Garantizar la seguridad de las tecnologías digitales de la próxima generación de reactores nucleares

Joanne Liou

Aunque todas las innovaciones traen consigo potenciales beneficios que podrían transformar las industrias, también conllevan potenciales riesgos. En el ámbito nuclear, los reactores nucleares avanzados, incluidos los reactores modulares pequeños (SMR), están incorporando tecnologías innovadoras, sobre todo digitales, que aportan soluciones novedosas.

Existe un creciente interés por los SMR. Estos reactores nucleares avanzados tienen una capacidad de potencia limitada, generalmente de hasta 300 MW(e) por unidad, lo que representa cerca de un tercio de la capacidad de generación de los reactores nucleares de potencia tradicionales. No obstante, el uso de tecnología digital de vanguardia en estos nuevos reactores plantea nuevos desafíos en materia de seguridad nuclear tecnológica y física. En todo el mundo hay más de 80 diseños y conceptos de SMR que se encuentran en diferentes fases de desarrollo.

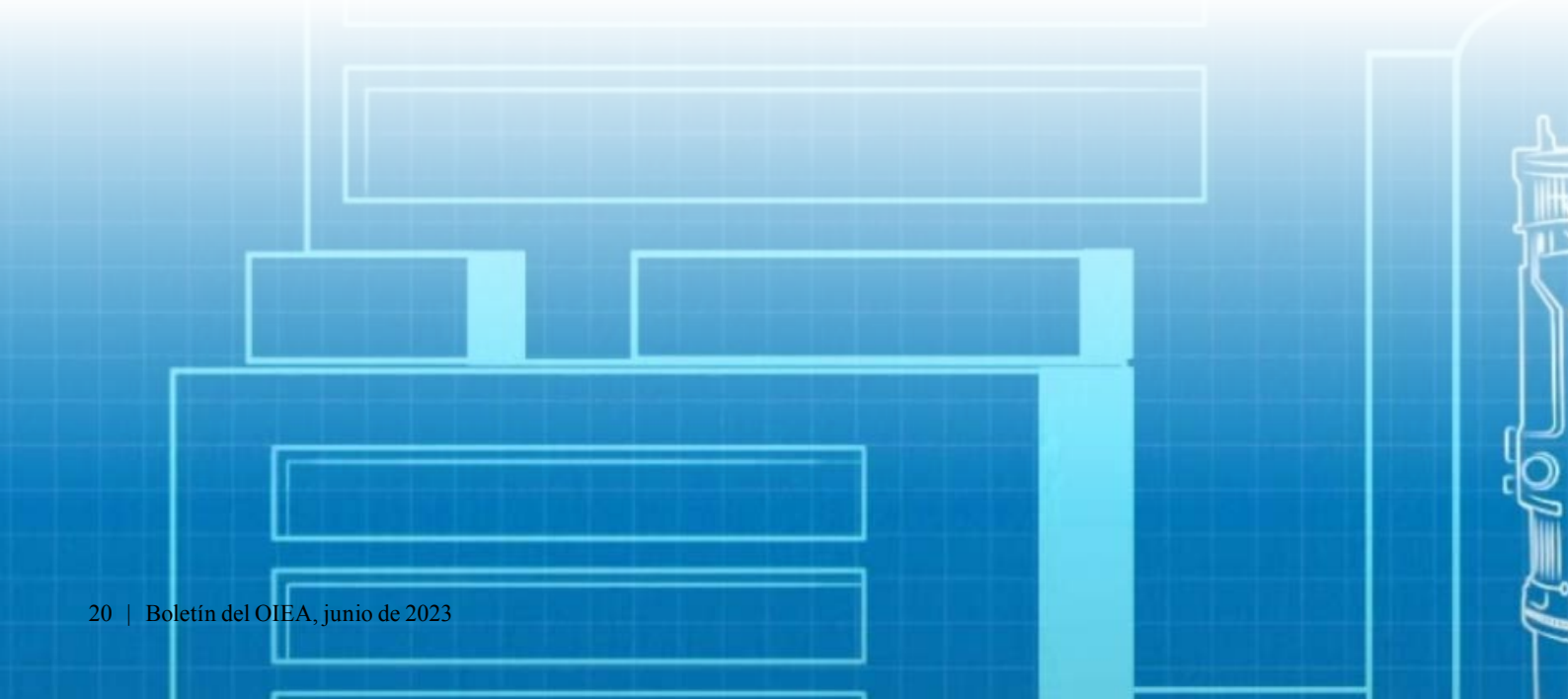
"Uno de los desafíos para el despliegue de SMR es de qué manera acelerar el desarrollo de la tecnología que utilizan y demostrar su nivel de preparación y, al mismo tiempo, mantener el cumplimiento de las normas de la seguridad nuclear tecnológica y física —declara Rodney Busquim e Silva, Oficial de Seguridad de la Tecnología de la Información del OIEA—. Esto reafirma la necesidad de considerar y mantener soluciones de instrumentación y control digitales y de seguridad informática durante el ciclo de vida de los SMR".

Soluciones y desafíos informáticos

Los innovadores diseños de los SMR se basan en sistemas de instrumentación y control digitales que hacen posibles sus características innovadoras. El hecho de que cada vez se necesiten más tecnologías digitales para la automatización, el control de supervisión y el mantenimiento a distancia, junto con otras características novedosas, pone de relieve la necesidad de soluciones informáticas.

Algunos SMR están diseñados para el despliegue de la energía nucleoeléctrica en zonas aisladas y con un número reducido de personal sobre el terreno, lo que puede hacer necesaria la monitorización a distancia constante y fiable. Dado el diseño de los sistemas de instrumentación y control digitales, la aplicación de medidas de seguridad informática debería ser un requisito previo para una comunicación segura entre el emplazamiento del SMR y un centro de apoyo. "De la necesidad de intercambiar información pueden surgir vías susceptibles de ser explotadas por ciberdelincuentes, por lo que se deben aplicar consideraciones de ciberseguridad robustas a la infraestructura de comunicación —señala Mike St. John-Green, experto en seguridad informática que reside en el Reino Unido—. Es preciso proteger la confidencialidad, la disponibilidad y la integridad de la información en las operaciones a distancia para garantizar el funcionamiento seguro y fiable de los SMR y la infraestructura conexa".

La inteligencia artificial (IA) y el aprendizaje automático también apoyan las operaciones de los SMR. La IA comprende las tecnologías que producen sistemas capaces de rastrear problemas complejos, mientras que las tecnologías de aprendizaje automático "aprenden" cómo realizar una tarea concreta sobre la base de los datos disponibles. Al combinar simulaciones digitales de instalaciones nucleares y sistemas de vigilancia y control con sistemas de IA, la industria nuclear busca optimizar funciones complejas, lo que podría aumentar la eficiencia operacional. Sin embargo, estas ventajas llevan aparejada la posibilidad de ciberataques. Por ejemplo, los algoritmos de software de los que se sirven la IA y el aprendizaje automático dependen de bases de datos que



podrían ser objeto de manipulación para provocar errores en el proceso de toma de decisiones de la IA.

"Estos sistemas pueden ser objeto de inyección de código, por ejemplo, que consiste en alimentarlos intencionadamente con datos corruptos durante el proceso de desarrollo, distribución o instalación del software. El desafío general radica en cómo infundir suficiente transparencia a los algoritmos de IA y aprendizaje automático. El uso aceptable de la IA y el aprendizaje automático debe estar claramente definido con unos niveles de riesgo aceptables", afirma Si Wen, estudiante de doctorado de la Universidad de Tsinghua de China.

Seguridad física desde el diseño

Los expertos coinciden en que la seguridad informática de las instalaciones nucleares debe tenerse en cuenta desde buen principio. Esta lógica proactiva, denominada "seguridad física desde el diseño", se inspira en las prácticas óptimas y las lecciones extraídas de la experiencia del pasado y recoge el concepto de "incorporación en el diseño" que también se aplica en los ámbitos de la seguridad tecnológica nuclear, las salvaguardias y la clausura de instalaciones.

La seguridad informática desde el diseño tiene como objetivo reducir los riesgos para la seguridad física en su origen mediante un enfoque que contemple la seguridad física sistemática y constante a lo largo de todas las fases de la vida útil de la instalación o el proceso. "Las medidas de seguridad informática deben tomarse en cuenta y mantenerse durante todo el ciclo de vida de los SMR, desde el diseño hasta la clausura, pasando por la operación —afirma el Sr. Busquim e Silva—. Si piensan en la seguridad física, incluida la ciberseguridad, desde buen principio, los creadores de instalaciones pueden tomar decisiones relativas al diseño que las hagan más seguras desde el punto de vista tecnológico y físico, eficientes y eficaces en función del costo".

La función del OIEA

El OIEA conecta expertos, de organizaciones nucleares y de otra índole, con el objetivo de examinar y detectar los problemas y los desafíos relacionados con la seguridad informática que plantean las características tecnológicas y operacionales de los SMR. Por ejemplo, en febrero de 2022, el OIEA celebró una reunión técnica sobre sistemas de instrumentación y control y seguridad informática para SMR con el fin de promover la cooperación y facilitar el intercambio de información entre expertos internacionales. Los participantes coincidieron en la necesidad de armonizar los enfoques y los reglamentos nacionales para lograr la viabilidad del mercado internacional de los SMR. "En lo que respecta a los SMR normalizados, las soluciones de instrumentación y control abren un ámbito técnico completamente nuevo. La creciente automatización necesaria para los nuevos modos de operación y el amplio uso de sistemas digitales exigen medidas de seguridad informática y soluciones de ingeniería desde el nivel del diseño para garantizar un funcionamiento tecnológica y físicamente seguro de la central", señala Jorge Casanova de la Autoridad Regulatoria Nuclear de la Argentina, quien asistió a la reunión.

Además, en marzo de 2023, el OIEA organizó un taller para seguir estudiando la creación de capacidades técnicas relacionadas con la seguridad informática y la instrumentación y el control para SMR. Asimismo, el OIEA tiene previsto iniciar un proyecto coordinado de investigación sobre el tema en 2024.

En todo el mundo hay más de 80 diseños y conceptos de SMR que se encuentran en diferentes fases de desarrollo.