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





Esta imagen muestra la sala de control de una pequeña planta municipal de tratamiento de agua durante un turno matutino de rutina. Un único operador de la planta está sentado en una estación de trabajo con dos monitores que muestran el tablero SCADA de la planta: los niveles de químicos, las tasas de flujo y el estado del sistema se muestran todos en verde, lo que indica que están normales. El operador está llenando documentos y echa un vistazo de vez en cuando a la pantalla. Sin previo aviso, el cursor del monitor de la derecha comienza a moverse por sí solo. Se abre un menú desplegable. El valor de dosificación de un químico comienza a cambiar: el hidróxido de sodio sube rápidamente de 100 partes por millón hacia un número que el operador nunca ha visto ingresar antes. Se inclina hacia adelante, fijando la mirada en la pantalla.

Lo que está sucediendo en esta imagen no es una falla del equipo ni un error del sensor: es una persona en algún otro lugar del mundo, en este preciso momento, ajustando los niveles de sustancias químicas del suministro de agua para 15 000 personas desde un teclado que el operador no puede ver ni detener. El sistema de monitoreo remoto que se instaló para facilitar la gestión de esta instalación se ha convertido en el punto de acceso a través del cual se está realizando un cambio químico letal en tiempo real. No ha sonado ninguna alarma. No ha aparecido ninguna solicitud de autenticación. El sistema aceptó la conexión porque no tenía forma de distinguir entre un empleado autorizado y un atacante. Los sistemas digitales que controlan resultados de seguridad física deben tratarse con el mismo rigor que cualquier otro control crítico para la seguridad, porque cuando fallan, las consecuencias no son pérdidas de datos. Son quemaduras químicas, lesiones y muertes.