Digital Risk: Remote-Monitoring, IoT Sensors and Data Integrity Picture This – French





Cette image montre la salle de contrôle d’une petite station municipale de traitement de l’eau pendant un quart de travail matinal habituel. Un seul opérateur est assis à un poste de travail équipé de deux écrans affichant le tableau de bord SCADA de l’installation : les niveaux de produits chimiques, les débits et l’état du système indiquent tous une situation normale, en vert. L’opérateur remplit des documents administratifs tout en jetant de temps à autre un coup d’œil à l’écran. Sans crier gare, le curseur de l’écran de droite commence à bouger tout seul. Un menu déroulant s’ouvre. La valeur de dosage d’un produit chimique commence à changer : la concentration d’hydroxyde de sodium grimpe rapidement, passant de 100 parties par million à une valeur que l’opérateur n’a jamais vue auparavant. Il se penche en avant, les yeux rivés sur l’écran.

Ce qui se passe sur cette image n’est ni un dysfonctionnement de l’équipement ni une erreur de capteur : il s’agit d’une personne, quelque part ailleurs dans le monde, qui, en ce moment même, ajuste les concentrations chimiques d’un réseau d’approvisionnement en eau desservant 15 000 personnes à partir d’un clavier que l’opérateur ne peut ni voir ni bloquer. Le système de surveillance à distance, installé pour faciliter la gestion de cette installation, est devenu le point d’accès par lequel une modification chimique mortelle est effectuée en temps réel. Aucune alarme ne s’est déclenchée. Aucune demande d’authentification n’est apparue. Le système a accepté la connexion, car il n’avait aucun moyen de faire la différence entre un employé autorisé et un pirate. Les systèmes numériques qui contrôlent la sécurité physique doivent être traités avec la même rigueur que tout autre contrôle critique pour la sécurité – car lorsqu’ils échouent, les conséquences ne se limitent pas à des pertes de données. Il s’agit de brûlures chimiques, de blessures et de décès.