PRINCIPALES ESTÁNDARES INTERNACIONALES DE CIBERSEGURIDAD: PUNTOS EN COMÚN Y DIFERENCIAS

ANDREU VALLÉS CARBONERAS

Responsable de Ciberseguridad de la división de Salas de Control y Simulación.

TECNATOM

Ingeniero de Instrumentación y Control.

La digitalización de los sistemas de Instrumentación y Control (I&C) y monitorización de las plantas ha traído múltiples beneficios, derivados principalmente de la flexibilidad, escalabilidad y potencia que proporciona la tecnología digital. Sin embargo, el uso de esta tecnología ha expuesto a estos sistemas a las amenazas cibernéticas. No se trata de un problema menor habida cuenta de que la digitalización ha llegado ya a los equipos más sensibles de las centrales, es decir, aquellos encargados de ejecutar funciones de seguridad, actuación ante emergencias y seguridad física. El malfuncionamiento de uno de estos sistemas a consecuencia de un ciberataque podría tener, por tanto, consecuencias importantes tanto a nivel económico como para las personas y el medioambiente. Todo este contexto ha hecho que la ciberseguridad se haya convertido en una de las principales inquietudes de la industria a nivel mundial. Conscientes de ello, distintas entidades, tanto nacionales como supranacionales, han trabajado y trabajan en desarrollar una documentación que los distintos actores del sector, principalmente las plantas y los organismos reguladores, puedan usar como referencia para proteger los equipos digitales frente a amenazas cibernéticas.

INTRODUCCIÓN

Algunas de las entidades más importantes dedicadas a la elaboración de guías y estándares son el Organismo Internacional de Energía Atómica (OIEA), la *International Electrotechnical Comission* (IEC), y el *Nuclear Energy Institute* (NEI). Estos organismos llevan tiempo dedicando recursos para elaborar documentos que tratan la protección cibernética de los equipos digitales de las centrales nucleares. A continuación, se exponen estas líneas de trabajo y se realiza un análisis comparativo de sus propuestas.

LÍNEAS DE TRABAJO

Organismo Internacional de Energía Atómica (OIEA)

El OIEA elabora, para los distintos ámbitos de la energía nuclear, documentación con un marcado carácter general aunque clasificados en cuatro categorías en función del grado de detalle. Los más detallados son las guías técnicas, seguidas de las guías de implementación, las recomendaciones y, por último, los fundamentos, que tienen un marcado carácter estratégico.

La documentación relativa a la seguridad cibernética de la Organismo Internacional de Energía Atómica (OIEA) se contextualiza en la llamada *serie de seguridad nuclear*, conocida por sus siglas en inglés *NSS*, de *Nuclear Security Series*. Actualmente hay un documento publicado y varios borradores en curso. El publicado es el NSS 17 *Computer Security at Nuclear Facilites* (2011), y es el documento principal de la línea de trabajo del OIEA. Esta guía técnica establece las bases para el desarrollo de un programa de ciberseguridad para proteger los sistemas digitales de una planta nuclear. Como complemento a este documento, está previsto que el OIEA publique en 2017 una nueva guía técnica que se centra exclusivamente en la protección de los sistemas de instrumentación y control. La referencia y título de este documento es NST036 *Computer Security of Instrumentation and Control Systemas at Nuclear Facilites*.

Además de las guías anteriores, el OIEA trabaja en otros documentos en materia de ciberseguridad. Estos textos, en fase más temprana de elaboración, son los siguientes:

INTERNATIONAL STANDARDS ON CYBERSECURITY: COMMON POINTS AND DIFFERENCES

Digitalization of Instrumentation and Control (I&C) and monitoring systems has brought many benefits, mainly derived from flexibility, scalability and power provided by digital technology. However, the use of this technology has exposed these systems to cyber threats. This is not a minor issue, given that the digitalization has already reached the most sensitive plant equipment, that is, those responsible for performing security, emergency action and physical security functions. The malfunctioning of one of these systems as a result of a cyberattack could therefore have important consequences not only economically but also for people and environment. This context has made cybersecurity one of the industry's main concerns worldwide. Being aware of this, different national and supranational entities have been working on the development of documentation that different stakeholders, particularly plants and regulatory bodies, can use as a reference to protect digital equipment against cyber threats.

- NST045 *Computer Security for Nuclear Security*. Se trata de una guía de implementación enfocada a facilitar que los estados miembro de el OIEA desarrollen una estrategia nacional de ciberseguridad.
- NST047 *Computer Security Techniques for Nuclear Facilities*, una guía técnica que trata las buenas prácticas en la aplicación de medidas de ciberseguridad en plantas nucleares.

El OIEA ha publicado otros dos documentos fuera del contexto de *NSS* por no contar con el consenso internacional necesario. Uno enfocado a la auditoría y evaluación/revisión de programas de ciberseguridad, que tiene por título *Conducting Computer Security Assessments at Nuclear Facilites* y el otro, *Computer Security Incident Response Planning at Nuclear Facilites*, trata de la gestión de incidentes.

International Electrotechnical Commission (IEC)

Dentro de la *International Electrotechnical Commission*, el subcomité SC45A se ocupa del desarrollo de estándares relacionados con sistemas de instrumentación y control de plantas nucleares. Este grupo ha desarrollado documentos ampliamente reconocidos y aplicados en la industria, como IEC 61513 *Nuclear power plants – Instrumentation and control for systems important to Safety – General Requirements for Systems*. El SC45A colabora estrechamente con el Organismo Internacional de Energía Atómica (OIEA). Concretamente IEC desarrolla en sus estándares los detalles y las implicaciones más concretas de las líneas estratégicas que marcan los documentos del OIEA .

Desde 2008, el SC45A viene trabajando en la elaboración de estándares para el tratamiento de la protección de los equipos de I&C desde el punto de vista cibernético. En agosto de 2014 publicó el estándar IEC 62645, Ed. 1, *Nuclear Power Plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems*, que constituye el documento principal dentro de la serie de documentos de ciberseguridad. Este texto establece los requisitos y provee una guía para desarrollar un programa de ciberseguridad.

Tras la publicación de la primera edición del documento, y dado el intenso debate que tuvo lugar durante su desarrollo, se comenzó a trabajar para hacer una segunda edición, cuya fecha objetivo de publicación es 2018.

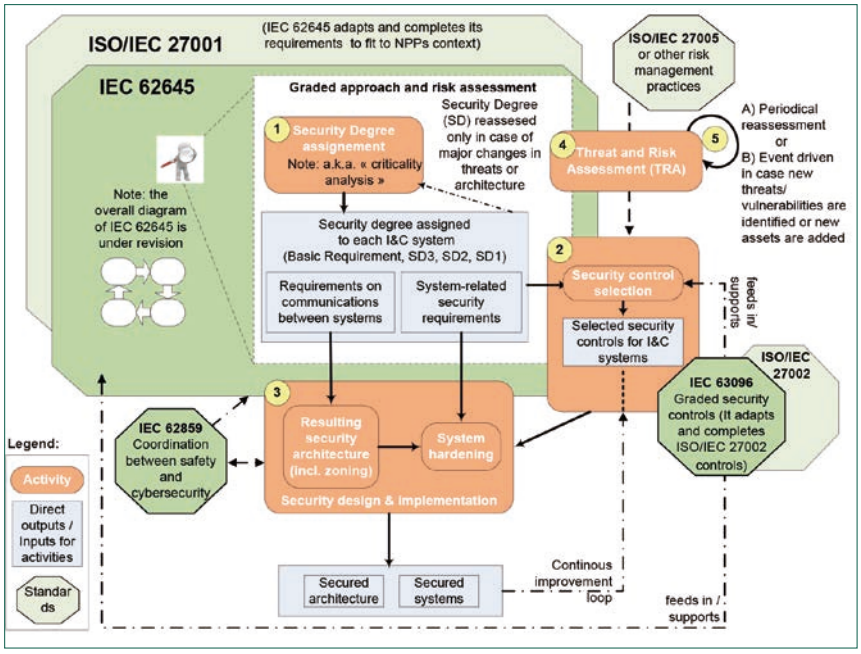

Figura 1. Estándares de ciberseguridad del IEC[2].

Como complemento al IEC 62645, el organismo internacional ha elaborado el estándar IEC 62859 *Coordination between safety and cybersecurity*, que trata cómo gestionar la confluencia de la seguridad (*safety*) y la ciberseguridad, dos conceptos que comparten el objetivo de minimizar riesgos, pero que pueden impactar, tanto positiva como negativamente, uno en el otro.

Por último, dentro del SC45A se está trabajando en el nuevo estándar internacional complementario a IEC 62645, el 63096 *Nuclear Power Plants – Instrumentation, control and electrical systems – Security Controls*. Este texto detalla las medidas de ciberseguridad recomendadas para cada uno de los niveles o grados[1] de seguridad que define IEC 62645. La fecha de publicación prevista de documento es 2019.

La Figura 1, contenida en IEC 63096, esquematiza la relación de estándares de ciberseguridad de IEC.

Nuclear Energy Institute (NEI)

El *Nuclear Energy Institute* es un organismo de Estados Unidos que elabora documentos para facilitar a las centrales el cumplimiento de leyes y directivas del regulador. El norteamericano es uno de los países que más tiempo lleva trabajando en la protección de sistemas digitales frente a amenazas cibernéticas en el mundo nuclear, y NEI ha jugado un papel muy importante en este sentido. El primer documento que elaboró fue NEI 04-04 *Cyber Security Program for Power Reactors*, una guía para la aplicación de un programa de ciberseguridad que, en 2005, refrendó el regulador, *Nuclear Regulatory Comission* (NRC), como un "enfoque aceptable de programa de ciberseguridad". Su aplicación, sin embargo, fue voluntaria y no un requisito regulatorio. Éste llegó en 2009 a través de una extensión de la normativa de seguridad física, cuando se publicó la llamada Regla de Ciberseguridad, 10 CFR 73.54. El enfoque de la protección del programa de ciberseguridad propuesto en NEI 04-04 no se estimó adecuado para satisfacer la Regla, de modo que NEI elaboró otro documento, NEI 08-09 *Cyber Security Plan for Nuclear Reactors*, que sí cubre ese marco legislativo.

Adicionalmente a NEI 08-09, el *Nuclear Energy Institute* ha elaborado otros documentos complementarios con distintos objetivos. Por un lado, NEI 10-04 *Identifying Systems and Assets Subject to the Cyber Security Rule*, cuyo objetivo es clarificar qué equipos están dentro del alcance de la Regla de Ciberseguridad y simplificar el proceso de identificación de los mismos. Tal y como se define en el propio NEI 08-09, estos dispositivos se conocen como activos digitales críticos, o, en inglés, *Critical Digital Assets* (CDA). Por otro lado, NEI 13-10 *Cyber Security Control Assessments*, que propone una metodología para clasificar los CDA en base a un análisis de consecuencias. Su objetivo es simplificar la protección

[1]Los niveles o grados de seguridad son las capas de protección de un modelo de defensa en profundidad.

[2]Imágenes pertenecientes a IEC 63096.

de los equipos menos críticos y centrar esfuerzos en aquellos cuya indisponibilidad tenga un impacto mayor.

SIMILITUDES

Cada una de las líneas de trabajo anteriores enfoca la protección de equipos digitales de un modo particular, aunque confluyen en algunos puntos comunes:

– **Desarrollo de un programa de ciberseguridad**
La protección de los sistemas digitales, ya no sólo de los de instrumentación y control, sino de otros equipos de la red informática, se acomete a través de un programa de ciberseguridad que debe implementarse en la planta y mantenerse en el tiempo. Las bases del programa se establecen en un plan de ciberseguridad, que es el documento formal que recoge todas las tareas relativas al programa, desde la organización de las personas implicadas hasta la aplicación de las medidas de protección más técnicas (instalación de programas y dispositivos, configuración de equipos, etc.). Todas las líneas de trabajo cubren la implantación y mantenimiento de un programa de ciberseguridad, y detallan, en mayor o menor medida, dependiendo de cada caso, el contenido que debe tener el plan de ciberseguridad.

– **Protección basada en una estructura de defensa en profundidad**
El plan de ciberseguridad que proponen todos, los estándares y guías existentes, se basa en una arquitectura de defensa en profundidad. Este concepto consiste en disgregar la protección en distintos niveles, grados o capas de seguridad, para cada uno de los cuales se aplican una serie de controles o medidas de protección. Además, se controlan los flujos de información permitidos entre niveles. La Figura 2 ilustra esta idea:
Dependiendo de su criticidad[3], cada activo digital 'se asigna' a un nivel de protección de la estructura; los equipos esenciales se asignarán a niveles de protección más exigentes; los menos críticos quedarán asignados a niveles con protección menos severos.

– **Ciberseguridad como parte de la seguridad integral**
Otros de los puntos comunes de todos los enfoques es que la ciberseguridad debe entenderse como un área más de la seguridad integral de la planta. Las medidas de seguridad cibernética se apoyan en las de seguridad física y de las personas, y viceversa. Es un error entender las distintas seguridades como entes independientes y aisladas.

– **Ciberseguridad y *safety***
La particularidad intrínseca de una central nuclear es el tratamiento de la seguridad (*safety*), de modo que todos los trabajos que se desarrollan en una planta nuclear la tienen en consideración. En el caso de la ciberseguridad, la relación con la seguridad viene marcada por el potencial impacto que las medidas de protección cibernética pueden tener sobre el funcionamiento de los equipos de I&C digital, y, por extensión, en la integridad y disponibilidad de las funciones de seguridad operacional que realizan esos dispositivos. Este aspecto, clave y particular de la industria nuclear, es tratado en todos los enfoques.

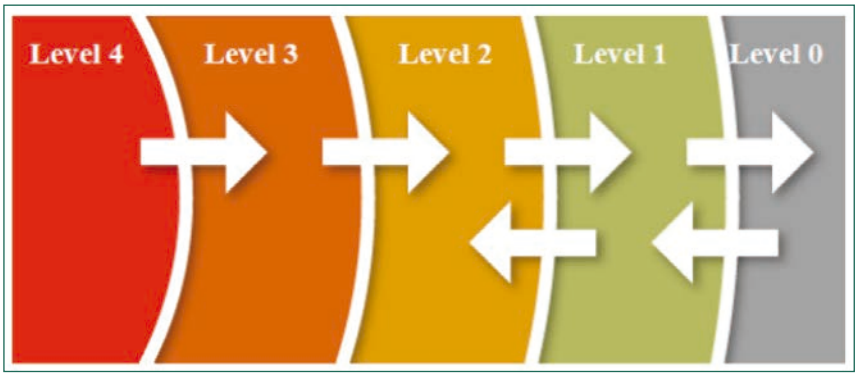

Figura 2. Esquema de defensa en produndidad.

DIFERENCIAS

- Nivel de detalle. El nivel de detalle de los programas que proponen IEC y el OIEA es sensiblemente menor que el de NEI. El motivo es que éste responde a un marco regulatorio concreto, mientras que IEC y el OIEA deben poder adaptarse a cualquier marco legislativo o regulatorio.
- Identificación de activos.
  – NEI – Los activos considerados en el programa de ciberseguridad de las guías de uso en EE.UU. son aquellos que pueden afectar al desempeño de las funciones de seguridad, seguridad física y actuación ante emergencias, incluyendo, además, los sistemas de soporte asociados a las funciones anteriores, como ventilación, aire acondicionado o sistemas contra incendios.
  – OIEA– El alcance del programa que propone el OIEA es muy amplio. Sin excluir ningún tipo de equipo, se centra en sistemas de seguridad y seguridad física, considerando también equipamiento para realizar su diagnóstico y mantenimiento. Menciona también otros equipos no relacionados de forma directa con los anteriores, como sistemas de gestión de órdenes de trabajo o de gestión documental, donde se almacenan diagramas, minutas de reuniones u otra información que pueda ser utilizada en un ataque.
  – IEC – El alcance del programa de IEC es sensiblemente más reducido, ya que sólo tiene en cuenta aquellos sistemas de I&C que desempeñan funciones de seguridad y los que tienen una incidencia en el funcionamiento global de la planta, incluyendo los equipos usados para diagnóstico y mantenimiento. Quedan excluidos explícitamente equipos de seguridad física y actuación ante emergencia, así como cualquier otro dispositivo que no sea de I&C.
- Niveles del modelo de defensa
  – NEI – Las guías que se utilizan en EE.UU. proponen, a modo de ejemplo, algunos modelos de defensa con cuatro y cinco niveles aplicables a todos los equipos digitales de la planta, ya sean CDA u otros dispositivos de naturaleza digital. No se impone, por tanto, ningún modelo (número y características de los niveles), aunque sí algunas restricciones, por ejemplo:
    – el control del flujo de información entre los niveles de mayor protección y los más bajos debe ser determinista[4], y
    – todos los flujos de información entre niveles están controlados

[3]El criterio para establecer la criticidad de un equipo es diferente en cada línea de trabajo.

y no existen baipases a los equipos de control (cortafuegos, diodos de datos).

– OIEA – Igual que en el caso anterior, el OIEA deja a criterio de la planta el número de niveles y las medidas de protección asignadas a esos niveles. Se da un ejemplo de un modelo de 5 niveles que aplica a todos los activos digitales de la planta. Además del nivel, la guía del OIEA define otro concepto relacionado: la *zona*, que es una agrupación, en base a consideraciones lógicas (por ejemplo, en la misma red de comunicaciones) y/o físicas (en la misma ubicación), de activos que tienen una importancia similar en cuanto a seguridad y/o seguridad física.

– IEC – Al contrario que en los casos anteriores, el programa de IEC define de manera explícita tres niveles (definidos "grados de ciberseguridad" en los documentos de IEC), denominados S1, S2 y S3 (en orden de mayor a menor protección). Estos niveles están pensados 'sólo' para los sistemas I&C digitales y no para todos los dispositivos de la planta, como en el caso de los ejemplos que exponen las otras guías. Los flujos de información entre niveles también quedan definidos en IEC 62645. Fundamentalmente,
  – se permite la comunicación entre dispositivos del mismo nivel
  – se permite el flujo descendente entre niveles adyacentes (S1 a S2 y S2 a S3, pero no S1 a S3)
  – cualquier flujo ascendente debe justificarse especialmente si es una comunicación hacia S1, que está explícitamente desaconsejada.

  IEC maneja el mismo concepto de zonas que el OIEA.

- Descripción de las medidas de ciberseguridad de los niveles de protección
  – NEI – Las guías de NEI establecen un catálogo de requisitos concretos de modo que todos los equipos en el alcance del programa de ciberseguridad deben, en principio, ser evaluados frente a ese listado de controles.
  – OIEA – La Agencia no detalla en sus textos qué medidas concretas deben aplicarse para proteger los equipos, y se refiere a la realización de un análisis de riesgo para identificar estas medidas.
  – IEC—El estándar principal de IEC en esta materia, IEC 62645, establece un conjunto de medidas mínimas para cada nivel de la estructura defensiva. El objetivo del estándar que está elaborando, IEC 63096, es describir de forma más explícita y detallada estas medidas.
- Categorización de los activos y asignación a los niveles de protección
  – NEI – la asignación de los CDA a los niveles del modelo de defensa no está definida y queda a criterio de la planta. En cualquier caso, las medidas de protección se asignan en función de la categoría del CDA y no del nivel del modelo. Estas categorías se definen en NEI 13-10 *Cyber Security Control Assessments*, y son tres: CDA de actuación ante emergencia con medios alternativos, CDA indirectas y CDA directas. La protección es menor para las primeras, algo mayor para las CDA indirectas y total para las directas.
  – OIEA – La Agencia supedita la asignación de los activos a los niveles del modelo de defensa en función de dos factores:
    – la relevancia o incidencia del activo sobre las funciones de seguridad y seguridad física, y
    – un análisis del riesgo que estudie vulnerabilidades, amenazas y potenciales consecuencias y probabilidad de ocurrencia de una malfunción o indisponibilidad del equipo. En este sentido, el OIEA no propone ninguna metodología concreta para hacer este análisis de riesgos.
  – IEC – La asignación de los dispositivos a los niveles o grados de seguridad depende de dos factores. Por un lado, la categoría (A, B o C) de la función de seguridad en la que participan. Estas categorías están definidas en IEC 61226 *Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions*. Por otro lado, las consecuencias más adversas, desde el punto de vista de la seguridad y del comportamiento de la planta, que tendría un ciberataque sobre el dispositivo, en caso de progresar. Estas potenciales consecuencias más adversas deben analizarse antes de llevar a cabo la asignación. En IEC 62645 se indican las siguientes consideraciones para llevar a cabo las asignaciones:
    – los sistemas que implementan funciones de categoría A se asignan al grado de ciberseguridad S1,
    – los sistemas que implementan funciones de categoría B y aquellos que son necesarios para la operación en tiempo real[5] de la planta se asignan al grado de ciberseguridad S2 como mínimo,
    – los sistemas implementando funciones de categoría C se asignan al grado de ciberseguridad adecuado al análisis de consecuencias,
    – los sistemas que contribuyen al funcionamiento global de la planta se asignan al grado de ciberseguridad S3, y
    – los equipos de diagnóstico y mantenimiento, en caso de que necesiten conectarse directamente al sistema de I&C, ya sea la conexión permanente o temporal, se asignan al grado de ciberseguridad que tenga el propio sistema I&C.

    NOTA: En relación a estas consideraciones, el estándar indica que un sistema puede asignarse a un nivel superior de protección si se considera que las consecuencias más adversas que tiene asociadas son equiparables a las de los equipos de ese nivel superior de protección.

CONCLUSIONES

La importancia que la industria nuclear está dando a la ciberprotección de los sistemas digitales queda de manifiesto en el interés que han mostrado en esta materia las organizaciones dedicadas a la publicación de estándares y guías. Ese interés se ha materializado en una serie de documentos cuyos enfoques son similares en líneas generales, pero que guardan también ciertas diferencias. En este artículo, de marcado carácter divulgativo, se han presentado las líneas de trabajo de las organizaciones más importantes y un análisis comparativo de sus enfoques, con el objetivo de proporcionar una referencia lo más completa posible que permita a una central valorar el grado de adecuación de sus políticas de ciberseguridad a los estándares y guías más reconocidas. ■

[4]Un control de flujo entre niveles puede ser basado en reglas o determinista. La diferencia entre ambos es que, para el caso determinista, la comunicación de datos en uno de los sentidos es físicamente imposible. Este tipo de control se hace típicamente con diodos de datos.

[5]El concepto de tiempo real supuso un gran debate en el desarrollo del estándar y será sustituido en la nueva edición por "sistemas con un impacto directo e inmediato en la seguridad o en la operación general de la planta".