comme vital, celui-ci est concerné par le SAIV, afin de garantir la continuité de la distribution et la protection de la ressource. La directive européenne REC (Résilience des entités critiques), qui en cours de transposition en droit français, va prochainement élargir ce cadre et harmoniser les exigences au niveau européen, en remplaçant l'actuelle directive de 2008 portant sur le recensement et la désignation des infrastructures critiques. L'évaluation des risques, la résilience des installations et la coordination entre autorités et opérateurs devraient donc être renforcées afin de mieux anticiper les menaces, améliorer la prévention et réduire l'impact des incidents sur les populations.

C'est également dans ce cadre que s'inscrit la directive NIS 2, avec laquelle le pont entre cybersécurité et sécurité physique deviendra incontournable pour les acteurs de l'eau, puisque protéger la continuité de service consiste à sécuriser à la fois les systèmes IT/OT et l'accès aux sites et équipements critiques. La directive NIS 2 exige ainsi des mesures de gestion des risques et de continuité qui, sur le terrain, passent par une maîtrise stricte des accès physiques, la traçabilité et la mise en place d'une supervision capable de corréler tout événement physique sur le terrain avec un événement « système » (connexion à distance, action sur l'automate, changement de paramètres).

Selon Aude Rouyer, d'Alcea, « *en tant que membre historique de la SPAC Alliance, Alcea contribue aux travaux d'écriture des textes de normalisation relatifs à la NIS 2. La directive permet une approche unifiée de la sûreté (cybersécurité) en harmonisant les règles, les responsabilités et les pratiques à l'échelle européenne. Tout cela sera mis au service d'une même exigence de résilience et de reporting, afin de déclencher la bonne réaction au bon moment et de documenter l'incident* ». La protection des infrastructures hydrauliques ne peut plus se limiter à des barrières physiques. Pour garantir la continuité

© Seneca

Pour garantir la continuité du service et la sécurité sanitaire, il est essentiel d'intégrer des données de terrain fiables, l'automatisation en périphérie et la cybersécurité.

6. *Low Prevention Certificate Board.*

du service et la sécurité sanitaire, il est essentiel d'intégrer des données de terrain fiables, l'automatisation en périphérie et la cybersécurité. Les technologies de Seneca apportent un cadre modulaire pour acquérir des signaux à partir de capteurs, les isoler électriquement, les traiter localement et les distribuer dans des formats interopérables vers des SCADA[7] ou des plateformes IIoT/SaaS/cloud.

De plus, l'approche proposée par les dispositifs Edge du fabricant italien permet de prendre des décisions en temps réel, réduisant ainsi les risques de panne d'information typiques des sites non surveillés et permettant la corrélation entre les événements physiques et numériques sans dépendre exclusivement des clouds centralisés. La sécurité des réseaux OT est également une condition préalable à la technologie de Seneca, grâce à l'adoption de stratégies de cybersécurité pour les dispositifs industriels, intégrées dès la conception, avec authentification, segmentation et protection des micrologiciels, minimisant ainsi les surfaces d'attaque.

Répondre aux exigences de ces directives nécessitera en outre la mise en place d'audits réguliers et une amélioration en continu des infrastructures, c'est pourquoi les fabricants innovent et font évoluer leurs solutions de sûreté.

Pour Sébastien Carré, d'EJ France, le rôle des fabricants – Alcea, Astee, Bayard, Deny Security (fournisseur de serrures et de solutions complètes de gestion des clés), EJ, iLoq, Iseo, Pixstart, Socotec, etc. et autres acteurs (Saur, Syndicat des eaux d'Île-de-France [Sedif])… – est clair : « *Nous voulons accompagner au mieux les exploitants publics comme privés dans la protection de leurs ouvrages et la conformité à ces nouvelles réglementations.* » ●

7 *Supervisory Control and Data Acquisition, ou Système de contrôle et d'acquisition de données en temps réel.*