Ciberseguridad en la Robótica Industrial

Raúl Soria González

***Resumen*—En este trabajo voy a hablar sobre los posibles riesgos que pueden surgir en la robótica industrial centrándome en el ámbito de la ciberseguridad.**

Es un área que no se ha tenido muy en cuenta en estos años dentro de al robótica industrial pero que ahora y sobretodo en el futuro, va a tener una gran importancia debido al gran desarrollo de las nuevas tecnologías y a la Revolución Industrial 4.0.

Los robots en general y los robots industriales en concreto cada vez están tomando una mayor importancia en nuestro día a día y en los procesos de producción industriales. Se calcula que en 2025 habrá un robot por cada trabajador industrial.

Con el avance de las tecnologías y un mundo cada vez más conectado, los robots industriales también evolucionan y ahora están conectados entre ellos y con el exterior a través de Internet. Esto abre nuevas vulnerabilidades a posibles ciberataques de los cuales es importante tener conocimiento y saber cómo prevenirlos.

I. Introducción

Tal y como nos explica el Instituto Nacional de Ciberseguridad en su página [7] dedicada a la ciberseguridad de la robótica industrial, la robótica industrial constituye uno de los eslabones más importantes en el sistema industrial y está expuesta a posibles ciberataques que podrían tener consecuencias fatales.

I-A. En la actualidad

A lo largo de los últimos años la robótica industrial ha tenido una grandísima importancia que sigue aumentando a día de hoy. En muchas actividades industriales, los robots han pasado a sustituir a los humanos a la hora de realizar trabajos, principalmente aquellos que requieren de tareas muy repetitivas que podían incluso terminar siendo actividades de riesgo para el trabajador [3].

Hasta día de hoy, la industria sólo se ha fijado y preocupado en los riesgos físicos que supone la robótica pero no se ha preocupado ni se ha tenido en consideración el riesgo que suponen los ciberataques.

El motivo principal de la poca importancia que se le ha dado a la ciberseguridad en la robótica es que aún no se ha registrado ningún ciberataque "importante" a un robot industrial. Esto no significa que no pueda ocurrir, y de ser el caso, podría provocar grandes pérdidas ya que la robótica hoy en día es un eslabón clave en el proceso industrial. Si un ciberataque afecta a un robot industrial, se produciría un parón en toda la cadena produción.

Tras realizar diversos estudios, se ha llegado a la conclusión de que se puede piratear de manera muy sencilla casi cualquier robot industrial, poniendo en peligro no sólo a la producción de la empresa sino también a los trabajadores que realizan su labor conjuntamente con uno de estos robots.

I-B. En un futuro

Hoy en día se está produciendo la llamada Cuarta Revolución Industrial o Industria 4.0 [6]. Ese es el nombre que se le da a una hipotética cuarta etapa de la evolución técnico-económica de la humanidad. Se prevee que irá desarrollándose hasta llegar a su auge en la tercera década del siglo XXI.

Esta revolución industrial va a cambiar la manera de organizar los medios de produción, poniendo en marcha un gran número de lo que llaman *"Fábricas Inteligentes"*, capaces de adaptarse mejor a los procesos de produción y consiguiendo una asignación más eficiente de los recursos.

La robótica actualmente está creciendo en todos los ámbitos de la vida cotidiana y en la industria cada vez toma un papel más importante. En la Industria 4.0, la robótica se está convirtiendo en una parte fundamental de nuestro ecosistema.

La Cuarta Revolución Industrial se apoya en bases tecnológicas como la Inteligencia Artificial, el Internet de las Cosas (IoT), la *"Cultura maker"* y los Sistemas ciberfísicos [11]. Estos últimos hacen referencia a un mecanismo (sistema físico) que está controlado por algún algoritmo y conectado a Internet.

Así es como se supone que evolucionará la robótica, acercándose cada vez más a Internet, siendo así cada vez más vulnerable a posibles ciberataques. Es por eso que aunque actualmente no se haya registrado ningún ciberataque a un robot industrial, esto no significa que no pueda pasar hoy en día, pero desde luego podemos afirmar con seguridad que si la robótica industrial evoluciona acercándose cada vez más a Internet, en un futuro cercano la ciberseguridad será un aspecto a tener muy en cuenta en la robótica industrial.

II. Puntos débiles de los robots

En la industria robótica encontramos numerosos problemas en cuanto a la ciberseguridad. La mayoría debido a la poca importancia que se le da a la seguridad informática de los robots.

II-A. Sistema Operativo

Uno de los puntos más débiles que encontramos en los robots industriales es el Sistema Operativo Robótico, conocido por sus siglas en inglés como ROS.

Tal y como explica Óscar Lage , experto en ciberseguridad de Tecnalia [5], este sistema operativo ROS surgió como una investigación de la Universidad de Stanford en 2007 para así mejorar los protocólos de comunicación, pero en ningún momento se pensó en la ciberseguridad del mismo ya que no era la finalidad del proyecto. El problema está en que las grandes productoras han adoptado ese sistema operativo para sus robots y casi ninguna empresa publica ningún tipo de actualización de seguridad para sus robots.

En 2016 al fin comenzaron a desarrollar la seguridad de la robótica con la segunda versión del sistema operativo, ROS2. El problema es que casi ninguna máquina lo tiene instalado, mantienen ROS y por consiguiente mantienen brechas en la seguridad del robot.

II-B. Estándar

O más bien, carencia de estándar, ya que aún no hay ningún tipo de estándar internacional que regule de ninguna forma los requisitos que debe cumplir un robot industrial en cuanto a ciberseguridad.

En la actualidad lo máximo a lo que se puede aspirar a la hora de comprar un robot industrial es a tener alguna opción para configurar la seguridad nosotros mismos una vez recibamos los robots.

El motivo al que achacan esta situación las marcas es la interoperabilidad con robots más antiguos, es decir que, supuestamente, si introducen caracteristicas de ciberseguridad a los nuevos robots utilizando nuevos lenguajes, es posible que estos nuevos robots no puedan comunicarse con los más antiguos.

Es cierto que la Unión Europea cada vez está más implicada con la digitalización y ha comenzado a tomar en serio el tema de la ciberseguridad. La Comisión Europea pedía en una recomendación [9] que desde Bruselas se comenzara a legislar para poder garantizar mejor protección a los usuarios y mayor seguridad jurídica.

Algunos gobiernos nacionales dentro de la Unión Europea como Reino Unido, Alemania y Francia también han dado algunos pasos en dirección de mejorar la situación de la robótica, aunque parecen ser insuficientes.

III. Vulnerabilidades de un robot ante un ciberataque

Endika Gil-Uriate, consejero delegado de Alias Robotics, afirma que la robótica en la actualidad es tan vulnerable como lo eran los PC a finales de los 80 o los 90 [8]. Esto se debe principalmente a que los robots tienen una gran componente software que se encarga de diversas funciones que puede desarrollar el robot. Y como casi todo software, es vulnerable a ciberataques.

Un ciberataque puede afectar de diversas formas a un robot industrial debido a que hay muchas partes del robot que se controlan mediante software. Algunos de los puntos que los ataques pueden comprometer son los siguientes:

- *Parametros del controlador*: El atacante puede modificar los parámetros que el robot tiene en su controlador, haciendo que el robot se comportamiento de manera inesperada.
- *Parametros de calibración*: Si el ataque modifica los parámetros de calibración del robot, esto hará que los movimientos del robot pierdan pecisión y no cumpla correctamente su función.
- *Comunicación*: El ataque puede interferir en la comunicación del robot con otros robots de su cadena de producción o incluso en la comunicación que realiza con el operador (humano) enviándole información incorrecta sobre su funcionamiento.
- *Control del robot*: El atacante también puede atacar al estado del robot manipulando el mismo y haciendo que el operador pierda el control del robot.

IV. Posibles problemas causados por ciberataques

Cuando un robot industrial es atacado, se pueden producir diversos problemas. Cada ciberataque puede tener una intención distinta y tener un móvil concreto pero lo que todos tienen en común es que son muy perjudiciales para la cadena de producción y la empresa afectada.

- *Sabotaje de la producción*: El atacante introduce cambios ínfimos e indetectables en el comportamiento del robot para que el producto final tenga alguna imperfección y funcione mal.
- *Daño físico*: El atacante puede tener intención de cambiar el comportamiento del robot haciendo que este destroce partes de la cadena de producción o incluso produzca daño físico a los trabajadores.
- *Ransomware*: Trata de lanzar un ataque a un robot industrial para pedir un rescate, si la empresa se niega, el atacante activaría el virus produciendo una parada en la producción.

Está claro que cualquier ciberataque que se produzca tendrá graves consecuencias. Por ello es importante conocer estos ataques para así poder prevenirlos.

V. Prevención de ciberataques

Los principales motivos por los que se abren brechas de seguridad en los robots industriales es por algún error de software desactualizado. Esto puede suceder o bien porque el sistema operativo no cuente con seguridad, como pasa con ROS, o porque las bibliotecas o el sistema no se encuentren en su última versión.

Desde la página dedicada a la ciberseguridad de la robótica industrial de INCIBE [7] nos explican que un diseño seguro debe incluir el ciclo completo del desarrollo, desde requerimientos, selección, arquitectura e implementación hasta, las operaciones en marcha.

Tabién nos proponen algunos puntos sobre cómo debemos abordar estos desafíos de seguridad:

- *Gobierno*
  - Establecer estructuras con roles y responsabilidades bien definidas.
  - Gestión de las amenazas identificadas a través de un programa de gestión de riesgos.
- *Seguridad del software*
  - Análisis de seguridad periódicos en los robots para identificar posibles fallos.
  - Utilizar testeo dinámico o fuzzing para escanear los bots creados para la detección de vulnerabilidades.
  - Revisiones para comprobar que los controles de seguridad de la autentificación y autorización funcionan correctamente.

- *Identidad y acceso digital*
  - Implantar el uso obligatorio de contraseñas de inicio de sesiones robóticas.
  - Centralizar la identidad y acceso robóticos para la gestión de los mismos.
  - Gestión de privilegios de acceso de los usuarios para conseguir que los bots realicen solo las tareas que se les han asignado, impidiendo así operaciones no autorizadas.
- *Protección de los datos*
  - Evaluaciones de cumplimiento de las regulaciones de los datos para así controlar la confidencialidad de estos.
  - Monitorización de datos sensibles para controlar el cumplimiento de las políticas de uso.
- *Operaciones de seguridad*
  - Realizar auditorías del rastreo de acctividades a partir del log del controlador del robot, pudiendo así encontrar anomalías.
  - Escanear vulnerabilidades de la plataforma robótica que se utilice y encontrar brechas de seguridad mediante ejercicios de modelado de amenazas.
  - Implementar un cortafuegos físico en los robots que permita analizar constantemente las ordenes que recibe el robot para así autorizarlas o denegarlas consultando con otro equipo que contenga todas las reglas que tiene que cumplir el robot.
- *Gestión de vulnerabilidades*
  - Estar al tanto de las vulnerabilidades que publica el fabricante para comprobar si nuestros robots están afectados y poder solucionar dichas vulnerabilidades.
  - Aplicar una política donde se explique cómo actualizar o cambiar las configuraciones de los robots.
- *Seguridad en las comunicaciones*
  - Utilización de protocolos de comunicación cifrados para mantener la confidencialidad e integridad de los mensajes.
  - Implementar *end-points* para detectar posibles infecciones.
  - Recolección de datos del robot para una posterior auditoría de red y así poder encontrar vulnerabilidades tanto en los sistemas robóticos como en las conexiones pudiendo así redefinir la arquitectura de red industrial y hacerla más segura.

Un gran problema es que muchos fabricantes de robots se desentienden de los aspectos relacionados con la protección contra ciberataques. Esto es aglo que muchos expertos como Gil-Uriate afirman que cambiará en poco tiempo, y que la seguridad en la robótica industrial y en la robótica en general llegará a ser más relevante que la de tecnologías de la información ya que en la robótica existen riesgos físicos detrás de los ciberataques [8].

Gil-Uriate también opina que no debemos dejar que los ataques a robots sean demasiado comunes antes de tomar acciones al respecto, por ello es importante la prevención de los mismos.

Una de las soluciones que propone para poder prevenir estos ataques es un *'antivirus'* para robots industriales. Es lo que propone la startup española en la que trabaja, Alias Robotics.

VI. Alias Robotics

Alias Robotics es una startup española fundada en 2018 y dedicada a ofrecer soluciones de ciberseguridad para robots industriales. Tienen en su plantilla especialistas en robótica, software, biología e inteligencia artificial para conseguir entre todos un sistema robótico seguro.

Según explican en su página web [14], la próxima generación de robots estarán conectados unos con otros y/o con Internet y eso conlleva grandes ventajas pero también grandes riesgos en cuanto a la ciberseguridad. Por eso la meta de Alias Robotics es proteger los robots de los clientes y sus componentes contra ataques de terceros. Dicen que la seguridad no es una meta o un producto sino un proceso.

El principal objetivo de la empresa es la creación de un *'Sistema Inmunológico para Robots'*, al que han llamado *RIS* (Robot Immune System).

VI-A. RIS

RIS pretende ser la solución a la ciberseguridad en los robots, un sistema que protege a los robots conectados, como comenta su CEO en una entrevista [1] "RIS funciona en paralelo a la aplicación robótica, sin generar complejidades añadidas, como un antivirus".

Es un sistema que, haciendo uso de técnicas de inteligencia artificial, es capaz de detectar y bloquear culaquier amenaza gracias a una monitorización activa y en tiempo real. Es un antivirus inteligente que vive dentro del robot.

Según comenta Alias Robotics en su página sobre el RIS [10], este se integra con el Robot Operating System "ROS" (tanto en su primera como en su segunda versión), integránose con el kernel del sistema operativo ofreciendo así integridad, confidencialidad, disponibilidad y sobretodo seguridad.

Según comenta su propio CEO, consiguen inmunizar a los robots a través de un software con arquitectura modular, este tiene un firewall específico para cada robot, lo que se traduce en una protección reforzada que está conectada a bases de datos que contienen amenazas ya detectadas. Con esto el RIS puede identificar una vulnerabilidad en un robot comparándola con las que dispone en las base de datos y pudiendo así poner una solución rápida y eficazmente.

RIS se adapta y aprende de cada despliegue robótico, recopilando información que pueda servir de utilidad en otro robot similar. El sistema ya está funcionando en más de 46 modelos distintos de robots, aquellos que son más usados en la industria.

VI-B. Black Box

Aunque el producto estrella de Alias Robotics sea el RIS también cuentan con otros productos. Uno de ellos es la llamada "Black Box" [2].

Black Box es como su nombre indica, una caja negra que se encarga de registrar varios meses (o incluso años) de todo

lo que realiza el robot, permitiendo así un análisis forense del mismo para así poder localizar ciberataques en la red o un mal funcionamiento del robot.

VI-C. Colaboración con Telefónica

Telefónica, una de las mayores compañías de telecomunicaciones, firmó en 2020 un acuerdo [13] con Alias Robotics con el objetivo de liderar el mercado de la ciberseguridad robótica.

El acuerdo entre ambas empresas incluye una inversión de Telefónica a través de su vehículo de inversión en startups de ciberseguridad, Telefónica Tech Ventures. Esto hace que la operadora tome una participación minoritaria en la compañía de ciberseguridad robótica.

Este acuerdo, además de para llevar el RIS al siguiente nivel y servirlo a más usuarios aún,también servirá para crear el primer laboratorio de ciberseguridad robótica del mundo.

VI-C1. Laboratorio de ciberseguridad robótica: Ese laboratorio con sede en Munich, Alemania, es pionero en el ámbito de la ciberseguridad en la robótica industrial [12]. Actuará como centro neurálgico de la tecnología, desde donde Alias Robotics podrá seguir proponiendo sus soluciones contra los cibercriminales.

El laboratorio también servirá como punto de encuentro de diferentes stakeholders interesados en saber cómo hay que proteger a los robots industriales eliminando sus puntos débiles. Además, el laboratorio servirá para que distintas empresas de la ciberseguridad y la robótica puedan trabajar conjuntamente proponiendo así nuevas souciones y realizando investigaciones conjuntas. Es el caso de Alias Robotics que podrá trabajar con ElevenPaths, otra empresa que pertenece a Telefónica Tech Ventures y ofrece diversas soluciones en ciberseguridad.

VII. Conclusiones

La ciberseguridad no se ha tenido demasiado en cuenta en la robótica industrial debido a que no era algo demasiado importante y tan sólo suponía un coste extra a tener en cuenta. Pero con la Industria 4.0 y el avance de las tecnologías, el auge del *IOT* y la cada vez mayor interconexión de todo con internet (incluidos los robots industriales), la ciberseguridad de estos se está convirtiendo cada vez en algo más a tener en cuenta.

Según muchos expertos la ciberseguridad en la robótica industrial es incluso más importante que en las TIC, ya que los robots industriales tienen una componente física que suele ser grande y pesada y en caso de descontrolarse uno de estos gigantes podría tener consecuencias fatales para los trabajadores de una fábrica.

Muchas empresas y gobiernos de todo el mundo se preocupan cada vez más por el tema aunque está siendo un proceso lento y aún hay muchos robots industriales que son vulnerables a este tipo de ataques.

Gracias a avances como los vistos por parte de Alias Robotics con su *RIS* o a los consejos de instituciones como INCIBE, cada vez los responsables de fábricas industriales y robots son más conscientes del peligro que suponen estos ataques y tienen acceso a herramientas y estrategias para evitarlos.

Referencias

[1] *Así es el 'antivirus' para robots industriales desarrollado por la española Alias Robotics*. URL: https://www.elespanol.com/invertia/disruptores-innovadores/disruptores/startups/20210310/antivirus-robots-industriales-desarrollado-espanola-alias-robotics/564444434_0.html (visitado 12-05-2021).

[2] *BlackBox, forensics for robots*. URL: https://www.aliasrobotics.com/blackbox.php (visitado 14-05-2021).

[3] *Ciberseguridad en la robótica industrial en 2018*. URL: https://netcloudengineering.com/ciberseguridad-robotica-industrial/ (visitado 12-05-2021).

[4] *Cultura maker*. En: *Wikipedia, la enciclopedia libre*. Page Version ID: 135430978. 10 de mayo de 2021. URL: https://es.wikipedia.org/w/index.php?title=Cultura_maker&oldid=135430978 (visitado 11-05-2021).

[5] Jorge G. García. «Los robots menosprecian la ciberseguridad». En: *El País* (30 de jun. de 2020). ISSN: 1134-6582. URL: https://elpais.com/retina/2020/06/30/tendencias/1593496452_756769.html (visitado 11-05-2021).

[6] *Industria 4.0*. En: *Wikipedia, la enciclopedia libre*. Page Version ID: 135284376. 4 de mayo de 2021. URL: https://es.wikipedia.org/w/index.php?title=Industria_4.0&oldid=135284376 (visitado 10-05-2021).

[7] *Los ciberdesafíos de la seguridad en la robótica industrial | INCIBE-CERT*. URL: https://www.incibe-cert.es/blog/los-ciberdesafios-seguridad-robotica-industrial (visitado 06-05-2021).

[8] *Los robots, vulnerables a los ciberataques*. URL: https://www.expansion.com/economia-digital/innovacion/2021/02/10/601bdd83468aeb65168b45f9.html (visitado 12-05-2021).

[9] Mariya Gabriel y Angelika Niebler. «Hacia un proyecto común de ciberseguridad en Europa». En: *El País* (16 de oct. de 2018). ISSN: 1134-6582. URL: https://elpais.com/retina/2018/10/15/tendencias/1539606790_424115.html (visitado 11-05-2021).

[10] *RIS, Robot Immune System*. URL: https://www.aliasrobotics.com/ris.php (visitado 14-05-2021).

[11] *Sistema ciberfísico*. En: *Wikipedia, la enciclopedia libre*. Page Version ID: 131287586. 28 de nov. de 2020. URL: https://es.wikipedia.org/w/index.php?title=Sistema_ciberf%C3%ADsico&oldid=131287586 (visitado 11-05-2021).

[12] *Telefónica invierte en Alias Robotics y ambas abrirán un laboratorio de ciberseguridad robótica en Alemania | Compañías | Cinco Días*. URL: https://cincodias.elpais.com/cincodias/2020/12/14/companias/1607938810_380153.html (visitado 14-05-2021).

[13] *Telefónica y Alias Robotics se alían para liderar la robótica cibersegura | Detalle | Noticias | Sala de Prensa | Telefónica*. URL: https://www.telefonica.com/es/web/sala-de-prensa/-/telefonica-y-alias-robotics-se-alian-para-liderar-la-robotica-cibersegura (visitado 13-05-2021).

[14] *We are Alias Robotics*. URL: https://www.aliasrobotics.com/about.php (visitado 13-05-2021).