



SERIE Smart OT, Número 4

Smart Factory ante el desafío de la seguridad

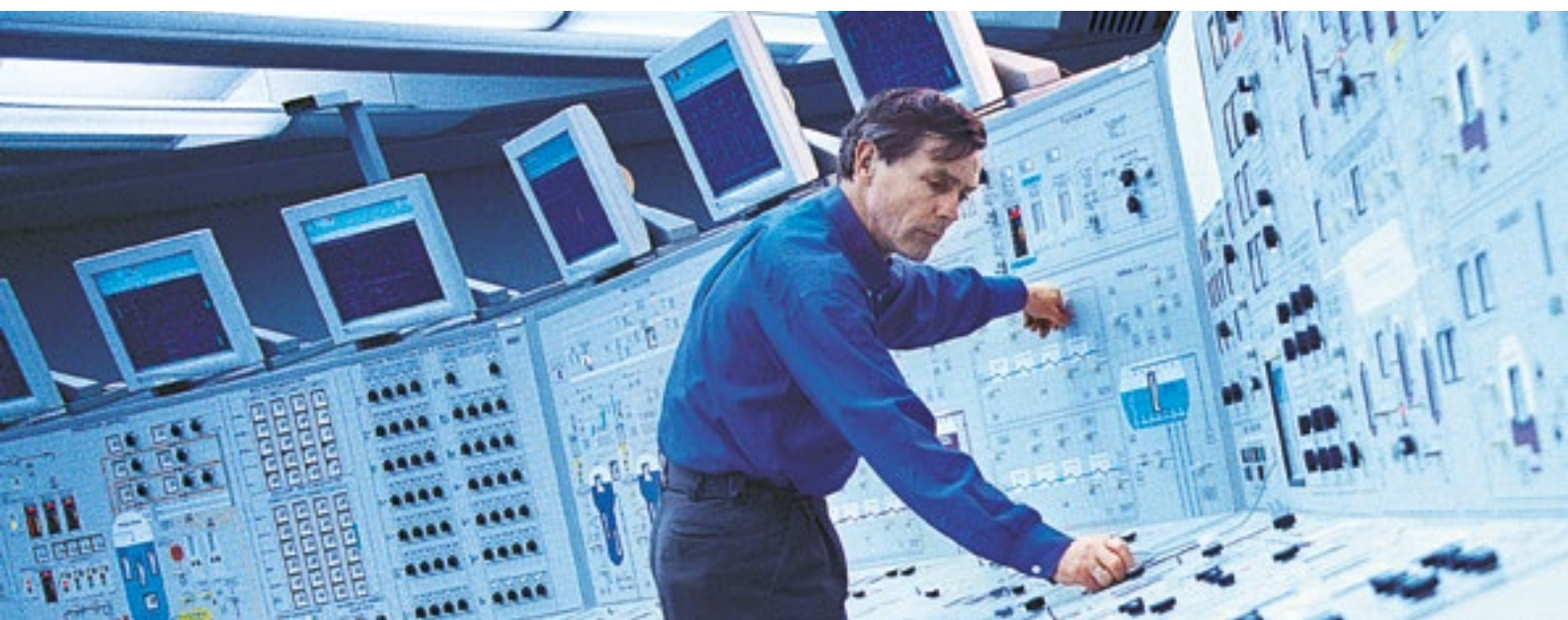
Retos en la adopción de Smart Factory en la industria



El Centro de Ciberseguridad Industrial (CCI) es una organización independiente, sin ánimo de lucro, cuya misión es impulsar y contribuir a la mejora de la Ciberseguridad Industrial, en un contexto en el que las organizaciones de sectores como el de fabricación o el energético juegan un papel crítico en la construcción de la Sociedad actual, como puntales del estado del bienestar.

CCI afronta ese reto mediante el desarrollo de actividades de investigación y análisis, generación de opinión, elaboración y publicación de estudios y herramientas, e intercambio de información y conocimiento, sobre la influencia, tanto de las tecnologías, incluidos sus procesos y prácticas, como de los individuos, en lo relativo a los riesgos -y su gestión- derivados de la integración de los procesos e infraestructuras industriales en el Ciberespacio.

CCI es, hoy, el ecosistema y el punto de encuentro de las entidades -privadas y públicas- y de los profesionales afectados, preocupados u ocupados de la Ciberseguridad Industrial; y es, asimismo, la referencia hispanohablante para el intercambio de experiencias y la dinamización de los sectores involucrados en este ámbito



Edición: 2018-2019

ISBN: 978-84-121149-2-8

Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra queda rigurosamente prohibida y estará sometida a las sanciones establecidas por la ley. Solamente el autor (Centro de Ciberseguridad Industrial, www.cci-es.org), puede autorizar la fotocopia o el escaneado de algún fragmento a las personas que estén interesadas en ello.

➤ Paseo de las Delicias, 30 · 2º piso
28045 MADRID
☎ +34 910 910 751
✉ info@CCI-es.org
🌐 www.CCI-es.org
📖 blog.CCI-es.org
🐦 @info_CCI



Consejos

Alt+flecha izquierda para volver a la vista anterior después de ir a un hipervínculo

Haz click en nuestro icono  y visita nuestra web

Haciendo click en la banderas de la portada podrás ver la actividad de CCI en cada uno de esos países

Haciendo click en el título de la cabecera volverás al índice



PATROCINADORES DE CCI

Platinum



Gold



Silver



Bronze





TABLA DE CONTENIDO

› INTRODUCCIÓN	6
› INDUSTRIA 4.0 Y SMART FACTORY	7
LA CUARTA REVOLUCIÓN INDUSTRIAL	7
SMART FACTORY	9
MARCOS DE REFERENCIA DE INDUSTRIA 4.0	9
INICIATIVAS EUROPEAS DE INDUSTRIA 4.0	10
› OPORTUNIDADES Y BENEFICIOS DE SMART FACTORY	11
› SEGURIDAD Y SMART FACTORY	13
› RIESGOS Y DESAFÍOS DE SMART FACTORY	13
› HACIA EL OBJETIVO DE LA CIBERSEGURIDAD EN SMART FACTORY	15
› BIBLIOGRAFÍA	17
› AUTORES	18
› OTROS NÚMEROS PUBLICADOS DE ESTA SERIE	19

ÍNDICE DE FIGURAS

› FIGURA 1. INTEGRACIÓN DE LAS TECNOLOGÍAS DE OPERACIÓN Y TECNOLOGÍAS DE LA INFORMACIÓN	6
› FIGURA 2. DIAGRAMA DEL DKFI DE LAS CUATRO EVOLUCIONES INDUSTRIALES	7
› FIGURA 3. CAMBIOS TECNOLÓGICOS EN LA INDUSTRIA 4.0	8
› FIGURA 4. ECOSISTEMA SMART OT	12
› FIGURA 5. VOLUMEN DE NEGOCIO DE LA APLICACIÓN SMART OT	14
› FIGURA 6. IMPACTO DE INTERNET INDUSTRIAL O SMART OT EN EL MUNDO (WORLD ECONOMIC FORUM)	15

INTRODUCCIÓN

Este documento, el número 4 de la Serie Smart OT muestra cuales son los principales retos de ciberseguridad al adoptar Smart Factory. Estos retos deberán tenerse presentes al establecer requisitos clave en su adopción.

La transformación digital, y especialmente el uso de IoT (Internet de las Cosas) en el mundo está cambiando drásticamente los sectores más relevantes: Energía, Agricultura, Transporte, Salud y otros sectores industriales de la economía que, en su conjunto, representan casi dos tercios PIB mundial. Además, transformará el modo de trabajar entre humanos y máquinas.

En el Centro de Ciberseguridad Industrial nos gusta denominar Smart OT, a la integración de IT con OT que posibilita Smart Grid, Smart Cities, Smart Health, Smart Car y por supuesto **Smart Factory**, concepto surgido de la Industria 4.0, como la culminación de todo lo que engloba la Industria 4.0, pretende que las fábricas sean capaces de adaptarse de forma continua e inmediata a distintas tareas, cambiar los productos que se fabrican y adaptarlos a las necesidades específicas de cada cliente. Smart Factory empieza a proporcionar oportunidades sin precedentes, además de nuevos riesgos, a los negocios y la sociedad.

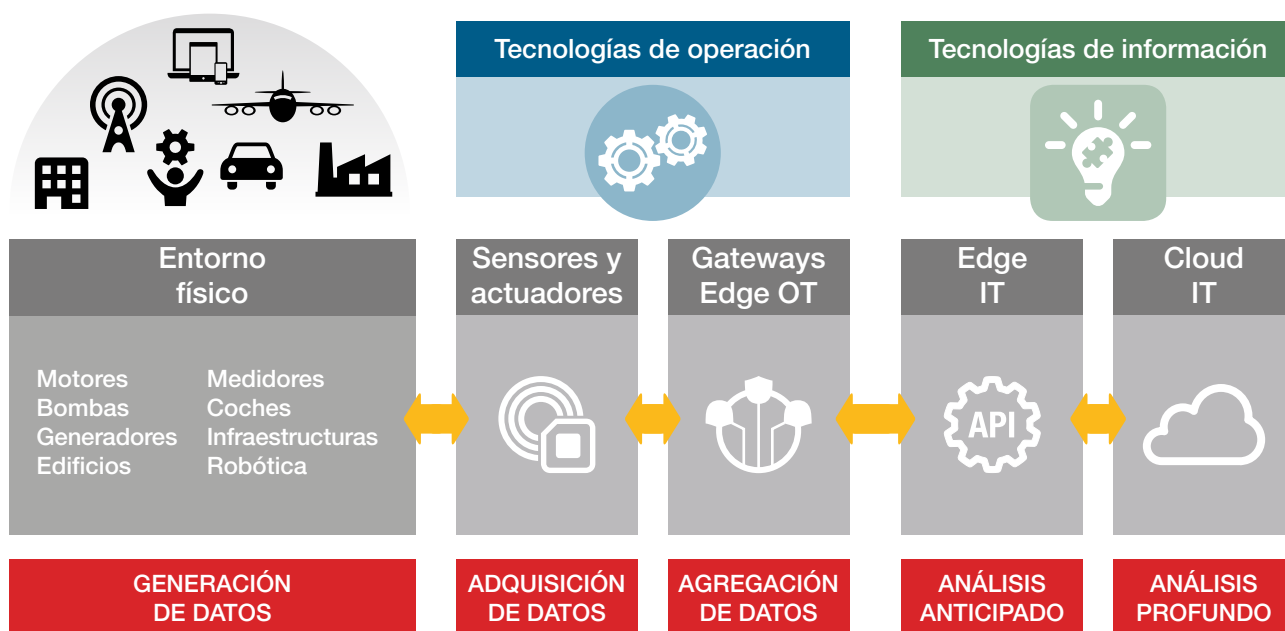


Figura 1 : Integración de las tecnologías de operación y tecnologías de información.

La revolución Smart OT está siendo transformadora, y está cambiando la base de la competencia, redibujando los límites de la industria y creando una **nueva generación de empresas disruptivas**, similar a lo que la actual Internet ha dado a Amazon, Google, Netflix, etc. Sin embargo, este cambio no está siendo fácil, la gran mayoría de las organizaciones luchan por entender las implicaciones del Internet Industrial en sus empresas e industrias. Para estas organizaciones, los riesgos de quedarse atrás son reales.

INDUSTRIA 4.0 Y SMART FACTORY

LA CUARTA REVOLUCIÓN INDUSTRIAL

La idea de que se avecinaban importantes cambios en el sector de la fabricación industrial se muestra por primera vez en 2005, con la publicación de la obra de Neil Gershenfeld: “FAB: The Coming Revolution on Your Desktop. From Personal Computers to Personal Fabrication”. En ella se introducía el concepto de Fabricación Personal, esto es, la capacidad de diseñar y producir productos propios en el ámbito doméstico gracias a un equipo que combina la electrónica de consumo con las herramientas industriales. La obra asimila la revolución que supondrá la fabricación personal a la que supuso la informática personal a finales del siglo XX con el paso de los grandes equipos de cálculo a los ordenadores de sobremesa.

Desde ese momento diversos autores introducen el concepto de “revolución” en sus trabajos para referirse a un nuevo escenario industrial en el que se tratan conceptos como la replicación de objetos, la confluencia entre los mundos físico y digital (sistemas ciberfísicos), la conectividad entre máquinas (M2M), etc. Así, en 2011, el DFKI (Centro Alemán de Investigación en Inteligencia Artificial) presenta el diagrama que muestra las cuatro revoluciones industriales a lo largo de la historia, el cuál sirvió como base del término Industria 4.0, utilizado por primera vez ese mismo año en la Feria de Hanover (Hannover Messe), una de las ferias industriales más importantes del mundo.

Siguiendo el diagrama del DFKI, la segunda revolución industrial se situaría a principios del siglo XX con la aparición de la cadena de producción (división del trabajo en tareas y producción en masa) gracias, principalmente, a la aplicación de la energía eléctrica.

DE LA INDUSTRIA 1.0 A LA INDUSTRIA 4.0

GRADO DE COMPLEJIDAD

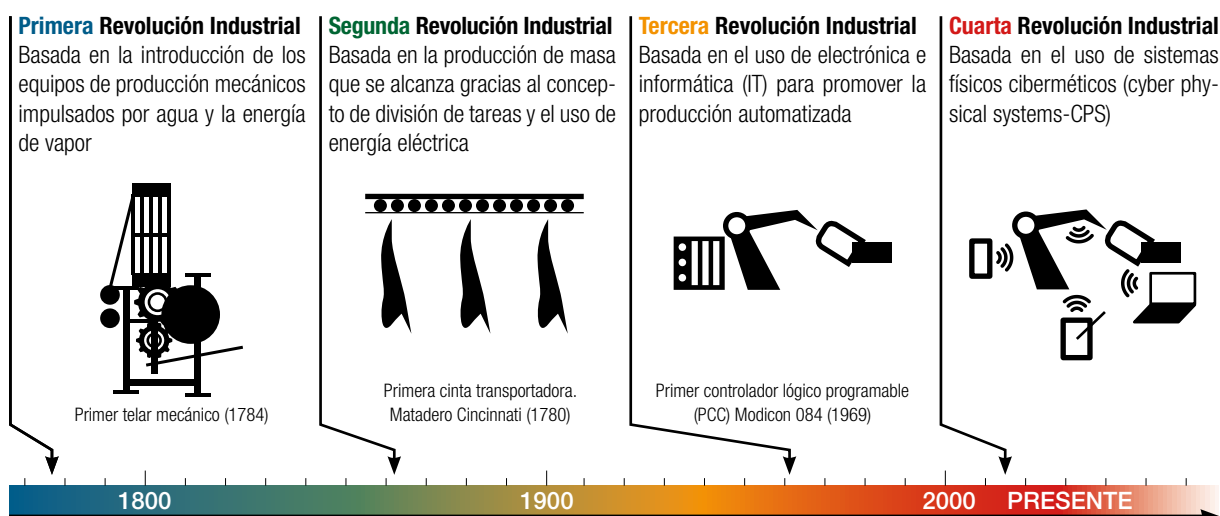


Figura 2 : Diagrama del DFKI de las cuatro revoluciones industriales.

La tercera revolución industrial se inició en el último tercio del siglo XX y tiene que ver con la aparición del microprocesador y el consecuente desarrollo de la electrónica y la informática. Un hito destacable es la aparición del primer controlador programable (PLC), el Modicon 084, en 1969.

Finalmente, el desarrollo de Internet de las Cosas (IoT) y el concepto de los sistemas ciberfísicos conectados nos lleva a las puertas de la cuarta revolución industrial en la que estamos inmersos actualmente. Si bien los sistemas ciberfísicos es un concepto que ya existía en la tercera revolución industrial (PLCs y robots industriales, por ejemplo) la revolución aparece cuando estos sistemas evolucionan para aprovechar las capacidades de comunicación y tratamiento de datos actuales: IIoT, sistemas embedded, robótica colaborativa, fabricación aditiva, impresoras 3D, procesamiento y almacenamiento en la nube, analítica de datos, etc.

El Grupo de Trabajo “Industrie 4.0” elaboró en 2013 el informe “Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0: Securing the Future of German Manufacturing Industry” los principales cambios tecnológicos que aportaría la industria 4.0 a Smart factory son los siguientes:

- Mejora de la eficiencia como resultado de mantenimientos precisos y tiempos de parada cercanos a cero.
- Personalización de la impresión 3D y posibilidad de producción local.
- Incremento de la seguridad física y operacional como consecuencia de la auto-optimización y corrección.
- Optimización de los ciclos de producción gracias a la comunicación entre componentes de modo que serán capaces de preparar los siguientes pasos hasta la entrega final.
- Industrialización virtual, facilitando el diseño y testeo de nuevas plantas o procesos en el mundo digital, reduciendo los fallos posteriores.
- Integración extrema a extremo de los equipos de ingeniería en toda la cadena de valor.
- Integración vertical y sistemas de producción en red.

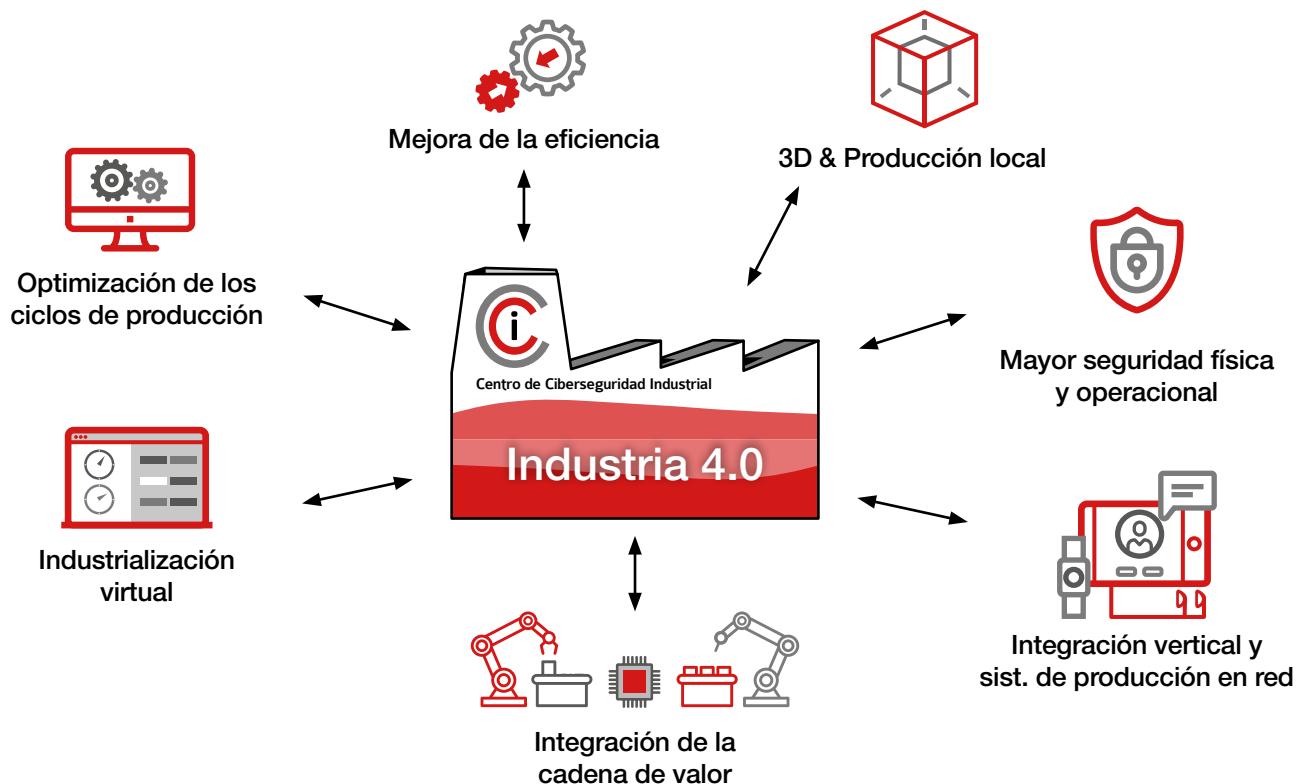


Figura 3 : Cambios tecnológicos en la Industria 4.0.



SMART FACTORY

Una Smart factory (considerada como la fábrica del futuro o fábrica inteligente) es una instalación de producción que se encuentra altamente digitalizada y conectada. Es un término que se encuentra unido a la cuarta revolución industrial o Industria 4.0.

La principal característica de Smart Factory es su capacidad para funcionar con mínima intervención humana, así como aprender y adaptarse a los cambios en tiempo real. Cuenta con procesos mucho más flexibles que las fábricas del pasado y pueden funcionar de forma autónoma.

Los procesos productivos son capaces de adaptarse de forma continua e inmediata a distintas tareas. A diferencia de las antiguas fábricas de producción en serie, donde se establecía una cadena de producción muy rígida, en smart factory los componentes envían información constantemente.

El análisis de la información mediante Big Data permite adaptar la fabricación a cada necesidad. La producción es más versátil y varía según la necesidad de cada momento.

En Smart factory los departamentos están conectados entre sí, y también externamente con clientes y proveedores. P.e. Las máquinas de producción ubicadas en la red local reciben pedidos. Podrán acceder a las instrucciones de trabajo, informar del progreso de producción y estarán en interacción los sistemas de calidad y trazabilidad. Los operarios de planta en tiempo real tienen acceso a información relevante como instrucciones, horarios, datos de calidad, inventario, etc.

En Smart Factory se trabaja de forma conjunta para cubrir las necesidades específicas de cada cliente / producción y se logra un gran ahorro al aumentar la eficiencia de toda la fábrica.

MARCOS DE REFERENCIA DE INDUSTRIA 4.0

El actual panorama industrial propone nuevos retos derivados de un mercado global, la necesidad de interoperabilidad entre productos o el máximo aprovechamiento de las tecnologías industriales para satisfacer las nuevas necesidades y requerimientos de los clientes. En este contexto, el término Industria 4.0 ha sido ampliamente adoptado, tanto en su acepción en referencia a la denominada 4ª Revolución Industrial como por lo concerniente al paradigma de la industria inteligente, conocido también como Smart Factories o Smart Manufacturing. Varios consorcios han redactado sus propios marcos de referencia en cuanto a las arquitecturas de la Industria 4.0, cada uno de ellos respaldado por su correspondiente organización. Destacamos, a continuación, los dos principales.

Por un lado, tenemos la Plattform Industrie 4.0, organización de origen alemán que presenta la arquitectura RAMI 4.0 (Reference Architecture Model Industrie 4.0) que desde 2016 se ha convertido en estándar al integrarse en la norma DIN 91345 y, recientemente, como estándar internacional en el marco de la norma IEC/PAS 63088 («Smart manufacturing – Reference architecture model industry 4.0»). RAMI 4.0 propone un modelo de capas tridimensional que combina las siguientes dimensiones: los componentes de la Industria 4.0, desde el producto hasta el mundo conectado; el ciclo de vida de los productos y sistemas de producción; y la asignación de funciones y responsabilidades.

Por otro lado, el Industrial Internet Consortium (IIC), de origen estadounidense, pero con vocación internacional, propone su arquitectura de referencia denominada IIRA (Industrial Internet Reference Architecture), aunque -por el momento- no ha llegado a convertirse en estándar. A diferencia de RAMI 4.0, que tiene su base en las tecnologías operacionales, IIRA tiene su origen en el mundo de las TIC. Define unos dominios funcionales agrupados en capas, siendo la capa superior la de negocio, que se apoya solidariamente sobre las de operaciones, información y aplicaciones. Estas capas interactúan con los sistemas físicos a través de la capa de control (que contiene los sensores y actuadores).



La interconexión –digital– entre las capas del modelo, ya sea en una arquitectura o en la otra, introduce ciertas vulnerabilidades que inciden en la protección de los sistemas industriales. En este sentido, el enfoque desde la perspectiva de la ciberseguridad está mucho más desarrollado por parte del Industrial Internet Consortium, quienes, partiendo del modelo propuesto por el IIRA han desarrollado su propio marco de referencia sobre ciberseguridad, denominado IISF (Industrial Internet Security Framework). Este marco ayuda en la toma de decisiones informadas partiendo de un diseño de evaluaciones de riesgos. El IISF también define los riesgos, las evaluaciones, las amenazas, las métricas e indicadores de rendimiento para ayudar a los gerentes de empresas a proteger sus organizaciones.

INICIATIVAS EUROPEAS DE INDUSTRIA 4.0

En 2015 la Comisión Europea propuso la “Estrategia para el Mercado Único Digital” (Digital Single Market) con el objetivo de lograr que la economía, la industria y la sociedad europeas aprovechen plenamente la nueva era digital. Entre las iniciativas derivadas de esta Estrategia se encuentra la política denominada “Digitising European Industry”.

Según cifras de la Unión Europea, dos millones de compañías comprenden el sector industrial en Europa, dando empleo a 33 millones de personas. La digitalización de la industria y la adopción de nuevas estrategias empresariales, como Industria 4.0, aportarán unos ingresos de más de 110 billones de euros en los próximos cinco años. La Comisión ha impulsado la creación de iniciativas de iniciativas nacionales de apoyo a la digitalización industrial.

A fecha de junio de 2018, 15 países han puesto en marcha sus iniciativas nacionales, con diferentes niveles de madurez, entre cuyos resultados cabe citar la financiación de actividades o centros de investigación, el impulso de iniciativas público-privadas, creación de “clusters” industriales, puesta a disposición de “test-beds”, etc.

› DINAMARCA

Manufacturing Academy of Denmark (MADE)

<http://made.dk/>

› ESPAÑA

Industria Conectada 4.0

<http://www.industriaconectada40.gob.es/>

› FRANCIA

Alliance pour l'Industrie du Futur

<http://allianceindustrie.wix.com/industrie-dufutur>

› HOLANDA

Smart Industry

<http://www.smartindustry.nl/>

› HUNGRÍA

IPAR4.0 National Technology Initiative

https://www.i40platform.hu/en/about_us

› ITALIA

Industria 4.0

<http://www.sviluppoeconomico.gov.it/index.php/it/>

› LITUANIA

Pramonė 4.0

<http://www.industrie40.lt/platform/>

› LUXEMBURGO

Digital For Industry Luxembourg

<https://www.fedil.lu/>

› POLONIA

Initiative and Platform Industry 4.0

<http://www.mii.gov.pl/>

› PORTUGAL

Indústria 4.0

<https://www.industria4-0.cotec.pt/>

› SUECIA

Smart Industry

<http://www.government.se/information-material/2016/04/smart-industry---a-strategy-for-new-industrialisation-for-sweden/>



En España, la iniciativa Industria Conectada 4.0 se puso en marcha en 2015 desde el Ministerio de Industria, Energía y Turismo en colaboración con la Secretaría de Estado de Telecomunicaciones para la Sociedad de la Información. En su documento de presentación establece que:

“Su misión es la definición de la estrategia para la digitalización de la industria, y se persiguen tres objetivos orientados a reforzar la competitividad del sector industrial español:

- *Incrementar el valor añadido y el empleo en la industria nacional.*
- *Favorecer el modelo español para la industria del futuro orientada hacia sectores con potencial de crecimiento (potenciando los sectores y desarrollando una oferta local de soluciones digitales).*
- *Desarrollar palancas competitivas diferenciales para favorecer la industria española e impulsar sus exportaciones.”*

También existen iniciativas como Industria X.0 (<https://www.accenture.com/us-en/services/industryx0-index>), que van más allá de los principios de Industria 4.0, planteando una transformación digital total en las cosas que hacemos y la forma en que las hacemos y combinando capacidades como inteligencia industrial, trabajador conectado, operaciones ágiles, 'servitización' y la ciberseguridad industrial.

OPORTUNIDADES Y BENEFICIOS DE SMART FACTORY

De la irrupción de Smart OT vendrá la creación de un nuevo “valor” en Smart Factory, gracias a los volúmenes masivos de datos de dispositivos conectados, y el aumento de la capacidad para tomar decisiones automatizadas y acciones en tiempo real. En principio las oportunidades claves de negocio se encuentran en cuatro áreas principales:

- **Mejora de la eficiencia operativa** (operational efficiency) (por ejemplo, la mejora de tiempo de actividad, la utilización de activos) a través del mantenimiento predictivo y gestión remota.

- **El resurgimiento de una nueva economía de resultado** (outcome economy), impulsado por los servicios de software; innovaciones en hardware; y el aumento de la visibilidad de los productos, procesos, clientes y socios.
- **Nuevos ecosistemas conectados**, coalescentes alrededor de plataformas de software que desdibujarán las fronteras tradicionales de la industria.
- **Colaboración entre humanos-máquina**, que se traducirá en un aumento de productividad a niveles sin precedentes y nuevas experiencias de acople al trabajo.

A medida que Smart factory tenga una adopción más amplia, las empresas pasarán de productos a servicios basados en resultados, donde las empresas competirán en su capacidad para entregar resultados medibles a los clientes. Tales resultados pueden variar desde tiempos garantizados de actividad productiva de una máquina, a cantidades reales de ahorro energético en edificios comerciales, o a rendimientos de cultivos garantizados en una parcela específica de terreno agrícola.

La entrega de estos resultados requerirá de nuevos niveles de colaboración a través de un ecosistema de Partners y/o actores comunes en todos los países, los cuales tendrán que combinar sus productos, servicios y conocimientos para satisfacer las expectativas creadas (ver figura adjunta).

Organismos Gubernamentales: Incluir actuaciones, tanto del gobierno local (agentes locales) como nacional, que incluya una estrategia clara de Smart OT, aporte de financiación.

La comunidad: Implementar proyectos orientado a los ciudadanos y grupos comunitarios.

Universidades y centros de investigación: Aportar conocimiento, proyectos de I+D.

PYMES: Creadoras de productos y servicios enfocados al área SmartOT, Big Data, etc.

Infraestructura: Empresas que aportarán las redes de transporte de agua, energía, etc.

Los grandes ganadores en la carrera del liderazgo de Smart Factory serán los que puedan aprovechar las oportunidades inherentes a estos nuevos modelos de negocio digitales y crear nuevos valores añadidos, aliándose con los partners adecuados.

Smart Factory impulsará el crecimiento en la productividad, ofreciendo nuevas oportunidades a las personas para mejorar sus habilidades y asumir la creación de nuevos tipos de puestos de trabajo. Una gran mayoría de ejecutivos encuestados creen que el creciente uso de "mano de obra digital" en forma de sensores inteligentes, asistentes inteligentes y robots transformarán las habilidades laborales del mañana. A la vez que los trabajos menos cualificados, serán cada vez más, sustituidos por máquinas, SmartOT permitirá crear nuevos puestos de trabajo altamente capacitados que antes no existían.

A su vez, las empresas también utilizarán las tecnologías de Smart OT para que sus puestos de trabajo sean más seguros y productivos, flexibles y atractivos.

A medida que estas tendencias se afiancen y se requieran nuevas habilidades, las personas van a depender cada vez más de las máquinas inteligentes para la capacitación laboral y desarrollo de habilidades.

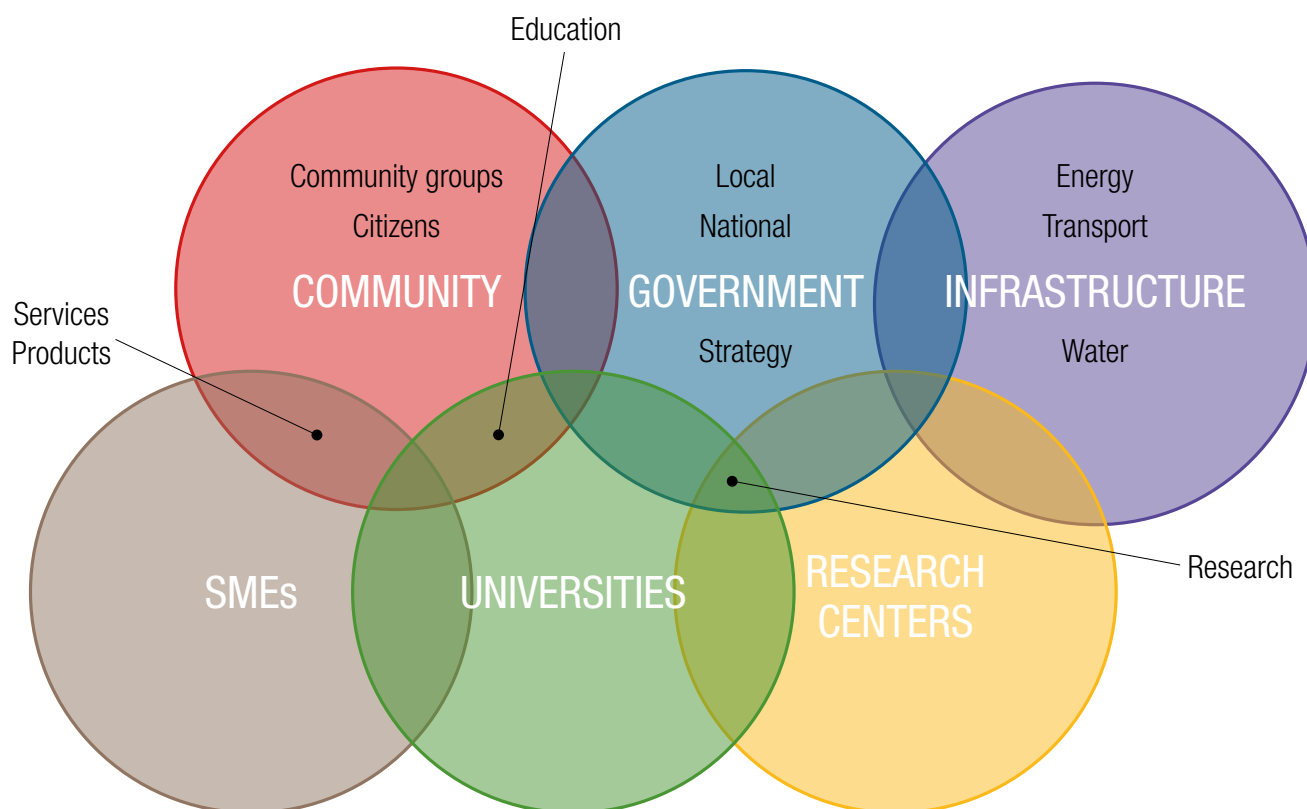


Figura 4 : Ecosistema Smart OT.



SEGURIDAD Y SMART FACTORY

Las ventajas competitivas que aporta el modelo de Smart Factory tienen su base en la capacidad de comunicación y de análisis de datos de los sistemas involucrados. Y son precisamente esas fortalezas del modelo las que pueden convertirse en sus mayores debilidades cuando las examinamos desde el punto de vista de la seguridad. La interconexión de los dispositivos ciberfísicos está ampliando considerablemente el perímetro que las empresas deben proteger puesto que el concepto de red industrial se está extendiendo más allá del ámbito hasta ahora bien definido y controlado de la planta industrial. No sólo por la proliferación de dispositivos, en cuanto a número de estos, o por la dispersión geográfica dónde éstos pueden encontrarse, sino también por la descentralización de los datos que generan o almacenan estos dispositivos. Así, conceptos como cloud o big data vienen estrechamente asociados a Smart Factory.

En este sentido, el documento “Industry 4.0” de la Comisión Europea (2016) incorpora la **ciberseguridad** como uno de los requisitos previos para la implementación de Smart Factory, junto con la estandarización de los sistemas, plataformas, protocolos...; el cambio en el sistema de gestión de los nuevos modelos de negocio; o la necesidad de trabajadores competentes y bien formados. La Comisión apuesta por la creación de instituciones públicas en los diferentes países para abordar la mejora de la ciberseguridad, aunque se refiere al paradigma de seguridad digital de un modo amplio, incluyendo: protección de la propiedad intelectual; privacidad y protección de datos personales; seguridad operacional y de los sistemas; protección del medioambiente, de la salud y de la seguridad física de las personas.

Hay que tener presente, también, que otro de los principios de Smart Factory tiene que ver con la cooperación dentro de la organización y entre compañías, así como la capacidad de crear redes ágiles de comunicación entre ellas. Esta situación añade un escenario más a la ampliación del perímetro corporativo que se menciona al principio de este apartado. Para mejorar la eficiencia de los procesos debe haber una comunicación total entre las entidades involucradas: personal, equipos, productos, etc. de diferentes compañías. Todo ello debe realizarse en un entorno protegido y de confianza para todas las partes ya que el ecosistema va

más allá de la pareja formada por el cliente y el proveedor, integrando a terceras partes como pueden ser ingenierías, consultoras, integradores, fabricantes de la maquinaria, empresas de mantenimiento, operadores logísticos, etc.

Si bien, a menudo, al analizar los principios de la seguridad en las redes de control industrial (ICS) se concede una mayor importancia a la Disponibilidad frente a la Confidencialidad de los datos, este enfoque puede variar cuando nos situamos en el ámbito de la Smart Factory. En un escenario de producción en red, con la interconexión e intervención de diferentes compañías en el proceso productivo, es necesario garantizar sin concesiones la protección de los tres principios básicos de la seguridad (Confidencialidad, Integridad y Disponibilidad). Es más, será de vital importancia para el éxito de Smart Factory, contar con las medidas adecuadas que garanticen también la Autenticidad (identificación y autorización de los participantes: compañías, usuarios, sistemas...) en la mencionada red de fabricación multi-empresa. La gestión de usuarios y de identidades, concepto poco explotado en la protección de los sistemas de automatización y control industrial, adquiere una importancia significativa en un proyecto de gestión de la ciberseguridad en Smart Factory.

RIESGOS Y DESAFÍOS DE SMART FACTORY

Para aprovechar todo el potencial del Smart Factory, las empresas y los gobiernos tendrán que superar una serie de obstáculos importantes. El principal de ellos será contemplar la seguridad y la privacidad de los datos, que ya están aumentando en importancia, dada la mayor vulnerabilidad a los ataques, el espionaje y el robo de datos impulsados por el aumento de la conectividad y el intercambio de datos. Hasta hace poco, la seguridad cibernética se ha centrado en un número de puntos limitado. Con la llegada de Internet Industrial, estas medidas ya no serán adecuadas pues el mundo físico y virtual se combinan a gran escala. **Las organizaciones necesitarán nuevos marcos de seguridad que abarquen todo el esquema de seguridad**, desde la autenticación a nivel de dispositivo, a los modelos de aseguramiento, resiliencia y respuesta a una incidencia concreta en todo el sistema.

Otra barrera importante es la falta de interoperabilidad entre los sistemas ya existentes, lo que aumentará significativamente la complejidad y el costo del despliegue del Internet Industrial en Smart Factory. Pero al mismo tiempo el crecimiento de la explotación de los datos en el ámbito industrial no se verá afectado por las regulaciones referentes a la privacidad, al no manejarse datos de carácter personal, como si ocurre en los sistemas de información.

No obstante, surgen nuevas obligaciones ligadas a la seguridad del dato, relacionadas con su propiedad, y es necesario delimitar quien puede acceder al dato: solo propietario, solo el fabricante de la máquina, ambos... ya que se trata de posible información que afecta a la confidencialidad y al secreto empresarial, estos aspectos deberán clarificarse. Por otro lado, los datos almacenados por los sistemas de monitorización pueden, en ciertas ocasiones, llegar a incidir en aspectos de productividad de los operarios, siendo por tanto ya un escenario para analizar, presumiendo una posible necesidad de consentimiento previo por parte del trabajador. La conectividad de las máquinas, la producción y los entornos generan nuevas cuestiones a las que hay que prestar una atención minuciosa en materia de seguridad, regulación, propiedad y derecho de acceso al dato.

En el futuro, un ecosistema digital completamente funcional requerirá el intercambio de datos entre máquinas y otros sistemas físicos de diferentes fabricantes. El impulso hacia la interoperabilidad será más complicado por la larga vida útil de la maquinaria industrial, que requerirá de una adaptación costosa o de un reemplazo para trabajar con las últimas tecnologías.

Además, otro riesgo es el rendimiento incierto frente a las fuertes inversiones en nuevas tecnologías inmaduras o no probadas, además de la falta de las reglamentaciones de los gobiernos, las fronteras geográficas y la escasez del conocimiento de la tecnología digital. La superación de estos desafíos requerirá de liderazgo, las implicaciones y acciones de colaboración entre las partes interesadas.

La firma Gartner declaró que la Internet de Cosas (IoT) fue la tecnología más publicitada en 2014. La gran mayoría se centra en aplicaciones de consumo, tales como casas inteligentes, coches conectados y wearables de consumo. Sin embargo, dentro de Smart OT es el negocio de Smart Factory, en última instancia, donde se encuentra el mayor potencial de negocio e impactos socioeconómicos como se puede apreciar en la siguiente gráfica.

NEGOCIO SMART OT

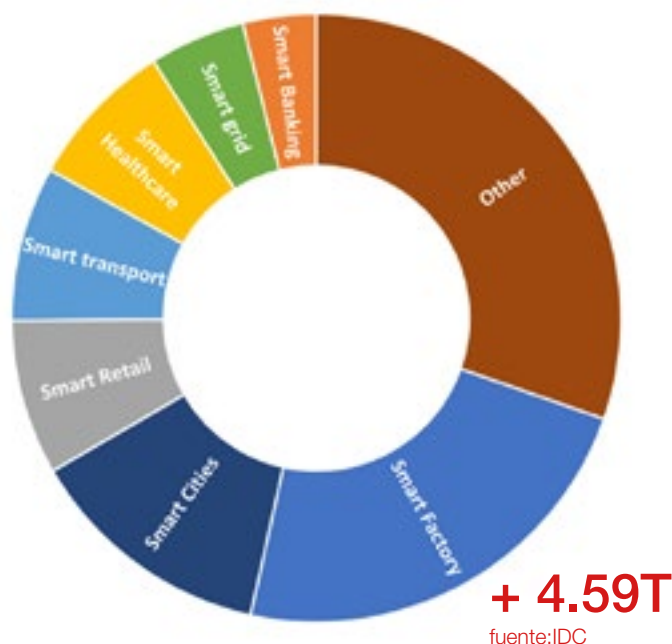


Figura 5 : Volumen de negocio de la aplicación de Smart OT.

Smart Factory a nivel mundial, se encuentra todavía en una etapa temprana, similar a lo que el Internet era a finales de 1990. Encuestas realizadas subrayan este punto: la gran mayoría (88%) de los encuestados dicen que todavía no entienden plenamente su modelo de negocio subyacentes y las implicaciones a largo plazo en sus industrias. Mientras que la evolución del consumidor de Internet en las últimas dos décadas proporciona algunas lecciones importantes, no está claro cuánto de este aprendizaje es aplicable al Internet Industrial dado su ámbito de aplicación específico. Por ejemplo: las respuestas en tiempo real son críticas en las industrias manufacturera, energía, transporte y sanidad. El tiempo real para el Internet de hoy son unos pocos segundos, mientras que el tiempo real para las máquinas industriales son milisegundos.

A pesar de estas barreras, la adopción de la Internet Industrial se está acelerando. Durante los últimos tres años, el número de sensores instalados ha aumentado más de cinco veces desde 4,2 mil millones en 2012 a 34 mil millones en 2018. Llama la atención los esfuerzos de las grandes empresas tales como Siemens, Cisco, GE, y Huawei, y las iniciativas del gobierno como Industrie 4.0 en Alemania. El segundo Foro del Internet Cosas Mundial organizado por Cisco presentó más de 250 ejemplos de implementación en el mundo real que muestran cómo empresas y municipios de todo el mundo aplican el Internet Industrial para impulsar la eficiencia, crear nuevas fuentes de ingresos y mejorar la calidad de vida de los ciudadanos y consumidores.

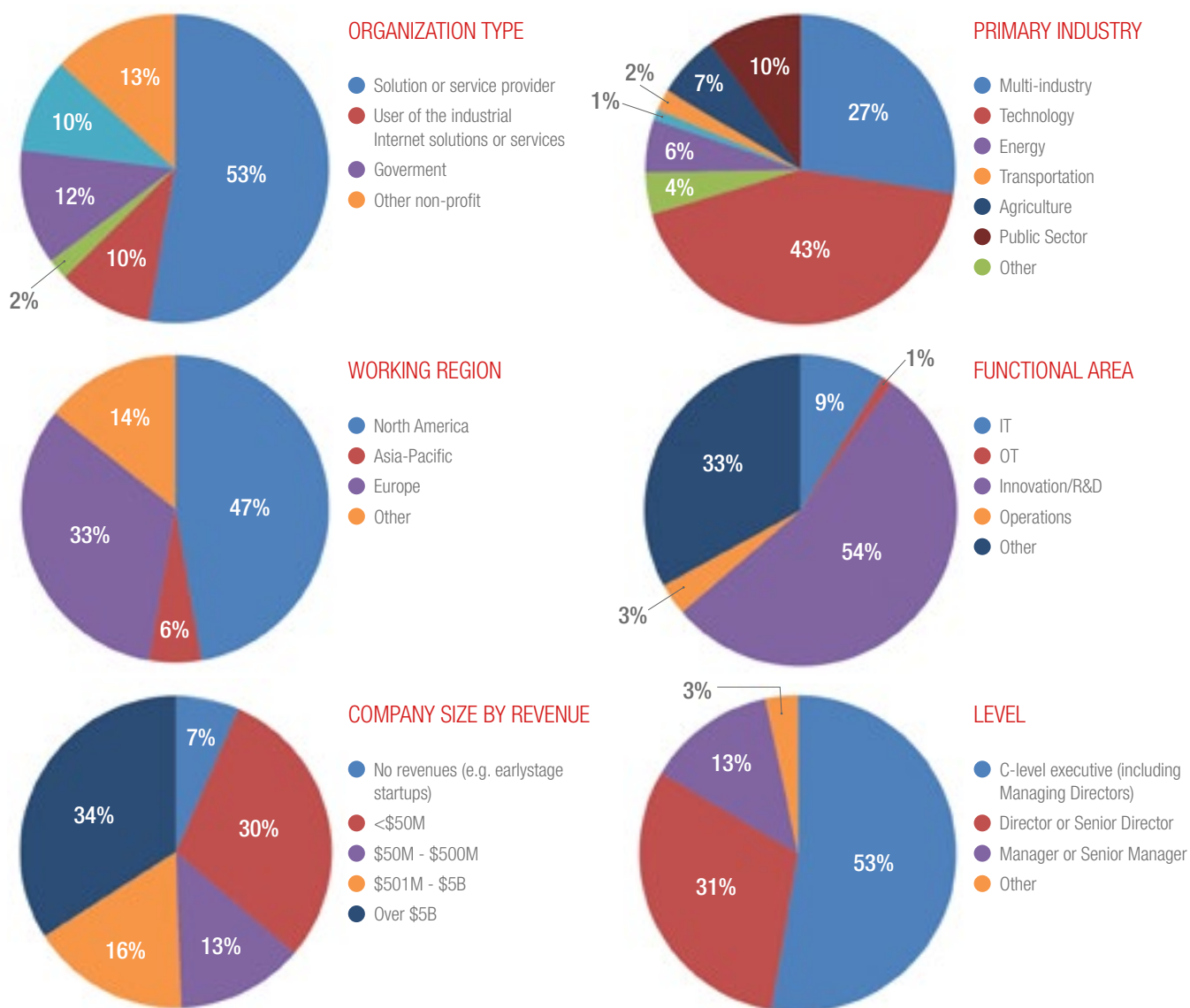


Figura 6 : Impacto del Internet Industrial o Smart OT en el mundo (Wold Economic Forum).

HACIA EL OBJETIVO DE LA SEGURIDAD EN SMART FACTORY

Si bien la revolución industrial ha sido creada por la demanda actual de los clientes, las organizaciones al emprender su plan de negocio hacia una tecnología puntera no siempre contemplan los riesgos que supone la interconexión de los diferentes dispositivos en una planta industrial. La convergencia entre los dispositivos ya existentes y la incorporación de nuevos da lugar a vulnerabilidades que pueden ser aprovechadas por aquellos que buscan la interrupción del funcionamiento del proceso, beneficio económico, o simplemente el error humano que se pueda producir de forma no voluntaria.

Las tecnologías para crear una fábrica inteligente ya existen y hay multitud de empresas que están disfrutando de sus ventajas. Sin embargo, existen hoy en día una serie de desafíos que impiden su adopción generalizada por parte de todas las industrias.

El principal escollo lo encontramos en la gran cantidad de datos que es necesario procesar. Dada la multitud de conexiones, el riesgo de ciberseguridad parece crecer exponencialmente. A todo esto, hay que sumar los costes o la inversión de proteger todos esos datos generados con nuevos dispositivos ciberseguros para la comunicación de éstos entre sí.



Un gran porcentaje de organizaciones se plantean si es verdaderamente necesario esta inversión o si es simplemente otro gasto más que hay que asumir. El ignorar la protección de los datos o de la misma planta de producción es un acto de riesgo en sí, ya que cada día que pasa, no sólo la industria gana en innovación sino los tipos de ataques diseñados para provocar el caos o en el peor escenario, el cierre de una organización. Un ejemplo no muy lejano, es el malware Wannacry, capaz de infectar, a la vez, a cientos de multinacionales y organismos institucionales en todo el mundo. Otros ataques informados en los sistemas de Industrial Internet of Things (IIoT) no solo sirven como un recordatorio de cómo son las amenazas reales en este campo, sino que también sirven como caso de estudio para comprender mejor las amenazas a las que nos podemos enfrentar.

Cualquier parada puede suponer grandes costes para la fábrica. Si además es necesario reconstruir el proceso hay que hacer frente a distintos gastos:

- Nuevo equipamiento, más moderno y capaz de registrar todo lo que hace.
- Posibles pérdidas por las paradas en la producción.
- Ralentizamiento de la producción hasta que se consiga ajustar a los parámetros deseados.
- Inversión en ingeniería y desarrollo.
- Costes de análisis de BigData y sistemas necesarios para el almacenamiento y proceso de los datos.
- Costes de especialistas en análisis

Para combatir todo ello, existe ya desde hace años un plan de concienciación por parte de las entidades públicas al igual que privadas, sobre los posibles riesgos que existen en el escenario industrial actual, y la necesidad no sólo de implantar medidas de ciberseguridad en los diferentes sectores de la organización y de sus equipos industriales, sino también en la formación de profesionales en el ámbito de la ciberseguridad industrial así como los altos cargos y sus empleados.

El avance es necesario para ser competitivo, pero sin las personas bien cualificadas para llevar a cabo las diferentes

funciones que las Smart Factories demandan, seguiremos expuestos a los riesgos externos y las consecuencias pueden llegar a ser devastadoras además de costosas.

Los operadores de planta, proveedores, clientes y otros fabricantes deben hacer de la ciberseguridad una prioridad en su estrategia de fábrica inteligente desde el principio.

Las organizaciones podrían comenzar examinando el equipo en la fábrica, desde los brazos del robot hasta sus HMI, para asegurarse de que cada dispositivo no esté expuesto en línea o tenga una autenticación débil o deshabilitada.

Las organizaciones de IIoT deben dar mayor importancia a la seguridad y la capacidad de recuperación. Los sistemas IIoT también pueden tener flujos de datos que incluyen intermediarios e involucran a múltiples organizaciones, que requieren una seguridad más sofisticada. Los integradores deben prepararse desde el principio para la gran cantidad de datos que implican las Smart Factories. Esto significa planificar por adelantado el tipo de equipo a utilizar, evaluar el protocolo de comunicación a adoptar, preparar procedimientos o estándares a seguir entre otras consideraciones.

El poder de adaptación a los cambios será un punto decisivo en muchas organizaciones para esta nueva Era de conectividad e innovadora productividad. La incorporación de medidas de ciberseguridad en una planta Smart tiene y debe ser primordial para el conjunto de la organización en sí y no sólo de los expertos.



BIBLIOGRAFÍA

- [1] ISO/IEC JTC 1 “Smart City Preliminary Report 2014” 2015.
URL (a 2016.04.30) http://www.iso.org/iso/smart_cities_report-jtc1.pdf .

Fuentes:

http://www.iso.org/iso/smart_cities_report-jtc1.pdf

http://www.osborneclarke.com/media/filer_public/b3/bc/b3bcaffa-2b02-465d-804d-af85d735e8e9/smart_cities_in_europe_e-version.pdf

<http://hipertextual.com/2015/05/smart-cities-espana>

http://www.voesi.or.at/wp-content/uploads/2013/02/Industry_40_Future_of_Productivity_April_2015_tcm80-185183.pdf

http://china.ahk.de/fileadmin/ahk_china/newsletter_magazines/01-2015_Ticker_GCT_S.pdf

http://www.bosch-si.com/media/si_form/index.php/confirm/index?fmfconfirm=03a264b227194d11d0aafc8ea9f432a5&fmfserv=en&fmftype=pdf

<http://www.eesc.europa.eu/resources/docs/labaye.pdf>

http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf

<http://hipertextual.com/2015/05/smart-cities-espana>

<https://www.futurelearn.com/courses/smart-cities/>

<https://industria40.me/blog/smart-factory>

<https://www.trendmicro.com/vinfo/mx/security/news/internet-of-things/security-threats-and-risks-in-smart-factories>



AUTORES

- › Susana Asensio, CCI.
- › Maite Carli, CCI.
- › José Luís Jiménez Izquierdo, Nunsys.
- › José Valiente, CCI.

COLABORADORES

- › Ignacio Álvarez, SIEMENS
- › Álvaro Anaya, EVERIS
- › Edorta Echave, LKS
- › Samuel Linares, ACCENTURE
- › José Lorenzo, EDP
- › Javier Pagès, ARKOSSA
- › Ignacio Redondo, SIDE



OTROS NÚMEROS, YA PUBLICADOS, DE ESTA SERIE

- | | |
|--|-------------------|
| 1. <i>'Smart grids' ante el desafío de la seguridad</i> | Noviembre de 2015 |
| 2. <i>'Smart Cities' ante el desafío de la seguridad</i> | Mayo de 2016 |
| 3. <i>El papel de los actores en Smart OT</i> | Mayo de 2018 |



📍 Paseo de las Delicias, 30 · 2º piso
28045 MADRID
☎ +34 910 910 751
✉ info@CCI-es.org
🌐 www.CCI-es.org
B blog.CCI-es.org
🐦 [@info_CCI](https://twitter.com/info_CCI)