ANÁLISIS DE REQUERIMIENTOS PARA SOLUCIONES EN LA CIBERSEGURIDAD DE PLATAFORMAS DE LA INDUSTRIA 4.0

Boletín No. 80
1o. de septiembre de 2020

Mtro. Flores Montaño Luis Alberto
Email: luisfloresmontano@hotmail.com
Mtra. Esther Viridiana Vázquez Carmona
evazquezc1801@alumno.ipn.mx
Mtro. Rodrigo Vázquez López
rodrigo_em2@hotmail.com
Dr. Juan Carlos Herrera Lozada
jlozada@ipn.mx

Instituto Politécnico Nacional
Centro de Innovación y Desarrollo Tecnológico en Cómputo

Resumen

El desarrollo de la tecnología y el uso del internet han provocado una revolución en la Industria 4.0; tal es el caso del internet de las cosas, dispositivos inteligentes, e información y datos que están en muchos sistemas, todo esto es posible en plena era de desarrollo tecnológico. Los principales componentes de la industria 4.0 como los sistemas ciberfísicos, el internet de objetos, el big data y la computación en la nube tienen algunos desafíos que deben superarse. Uno de estos desafíos es la ciberseguridad. En este documento, se analiza la estructura de las tecnologías en la industria 4.0 y la ciberseguridad. Adicionalmente se analizan los requisitos de estas tecnologías, para posteriormente tomar recomendaciones; todo esto con el propósito de usar dichas tecnologías en la Industria 4.0 de una forma segura. Finalmente, se toman medidas necesarias en contra de ciberataques y riesgos en el desarrollo; se discuten tecnologías y el uso de sistemas de seguridad.

Keywords: Ciberseguridad, solución, industria 4.0, análisis y requerimientos.

Abstract

The increase in technology development and the use of the internet have caused a revolution in Industry 4.0; such is the case of the internet of things, smart devices, information and data that are in many systems, all in the midst of technological development. The main components of Industry 4.0 such as cyber-physical systems, the Internet of Things, big data and cloud computing have some challenges that must be met. One of these challenges is cybersecurity. In this document, we discuss the structure of technologies in Industry 4.0 and cyber security. In addition, the requirements of these technologies are analyzed, to subsequently make recommendations, in order to use these technologies in Industry 4.0 in a safe way. Finally, necessary measures are taken against cyber attacks and development risks, and technologies and the use of security systems are discussed.

I Introducción

La revolución industrial ha comenzado a alcanzar su cuarta etapa, desarrollando y transformando diversos dispositivos. En primera instancia se tenían dispositivos mecánicos con funcionamiento de vapor y energía hidráulica constituyendo la primera revolución industrial. Después ocurrió el descubrimiento de la energía eléctrica, dando auge a la segunda revolución industrial, donde los dispositivos y la producción comenzaban a utilizar el ensamblaje en línea. Más tarde, con el desarrollo de tarjetas electrónicas y software, se reemplazaron los sistemas analógicos con sistemas digitales; a todos estos cambios se le conoció como la tercera revolución industrial. Los brazos robóticos, sensores y tecnologías de la información (TI) han sido utilizadas en los últimos años para la producción automática; adicionalmente son usadas en distintas áreas de la industria.

Así, con el desarrollo y la rápida expansión de internet, estas tecnologías se han convertido en nuevas e inevitables innovaciones; todo esto ha traído la cuarta revolución industrial. La industria 4.0 incluye dispositivos de mayor calidad y más rápidos para comunicarse entre sí y con las personas, con uso de sensores y sistemas de control, datos de proceso, y corrección de deficiencias y errores. Los sistemas ahora pueden comunicarse entre sí y comenzar a tomar decisiones sin necesidad de intervención humana. Las revoluciones industriales se muestran en la figura 1.

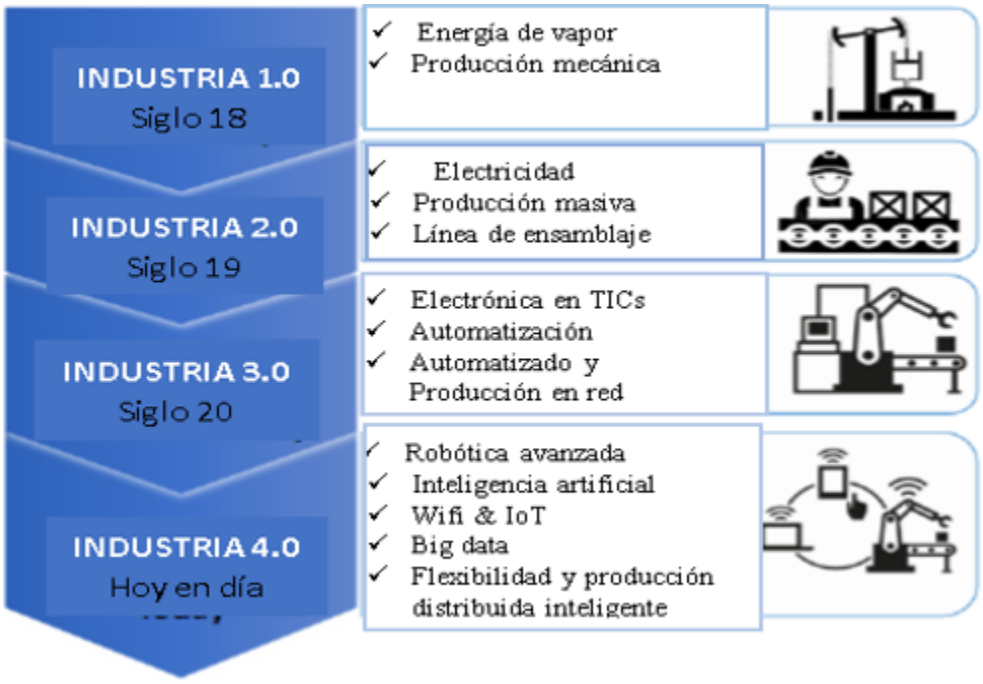

Figura 1. Revolución industrial.

Este artículo tiene como objetivo discutir algunos de los temas como las necesidades cibernéticas y métodos de solución que se están volviendo de suma importancia, debido al uso intensivo de las existentes tecnologías en la Industria 4.0, su comunicación con el Internet y el uso de tecnologías cibernéticas. También se discute acerca de las tecnologías en la industria 4.0 explicando brevemente cada una de ellas, así como las soluciones aplicadas a la ciberseguridad, y los requisitos de esta. Finalmente, se analiza la evaluación y los estudios futuros sobre esta materia.

II Plataformas de la industria 4.0

Las tecnologías básicas utilizadas en la Industria 4.0 se muestran en la Figura 2, cabe mencionar que estas tecnologías no se limitan únicamente a estas; existen además, los sistemas ciberfísicos (en inglés CPS), los identificadores por radiofrecuencia (en inglés RFID), la planificación de recursos empresariales (en inglés ERP), la nube basada en la manufactura (en inglés CBM), simulación, redes inalámbricas de sensores (en inglés WSN), aplicaciones inteligentes, inteligencia artificial (en inglés AI), y tecnología blockchain.

A. Sistemas ciberfísicos

Las estructuras que implican la comunicación y codificación entre el mundo físico y el mundo cibernético se llaman sistemas ciberfísicos o también CBS. Hay una interacción de componentes físicos y cibernéticos, ya que estos tienen las habilidades de entrenamiento y adaptación. Adicionalmente tienen un software integrado o embebido; también pueden trabajar juntos a través del internet e intercambiar datos tanto dentro como fuera del sistema.

Figura 2. La tecnología de la industria 4.0.

De acuerdo con la arquitectura CPS, la integración de hardware, software, así como de tecnologías que pueden detectar, responder, aprender y adaptarse a cambios En la figura 3 se muestra la estructura de la arquitectura CPS.

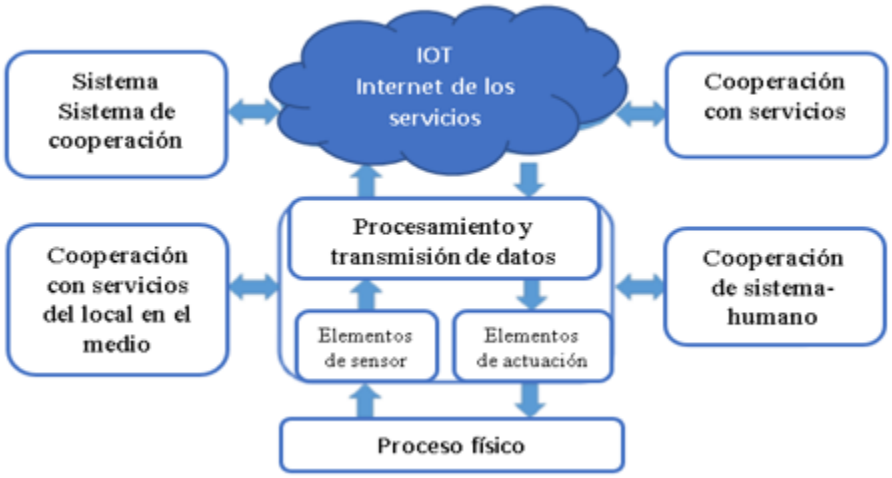

Figura 3. Estructura de CPS.

B. Internet de las cosas e internet de las cosas industriales

Las estructuras que permiten que los objetos se comuniquen son conocidas como Internet de las cosas (en inglés, IoT). Desde un punto de vista técnico, el internet de las cosas incluye sistemas ciberfísicos como es el caso de sistemas eléctricos, mecánicos, informáticos y de comunicación que permiten la comunicación basada en el internet y el intercambio de datos; En la figura 4 se resumen las tecnologías disponibles para IoT.

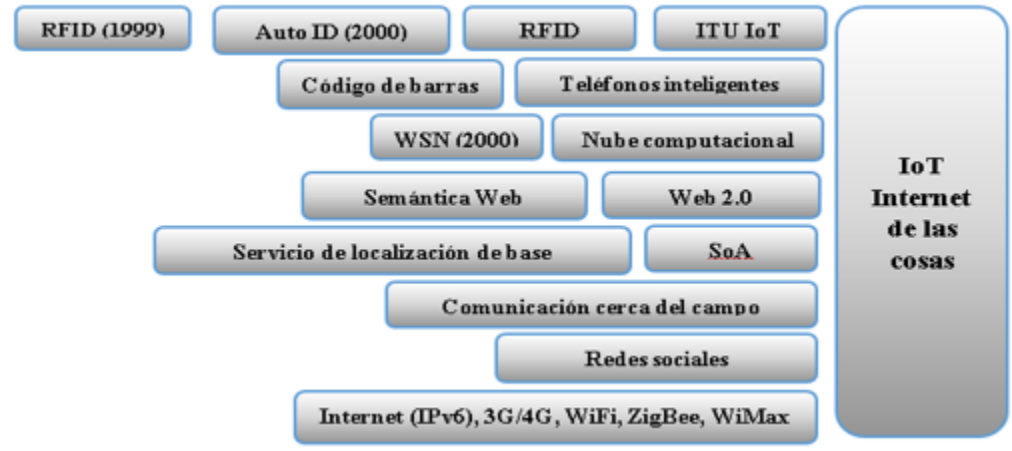

Figura 4. Tecnologías disponibles para IoT.

C. Big Data

El big data es la recopilación y evaluación de datos en diversas fuentes, así como de distintos clientes; estos datos se utilizan en sistemas de decisión en tiempo real, para distintos propósitos, como es el caso de la optimización de la producción, calidad, ahorro de energía y costos, y mejora en el servicio. Básicamente, una gran cantidad de datos ya sean estructurados o no estructurados son captados mediante sensores "inteligentes", dispositivos inteligentes, archivos de grabación y dispositivos de video y audio. La arquitectura de "Big Data" se muestra en la Figura 5.

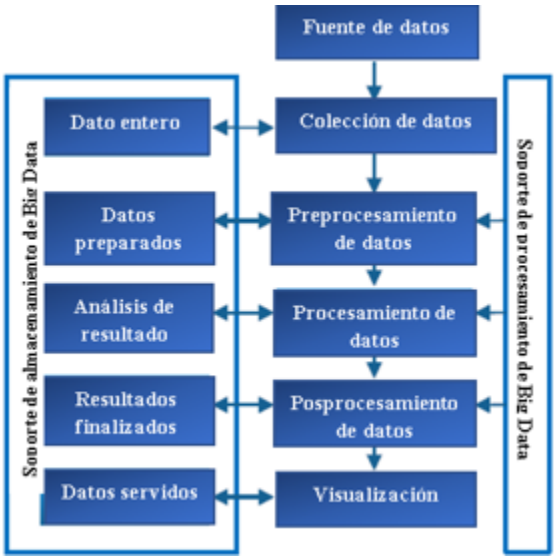

Figura 5. Arquitectura de Big Data.

D. Computación en la nube

La computación en la nube es una tecnología informática que ofrece un alto rendimiento de bajo costo. La industria 4.0 es una tecnología popular utilizada en sistemas de producción. La necesidad de potencia informática y de almacenamiento para mantenerse al día, y el volumen de datos de alta velocidad es requerido por las tecnologías industriales y las aplicaciones comerciales, esto ha llevado al desarrollo de una nube informática. La arquitectura de la computación en la nube se muestra en la figura 6.

Figura 6. Computadora de la nube.

F. Robótica avanzada

El uso de robots es cada vez más frecuente, como es caso de desarrollo de productos de alta calidad, sistemas de montaje y producción. Los robots pueden trabajar de manera más inteligente con procesamiento de información, inteligencia artificial, tecnologías de comunicación y control. La robótica es una tecnología capaz de hacer trabajos de mejor calidad, así como de apoyo humano y de prevención de accidentes laborales. El esquema de caracterización para robots autónomos se muestra en la Figura 7.

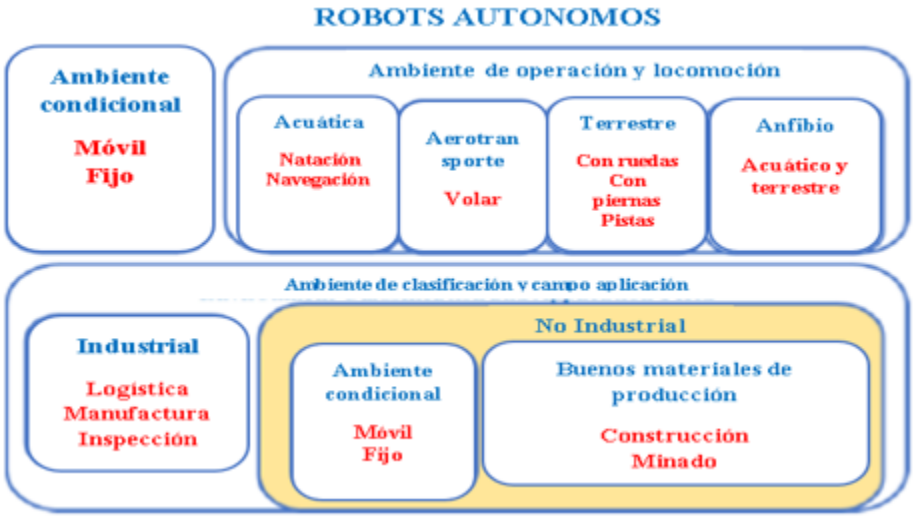

Figura 7. La caracterización de esquemas para robots autónomos.

H. Ciberseguridad

La unión internacional de telecomunicaciones (en inglés UIT) define la ciberseguridad como la suma de herramientas para proteger un entorno cibernético, ya sea para distintos elementos de una organización, los usuarios, políticas, conceptos de seguridad, medidas seguridad, enfoques de gestión de riesgos, acciones, capacitación, aseguramiento o tecnologías. La ciberseguridad busca fortalecer la seguridad de una organización, al igual que la confiabilidad de usuarios conectados a distintos dispositivos informáticos, así como la infraestructura, aplicaciones, servicios, sistemas de telecomunicaciones y la información transmitida y/o almacenada en el ciberespacio; todo esto debe ser protegido contra los riesgos relevantes.

III. Análisis de requerimientos para soluciones de seguridad cibernética

Los requisitos básicos para una adecuada implementación en la ciberseguridad consisten principalmente en los siguientes puntos:

A. Inventario de sistemas y dispositivos.

Se debe mantener el inventario de todos los dispositivos conectados a la red y se debe evitar que los dispositivos no autorizados o no incluidos en el inventario se conecten a la red. Todos los dispositivos conectados a la red deben ser monitoreados, si se requiere un nuevo sistema, a su vez debe estar aislada la red corporativa. El conocimiento de los sistemas conectados a la red corporativa constituye la base de la gestión y el monitoreo.

B. Inventario de software y aplicaciones.

Se debe mantener un inventario de todo el software y las aplicaciones utilizadas en la organización, se debe evitar la instalación y el uso de software o aplicaciones no aprobados. El conocimiento del software

y las aplicaciones utilizadas en la red corporativa proporcionará la base para que los administradores del sistema estén informados sobre la existencia de vulnerabilidades en la seguridad.

C. Configuración segura del software

Todos los dispositivos y software utilizados en la organización deben configurarse de manera segura y garantizar los cambios controlados. La configuración segura, en otras palabras, es el ajuste que elimina las debilidades potenciales del hardware y software, reduciendo los puntos donde estos puedan ser atacados.

D. Gestión de vulnerabilidades de seguridad

Las brechas de seguridad existentes en los sistemas de cierta institución deben ser monitoreados y administrados continuamente. Los fabricantes implementan parches y actualizaciones de seguridad que deben cubrir nuevas aperturas y corrección de errores. Las actualizaciones de seguridad y parches oportunos desactivan muchas vulnerabilidades que los atacantes pueden explotar.

III. Conclusiones

Este artículo describe las tecnologías básicas de la industria 4.0 y proporciona las precauciones y recomendaciones necesarias para posibles ciberataques de acuerdo con sus estructuras arquitectónicas.

Existen diversos métodos y recomendaciones en la literatura; en este estudio, se presentan los requisitos de seguridad necesarios. Dado que esta área es muy amplia y diversa, es imposible limitar los problemas y proporcionar soluciones definitivas. Siempre habrá soluciones alternativas contra los ciberataques que se desarrollen en paralelo con la tecnología. Para estudios futuros, se podría planear hacer una aplicación que investigue las tecnologías de aprendizaje automático utilizadas para la detección de ataques cibernéticos.

Referencia y Recursos Electrónicos

1. Lu Y. (**2017**). *Industry 4.0: A survey on technologies, applications and open research issuesJournal of Industrial Information Integration*6, pp. 1-10.

2. Vaidya S., Ambad P. y Bhosle S. (**2018**). *Industry 4.0–a glimpseProcedia Manufacturing*20, pp. 233-238.

3. Muhuri P. K., Shukla A. K., Abraham A. (**2019**). *Industry 4.0: A bibliometric analysis and detailed overviewEngineering Applications of Artificial Intelligence*78, pp. 218-235.

4. Alcácer V., Cruz-Machado V. (**2019**). *Scanning the Industry 4.0: A Literature Review on Technologies for Manufacturing SystemsEngineering Science and Technology*an International Journal.

5. Chhetri S. R., Rashid N., Faezi S. y Al Faruque M. A. (**2017**). *Security trends and advances in manufacturing systems in the era of industry 4.0In 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*IEEE, pp. 1039-1046.

6. Xu L. D., Xu E. L., Li L. (**2018**). *Industry 4.0: state of the art and future trendsInternational Journal of Production Research* 56(8), pp. 2941-2962, 2018.

7. Ervural B.C., Ervural B. (**2018**). *Overview of cybersecurity in the industry 4.0 Era. In: Industry 4.0Managing The Digital Transformation*Springer, Cham. pp. 267-284.

8. Weber R. H., Studer E. (**2016**). *Cybersecurity in the Internet of Things: Legal aspectsComputer Law & Security Review*32(5), pp. 715-728.

9. Anton S. D. D., Strufe M., Schotten H. D. (**2019**). *Modern Problems Require Modern Solutions: Hybrid Concepts for Industrial Intrusion Detection*

10. Lezzi M., Lazoi M., Corallo A. (**2018**). *Cybersecurity for Industry 4.0 in the current literature: A reference frameworkComputers in Industry*103, pp. 97-110.

11. Alaba F. A., Othman M., Hashem I. A. T., Alotaibi F. (**2018**). *Internet of Things security: A surveyJournal of Network and Computer Applications*88, pp.10-28.

12. Lu Y., Da Xu L. (**2018**). *Internet of Things (IoT) cybersecurity research: a review of current research topicsIEEE Internet of Things Journal.*

13. Flatt H., Schriegel S., Jasperneite J.,. Trsek H, & Adamczyk H. (**2016**). *Analysis of the Cyber-Security of industry 4.0 technologies based on RAMI 4.0 and identification of requirementsIn 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*IEEE, pp. 1-4, September.