Requisitos de ciberseguridad “asequibles” en la digitalización industrial

José Valiente
Director del Centro de Ciberseguridad Industrial

Son muchas las cuestiones que un área de ingeniería se plantea o planteará al intentar contemplar requisitos de ciberseguridad en sus nuevos proyectos de automatización y control industrial. Algunas de esas preguntas son: ¿Qué implicaciones tendrán los requisitos de ciberseguridad en el rendimiento o en el tiempo de despliegue, y en el coste? ¿Las tecnologías industriales disponen de las funcionalidades de ciberseguridad necesarias? ¿Están preparados los proveedores con los que trabajamos para implementar estos requisitos? ¿Quién los validará? ¿Qué estándares o regulaciones existen que deberían contemplarse? ¿Existen en la organización profesionales que nos puedan ayudar a identificar los requisitos más adecuados?

Si le diéramos al área de ingeniería una lámpara mágica para solicitar tres deseos al contemplar los requisitos de ciberseguridad en un proyecto de automatización industrial, seguramente serían los siguientes:

- Conocer qué requisitos de ciberseguridad se están solicitando en los proyectos de mi sector o proyectos similares.
- Un catálogo de requisitos de ciberseguridad basado en estándares que, además, identifique la regulación que debe cumplirse, que identifique las soluciones que soportan los requisitos, y a los proveedores con capacidad real para implementar dichos requisitos.
- Una plataforma técnica que me permita modelar mi proyecto de automatización industrial, y donde pueda seleccionar los requisitos de un catálogo e incluir los míos propios, y solicitar a los proveedores su grado de cumplimiento y capacidad para implementarlos.

Los ingenieros industriales llevan más de medio siglo automatizando procesos industriales, pero la verdadera carrera de la automatización industrial comenzó en los años ochenta, impulsada por el sector del automóvil. La automatización reduce el consumo de energía, optimiza el uso de los materiales, mejora la calidad, pero requiere de un alto coste en investigación, desarrollo e instalación de equipamiento.

» La digitalización debe ir acompañada de requisitos de ciberseguridad que otorguen disponibilidad, integridad y confidenciallidad desde su diseño

El principal cambio en la automatización industrial que se ha producido en los últimos quince años ha sido la proliferación de las tecnologías, y hoy en día la digitalización industrial depende casi totalmente del software, los sistemas y las comunicaciones para automatizar, optimizar e integrar los diferentes componentes de los sistemas de operación mediante sistemas con capacidades asociadas a trabajadores humanos, como la multifunción, la toma de decisiones, el autodiagnóstico, el mantenimiento predictivo y el trabajo de forma autónoma[1].

La digitalización industrial aprovecha todas las nuevas capacidades de las tecnologías de información, en cuanto a conectividad, análisis de datos y computación. Pero esta evolución tecnológica debe ir acompañada de requisitos de ciberseguridad que proporcionen la disponibilidad, integridad y confidencialidad necesarias desde su diseño, y así

1: Industrial Internet of Things: Unleashing the Potential of Connected Products and Services http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf

» La ciberseguridad desde el diseño es, en la actualidad, la base para construir plantas industriales eficientes

poder estar mejor preparados ante las amenazas cibernéticas que han ido aumentando[2] y evolucionando, en cuanto a su complejidad, a un ritmo muy rápido, como demuestra la existencia de las llamadas amenazas persistentes avanzadas, más conocidas por sus siglas en inglés, APT. Por ello, la calidad y salud digital es clave para que el proceso industrial sea eficiente.

Algunas organizaciones industriales de sectores como el energético, químico, agua, transporte o el de alimentación han empezado a incluir requisitos de ciberseguridad en sus nuevos proyectos de automatización o de renovación de tecnologías de operación, pero son muchas las dificultades que se encuentran para identificar qué requisitos de ciberseguridad deben incluir o qué capacidades deben solicitar a sus proveedores; pero, sobre todo, cuáles serán las exigencias de regulaciones o normativas en materia de ciberseguridad cuando la planta empiece a ser operada.

Para facilitar la incorporación de requisitos de ciberseguridad en proyectos industriales, el Centro de Ciberseguridad Industrial[3] está construyendo una plataforma técnica que permita establecer el tipo de planta, por ejemplo, de ciclo combinado o eólica, y modelar el proyecto de automatización, incluyendo las tecnologías de operación, proveedores, así como las redes y sistemas involucrados ordenados dentro de los cinco niveles del modelo de Purdue de ISA-95, como, por ejemplo, instrumentación de una turbina en el nivel 0, controladores en el nivel 1, SCADAs en el nivel 2, MES o LIMS en el nivel 3.

Esta plataforma permitirá seleccionar para cada componente o grupo de componentes requisitos de ciberseguridad de un catálogo que contemple normativas y regulaciones existentes, así como establecer las capacidades de ciberseguridad requeridas a los proveedores que participarán en el proyecto, permitiendo descargar los requisitos necesarios o directamente referenciar de forma segura un enlace de la plataforma.

Abordar la ciberseguridad desde el diseño es, en la actualidad, la base para construir plantas industriales eficientes, con mejores niveles de disponibilidad o rendimiento de la operación.

2: SANS. State of OT/ICS Cybersecurity Survey 2019 https://radiflow.com/wp-content/uploads/2019/06/Survey_ICS-2019_Radiflow.pdf

3: Centro de Ciberseguridad Industrial https://www.cci-es.org/