

5G e Industria 4.0

Retos y oportunidades de la cuarta
revolución industrial

Sobre ON5G

El Observatorio Nacional 5G (ON5G) es una iniciativa público-privada impulsada por Mobile World Capital Barcelona, la Secretaría de Estado para el Avance Digital y Red.es con el objetivo de analizar el ecosistema 5G en España e identificar a sus principales actores, así como las iniciativas en desarrollo a nivel nacional e internacional. El ON5G comparte conocimiento a través de informes, mejores prácticas y eventos, todo ello para avanzar en la creación e impulso del ecosistema 5G en España.

An initiative of



red.es

Índice

1 Introducción a la Industria 4.0	6
Modelo de las cuatro revoluciones industriales	7
Tecnologías habilitadoras de la Industria 4.0	10
Internet de las cosas y sistemas ciberfísicos	12
La inteligencia artificial	13
El gemelo digital	14
Casos de uso en la Industria 4.0	16
Caso de uso 1: la fábrica flexible basada en AGV	17
Caso de uso 2: control de calidad inteligente	18
2 La Industria 4.0, digital y conectada	20
Marco básico para la Industria 4.0: RAMI 4.0 e IIRA	21
Introducción a las comunicaciones industriales	25
Interconexión de sistemas OT (operaciones)	26
Interconexión de sistemas IT (sistemas de información)	28
Sistemas de comunicación inalámbricos	29
Introducción a los sistemas de comunicación inalámbricos	29
Sistemas de comunicación inalámbricos basados	32
en bandas de uso común (sin licencia de uso)	
Sistemas de comunicación inalámbricos basados	35
en bandas de uso privativo (con licencia de uso)	
3 La tecnología 5G	38
¿Qué ofrece la tecnología 5G?	40
¿Cómo se hace esto en 5G?	42
La transición del 4G al 5G: despliegues SA y NSA	43
La red de acceso	43
La red principal (core network)	44
Tipos de despliegue de la red 5G	46
Ciberseguridad en la Industria 4.0 y 5G	48
Introducción a la ciberseguridad en la Industria 4.0	48
Panorama de amenazas para la Industria 4.0	49
Enfoque de ciberseguridad para la Industria 4.0	51
Seguridad de las comunicaciones 5G	52
4 Aplicaciones representativas de 5G en el ámbito industrial	54
La fábrica flexible basada en AGV	55
Control de calidad inteligente	58
Conclusiones	60
Glosario	62

1

Introducción a la Industria 4.0

5G: una tecnología transformadora

La industria está viviendo un proceso profundamente transformador en este siglo XXI. Un proceso de digitalización e irrupción de nuevas tecnologías que prometen dirigir una nueva revolución industrial: la **cuarta revolución industrial**. Uno de los pilares de esta revolución es la conectividad ubicua de las máquinas. Sin embargo, las tecnologías de comunicación inalámbricas disponibles hoy en día no cubren todas sus necesidades: gran capacidad de transmisión de datos, elevado número de dispositivos conectados simultáneamente y fiabilidad en las comunicaciones. Es aquí donde la tecnología 5G va a suponer un avance significativo, facilitando el acceso ubicuo y habilitando nuevos modelos de uso y de negocio.

Teniendo en cuenta esto, en esta primera sección del documento se introducen las motivaciones y las tecnologías habilitadoras clave para esta nueva revolución industrial. Además, se presentan ejemplos representativos de casos de uso habilitados por la Industria 4.0.

Modelo de las cuatro revoluciones industriales

En el año 2013, la ACATECH (academia alemana de las ciencias) formuló el modelo de progreso industrial basado en cuatro revoluciones industriales. Este modelo ha dado lugar al término Industria 4.0.¹ En concreto, el documento «Recommendations for implementing the strategic initiative INDUSTRIE 4.0»² se puede considerar como el libro blanco de la Industria 4.0 alemana, y fue presentado en la edición de la Feria de Hannover de 2013 y entregado a la canciller Angela Merkel por representantes de la academia y la industria alemana.

¹ En el año 2011, el DFKI (centro alemán de inteligencia artificial) presentó un modelo diferente basado en una sola revolución industrial dividida en cuatro etapas.

² «Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Final report of the Industrie 4.0 Working Group», Academia Nacional de Ciencias e Ingeniería (ACATECH), abril de 2013.

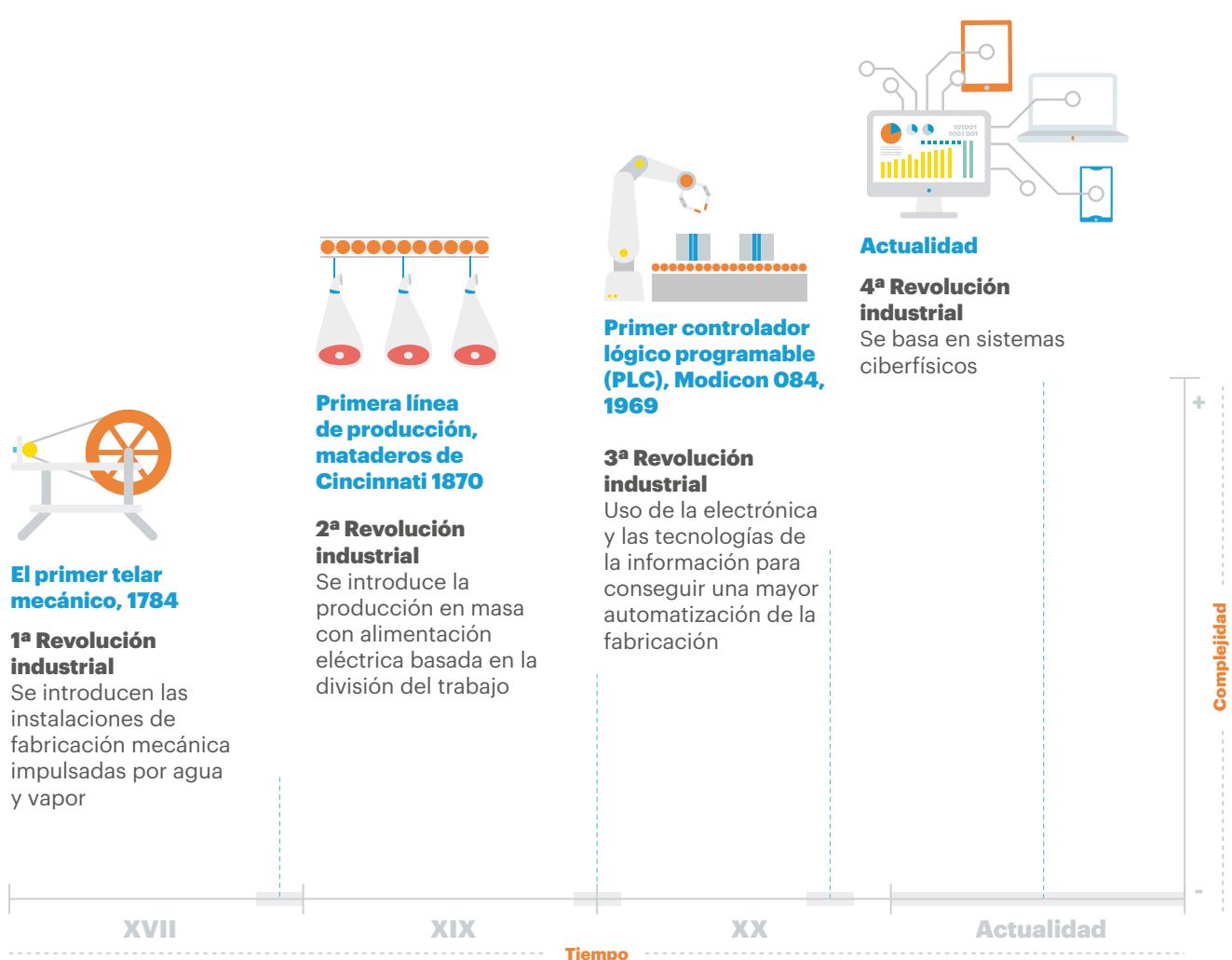


Figura 1. Las cuatro etapas de la revolución industrial.

Según este modelo de cuatro revoluciones industriales, ilustrado en la Figura 1, la invención del telar mecánico y la introducción de la máquina de vapor en el ámbito de la fabricación, a mediados del siglo XIX, dio lugar a la **primera revolución industrial**. Posteriormente, la introducción de la electricidad como fuerza motriz y la producción basada en la división del trabajo, junto con el desarrollo de las telecomunicaciones analógicas, dieron lugar, a principios del siglo XX, a la **segunda revolución industrial**. Los sistemas de producción en masa no automatizados alcanzaron su máximo apogeo a finales de los años cincuenta e inicios de los sesenta. Por último, la introducción de la electrónica digital en los sistemas de control industrial dio lugar a la **tercera revolución industrial**. Esta ha evolucionado con la adopción de la informática y la llegada de Internet y la telefonía móvil. En esta etapa, se ha materializado un aumento drástico de la productividad de los procesos industriales a gran escala. Esto ha sido posible gracias, entre otros motivos, a la introducción de la automatización y de la robótica, permitiendo un mayor grado de personalización de los productos. Esencialmente, la segunda revolución industrial fue de carácter analógico, mientras que la tercera fue de carácter digital.

La **cuarta revolución industrial** está motivada por la presión de un mercado global, de competencia sin fronteras, y por la necesidad de responder a una creciente demanda de flexibilidad, personalización y bajos precios por parte del mercado. A su vez, esta cuarta revolución es posible gracias al avance de la tecnología —su mayor capacidad de procesado, menor precio, menor consumo energético y miniaturización— que permite dar respuesta a las necesidades impuestas por el mercado, cumpliendo con los criterios de viabilidad técnica y económica.

La cuarta revolución industrial se puede interpretar como el resultado de la unión entre el mundo analógico y el mundo digital. Esta inminente cuarta revolución se fundamenta en la integración entre los mundos de la tecnología de operaciones (del inglés, *Operative Technologies*, OT) y las tecnologías de la información (del inglés, *Information Technologies*, IT), lo que da lugar a la denominada **convergencia IT/OT**. De esta unión emergen los denominados sistemas ciberfísicos, capaces de conectar el mundo digital con el mundo físico y habilitar lo que se conoce como la digitalización integral de la industria. Esta integración, además, se ve potenciada por la posibilidad de interconectar a las personas y los objetos en un mundo ciberfísico; en este ámbito, las tecnologías de comunicación, como es el caso de la tecnología 5G, juegan un papel fundamental, como veremos más adelante.

Esta integración IT/OT permite alcanzar la flexibilidad necesaria para responder a la demanda de adaptación, bajo coste y personalización de los mercados en relación a los productos, pero presenta el gran desafío de superar las históricas diferentes percepciones del tiempo y del riesgo entre los colectivos de IT y de OT. Para hacer efectiva esta convergencia, se precisan profesionales con perfil híbrido, que actúen con transversalidad en equipos interdisciplinares. Mediante esta integración IT/OT, y a través de la hiperconectividad entre personas y objetos, es posible disponer de información de la oferta en tiempo real, y canalizar la demanda de forma muy desintermediada. El cliente puede canalizar la información de la demanda, de sus deseos y necesidades, a través de, por ejemplo, aplicaciones software conectadas en tiempo real, que permiten ofrecer información asociada a todas las fases del ciclo de vida del producto: desde el diseño, el desarrollo, la producción, la logística de entrega, la puesta en marcha y el servicio posventa, hasta la retirada final. Todo ello, además, con circularidad.

Tecnologías habilitadoras de la Industria 4.0

Las tecnologías habilitadoras de la Industria 4.0 son aquellas que se incorporan a los productos y los procesos productivos para dotarlos de la flexibilidad, personalización y bajos precios que demanda el mercado. Actualmente existen diferentes modelos que agrupan estas tecnologías en categorías según diferentes criterios; por ejemplo, su ámbito de aplicación o su tipología.

Uno de los modelos más utilizados es el propuesto por el Boston Consulting Group (BCG), que se muestra en la Figura 2. Como se observa, este modelo identifica 9 tecnologías transformadoras de la Industria 4.0, agrupadas en 3 grupos: medios de producción, inteligencia y, finalmente, datos y conectividad. En el primer grupo, correspondiente a los medios de producción, se encuentra la robótica avanzada y la fabricación aditiva, también denominada impresión 3D. En el segundo grupo, denominado de inteligencia, se incluye la realidad aumentada, la simulación y la integración de sistemas. Finalmente, en el tercer grupo, correspondiente a datos y conectividad, se contemplan el Internet de las cosas, el cloud, el big data y la ciberseguridad.



Figura 2. Modelo de 9 tecnologías transformadoras del BCG.

Si bien esta propuesta de clasificación de las tecnologías habilitadoras de la Industria 4.0 resulta interesante, no tiene en cuenta todas las tecnologías disponibles ni tiene en cuenta las diferentes agrupaciones de las mismas para dar solución a una problemática concreta. Por ejemplo, el concepto Internet de las cosas rara vez estará desvinculado de los conceptos de *cloud computing* y en muchos casos del *big data*, pues los datos que generan los dispositivos se tienen que almacenar y procesar. Del mismo modo, la inteligencia artificial asume que existe una base de datos con gran cantidad de información que permite entrenar modelos matemáticos para realizar predicciones sobre el funcionamiento de un sistema.

Teniendo en cuenta esto, en los siguientes subapartados se explica la evolución y estado actual de los conceptos *Internet de las cosas* y *Sistemas ciberfísicos*, *Inteligencia artificial* y *Gemelo digital* en el marco de la Industria 4.0.



Internet de las cosas y sistemas ciberfísicos

Alrededor del año 1999 emerge el concepto Internet de las cosas (del inglés, *Internet of Things*, IoT). Un grupo de estudiantes de la Carnegie Mellon University, en EE. UU., desarrolló un sistema de monitorización remota, a través de Internet, para medir la temperatura y realizar un control de stock en una máquina de refrescos. El objetivo era poder decidir si desplazarse hasta la máquina de bebidas o no, en función de la disponibilidad y temperatura de las bebidas. La idea de poder conocer, a través de un sistema digital y a distancia —a través de Internet—, magnitudes físicas relacionadas con el mundo material, despertó un gran interés.

Posteriormente, alrededor del año 2006, se acuñó el término *sistema ciberfísico* (del inglés, *Cyber-Physical System*, CPS) en la NSF (en inglés, National Science Foundation) en EE. UU. Se definió como la integración de la computación, en el ámbito digital, cibernético, con los procesos físicos del mundo material. Podríamos decir que lo que se desarrolló para la máquina de refrescos de la Carnegie Mellon University fue un primer sistema ciberfísico para la monitorización de stock de bebidas.

Más recientemente, en 2013, Sabina Jeschke, de la Universidad de Aachen, propuso la definición de una capa (representada como una franja vertical) ciberfísica entre los mundos físico y digital, tal y como se muestra en la Figura 3. El diagrama se compone de una capa física, otra ciberfísica y una tercera capa digital, así como de los elementos clave que las componen y relacionan entre sí.

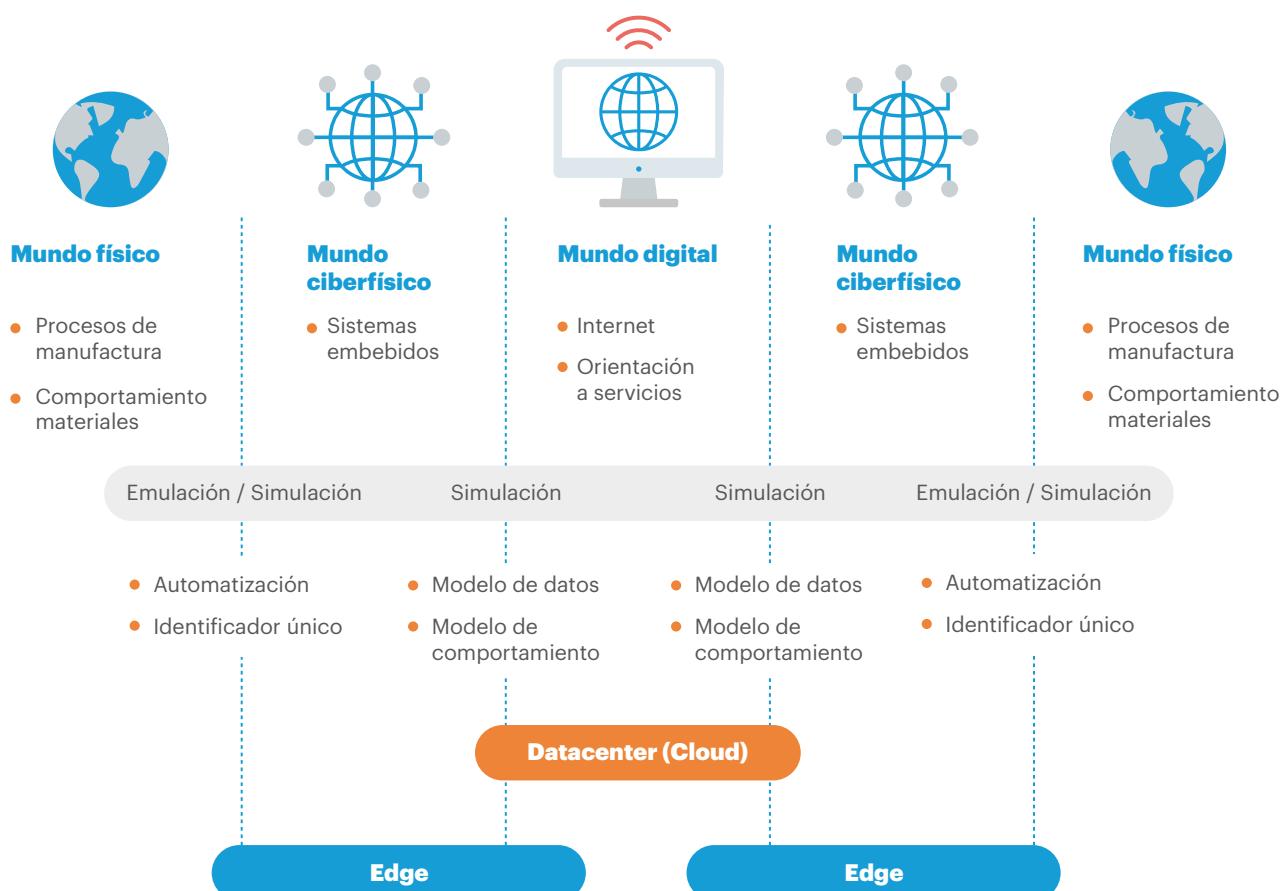


Figura 3. Elementos de los sistemas ciberfísicos.

A izquierda y derecha de la Figura 3, en los extremos, está el mundo físico, que se caracteriza por el comportamiento físico de los materiales y por los procesos de fabricación. A través de los sistemas embebidos electrónicos, equipados con sensores y actuadores, se conecta el mundo físico con el mundo digital. Los bloques del diagrama pueden leerse de la siguiente manera: la comunicación del mundo físico y del mundo ciberfísico se basa en la emulación/simulación (traslado de objetos del mundo físico al mundo digital) y en la automatización (mediante el control de objetos del mundo físico a través de objetos digitales), y para ello es necesario poder identificar únicamente los objetos físicos (mediante códigos ópticos, radiofrecuencia, etc.) y mapearlos con objetos de software. En el mundo digital, toda interacción se puede orientar a servicios, pudiendo almacenar información e intercambiarla a través de redes de comunicaciones, tales como Internet, y procesar datos para la toma de decisiones o, simplemente, para su visualización. Para ello, la comunicación entre el mundo ciberfísico y el mundo digital se realiza mediante los modelos de datos y los modelos de comportamiento, que son los dos pilares fundamentales de la ingeniería del software.

Es interesante resaltar que en la Figura 3 se muestran e introducen los términos *edge* (extremo) y *cloud* (la nube). El término *edge* hace referencia a un extremo de la red en el que los elementos conectados están próximos a la frontera con el mundo físico; pudiéndose definir esta proximidad tanto en distancia geográfica como en distancia temporal para el intercambio de datos. El *edge* está compuesto por sistemas con una pequeña distancia temporal entre ellos y el mundo físico, que ofrece prestaciones (en inglés, *capabilities*) en lo relativo a la velocidad de respuesta y fiabilidad. Por otra parte, el *cloud* hace referencia a los elementos de la red más alejados del mundo físico, en la frontera con los centros de proceso y almacenamiento de datos, conocidos en inglés como *data centers*, los cuales ofrecen grandes capacidades de almacenamiento y de cálculo, además de ser un punto global de encuentro de información gracias a Internet.

La inteligencia artificial

Uno de los elementos fundamentales para el desarrollo de la Industria 4.0 es la inteligencia artificial. Este concepto incluye una gran variedad de técnicas y mecanismos, de entre los que destaca el aprendizaje automático (en inglés, *machine learning*), que suele basarse en redes neuronales que tratan de imitar el comportamiento de los sistemas nerviosos biológicos. Estas redes pueden entenderse como una gigantesca matriz que relaciona entradas con salidas, de modo que, a medida que se introduce información, esta va almacenando (aprendiendo) las nuevas combinaciones, respetando las relaciones entrada/salida aprendidas en el pasado.

En la Figura 4 se muestra un sistema de IoT combinado con un sistema de aprendizaje automático. Por una parte, están las «cosas conectadas» que, bajo la visión de la Industria 4.0 se constituyen mediante sistemas ciberfísicos. Estos se comunican a través de redes inalámbricas con los sistemas de aprendizaje automático, los cuales necesitan ser previamente entrenados. Para ello, hay que conseguir conjuntos de datos que se puedan usar a modo de entrenamiento. Estos conjuntos de datos pueden suponer grandes volúmenes de información como, por ejemplo, secuencias de vídeo, audio o todo tipo de señales registradas. Estos datos se tienen que trasladar a los sistemas de entrenamiento de las redes

neuronales, los cuales, para obtener tiempos de entrenamiento reducidos, pueden requerir potentes procesadores y grandes volúmenes de memoria durante un corto espacio de tiempo. Para ello, los sistemas de *cloud* flexible, que se configuran en caliente bajo demanda, ofrecen la posibilidad de pagar el uso de estos recursos solo durante el tiempo de utilización del mismo, medido con una resolución de fracciones de segundo. Una vez entrenadas, las redes neuronales pueden operar procesando las entradas y las salidas en tiempo real con sistemas de computación de bajas prestaciones, los cuales pueden ejecutarse en el *edge*.

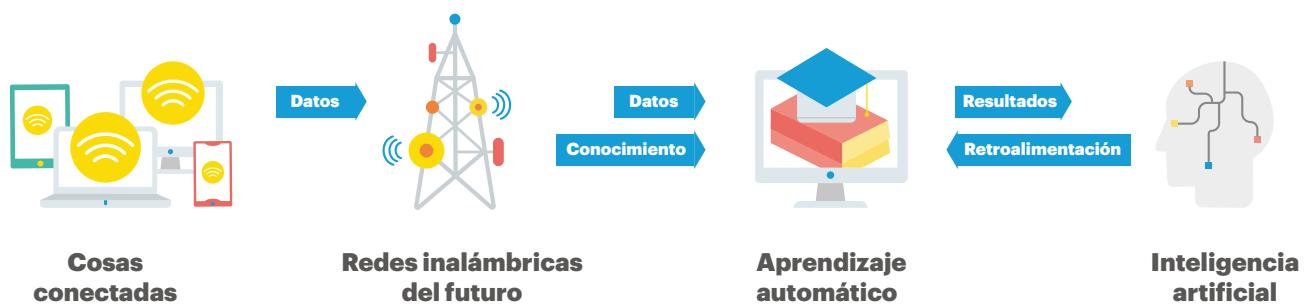


Figura 4. Escenario de aprendizaje automático para aplicaciones industriales.

Para realizar el proceso de aprendizaje y predicción es necesario recabar datos de muchos dispositivos distribuidos por la fábrica en tiempo real y hacerlos llegar a los sistemas de inteligencia artificial en el *edge* o en el *cloud* para llevar a cabo la predicción de los fallos, permitiendo adoptar medidas correctivas antes de que ocurran. Es decir, con la aplicación de estas tecnologías, ya no será necesario esperar a que una máquina falle por error de una pieza para repararla, sino que sería posible reponer una pieza que está a punto de fallar, antes de que el error suceda. Esta anticipación permite reducir el tiempo de parada y, por lo tanto, los gastos derivados de ella.

Por tanto, en vista de la gran cantidad de dispositivos a conectar y la posibilidad de que estos sean móviles, se trata de una tarea que se ve favorecida gracias al uso de sistemas de comunicación inalámbricos debido a la ubicuidad y facilidad de despliegue de los mismos.

El gemelo digital

Otro de los conceptos emergentes importantes para la Industria 4.0 es el gemelo digital (en inglés, *Digital Twin*). La noción de *gemelo digital* fue introducida por Michael Grieves en 2003, y se aplicó por primera vez en la NASA (en inglés, *National Aeronautics and Space Administration*). Según el Fraunhofer Institut IPK, el gemelo digital se define como la representación digital de un activo tangible o intangible que comprende sus propiedades, condición y comportamiento mediante modelos y datos.

Conceptualmente, el gemelo digital ha sufrido cuatro evoluciones principales a lo largo de su corta vida. En la primera etapa, se limitaba a modelos de CAD/CAM (en inglés, *Computer Aided Design / Computer Aided Manufacturing*), donde el modelo digital era una simple representación del modelo físico. Este es el caso de los planos de CAD de oficina técnica.

Posteriormente, con el aumento de las capacidades de computación, se amplió su funcionalidad con modelos de simulación, lo que permite validar los desarrollos antes de su implementación física. Este sería el caso de los modelos de simulación por elementos finitos realizados a partir de los planos de CAD.

En una tercera etapa, se incorporaron los datos provenientes del Internet de las cosas, lo que permite contrastar las predicciones de los modelos de simulación con los datos reales capturados por sensores. Finalmente, en la última etapa de su evolución, se ha añadido la inteligencia artificial que, además de validar los datos de simulación con los datos reales, también permite realizar predicciones y llevar a cabo la toma de decisiones de manera automatizada.

Según el modelo de *Digital Twin* del Fraunhofer Institut IPK, el *Digital Twin* se basa en dos conceptos: el *Digital Master* (DM) y el *Digital Shadow* (DS). Por un lado, el DM está constituido por los artefactos digitales (software y datos) necesarios y suficientes para poder crear activos tangibles o intangibles. Esta idea va más allá de una especificación técnica, y podría considerarse como una especificación ejecutable cuyo resultado es la materialización (parte física del activo) y la instanciación (parte digital del activo) de objetos a partir los modelos digitales del DM. Por otra parte, el DS, o sombra digital, está constituido por los datos recogidos a lo largo del tiempo. Dependiendo del número de sensores, su tipología y la frecuencia de muestreo, los volúmenes de datos pueden ser enormes, dando lugar al denominado *big data*, que se pueden gestionar en *data centers*, los cuales ofrecen soluciones tecnológicas flexibles y escalables para su almacenamiento y procesado.

Los gemelos digitales validados permiten la experimentación y el desarrollo de los elementos que se integrarán en un futuro con otros activos del mundo real, sin la necesidad de tener que esperar a que estos existan previamente en el mundo real. Ello permite drásticas reducciones en los tiempos de desarrollo e integración debido a la capacidad de paralelizar tareas de ingeniería con garantías de integración sin fisuras.

Para poder llevar a cabo el diseño e implementación de *digital twins*, así como la interacción entre el mundo digital y el mundo físico, es necesario contar con una tecnología de comunicaciones que permita un intercambio de grandes cantidades de datos (por ejemplo, de vídeo) en tiempo real, y un tiempo de respuesta muy pequeño para habilitar operaciones también en tiempo real. Este es el rol de las tecnologías de comunicaciones inalámbricas de nueva generación.

La inteligencia artificial se ha incorporado al digital twin en su última evolución y puede aplicarse con diversas finalidades. La inteligencia artificial, por ejemplo, se puede usar para reproducir el comportamiento de los activos reales en un entorno simulado. Por otra parte, los *digital twins* pueden ser una fuente de datos utilizables para el entrenamiento de sistemas inteligentes.



Casos de uso en la Industria 4.0

Se pueden consultar casos de uso y pruebas piloto de 5G para la industria en la página web de la iniciativa impulsada por la Mobile World Capital y otras entidades denominada «5G Barcelona» en <https://5gbarcelona.org/es/casos-de-uso>, indicando, en «Filtrar por», la opción «Industria».

El informe «**5G Unlocks A World of Opportunities. Top ten 5G Use Cases**»³ publicado por Huawei en 2017 identifica diez casos de uso para la fabricación inteligente (en inglés, *smart manufacturing*), la cual constituye un área principal de la Industria 4.0.

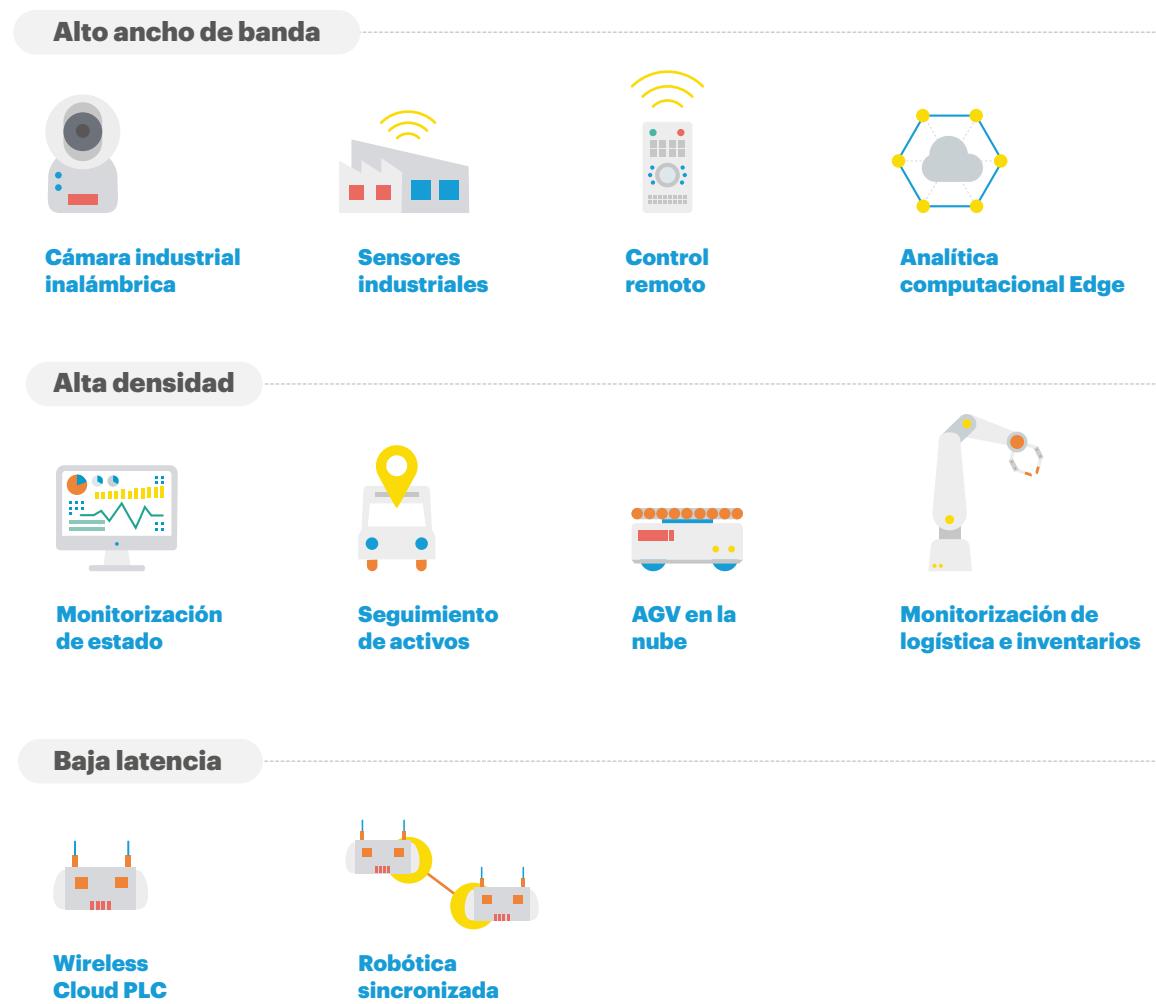


Figura 5. Tipologías de casos de uso en la Industria 4.0.

³ «A World of Opportunities. Top ten 5G Use Cases», Huawei (2017)

<https://www.huawei.com/en/industry-insights/outlook/mobile-broadband/insights-reports/5g-unlocks-a-world-of-opportunities>

Como vemos en la Figura 5, estas aplicaciones industriales se pueden clasificar según el ancho de banda, la densidad de dispositivos y la latencia en la comunicación. En primer lugar, encontramos las aplicaciones que requieren un gran ancho de banda, tales como sensores industriales que transmiten grandes volúmenes de información, como cámaras, o sistemas de monitorización y control remoto. En segundo lugar, encontramos aplicaciones que requieren una gran densidad de dispositivos, como sería el caso de la monitorización de la condición de activos, la gestión de flotas de vehículos autoguiados (del inglés, AGV, Auto Guided Vehicles) y el monitoreo de la logística y los inventarios. Finalmente, encontramos las aplicaciones que requieren de comunicaciones en tiempo real estricto, como los PLC (del inglés, Programmable Logic Controllers) para la automatización y la robótica sincronizada.

Teniendo en cuenta esto, a continuación se introducen dos casos de uso para la Industria 4.0, motivando la necesidad de una nueva generación de comunicaciones móviles que permita satisfacer los diversos requisitos impuestos por los diferentes casos de uso.

Caso de uso 1: La fábrica flexible basada en AGV

Como hemos mencionado antes, hoy en día la industria debe responder a una demanda que exige cada vez mayor grado de personalización. Para ello, las fábricas deben ofrecer un elevado grado de flexibilidad, permitiendo romper el paradigma de la línea de montaje establecida durante la segunda revolución industrial, para pasar a un concepto más modular en el que diferentes células de proceso pueden cambiar de posición y configuración, y entre las cuales existen medios de interconexión.

Una de las tecnologías habilitadoras para este tipo de diseño flexible son los AGV. Estos vehículos pueden transportar materiales, herramientas, productos u objetos de cualquier tipo entre células de producción, permitiendo un elevado grado de automatización en el proceso de fabricación con la consiguiente mejora de la eficiencia de los procesos. Todo ello, además, conlleva una reducción de costes. Un ejemplo de este tipo de configuración se muestra en la Figura 6.

La operativa y gestión de estos AGV, y, en particular, si se trata de un número elevado de ellos que deben funcionar simultáneamente, requiere del uso de una tecnología de comunicaciones de nueva generación que haga posible la comunicación permanente con vehículos para permitir una óptima operativa en los entornos de fabricación. La prestación característica indicada de este caso de uso es la alta densidad, pero puede también requerir un ancho de banda elevado en el caso de que los AGV vayan equipados con cámaras de vídeo, y también puede requerir comunicaciones con baja latencia para poder responder en tiempo real a las necesidades de cada situación posible. Pruebas realizadas para la sustitución de largas líneas de montaje por células flexibles conectadas con AGV han constatado la necesidad del 5G, puesto que la tecnología Wifi se muestra insuficiente para ello, afirma Henning Löser, responsable del Production Lab de Audi.⁴

⁴ <https://enterpriseiotinsights.com/20190508/internet-of-things/two-visions-of-5g-factories>

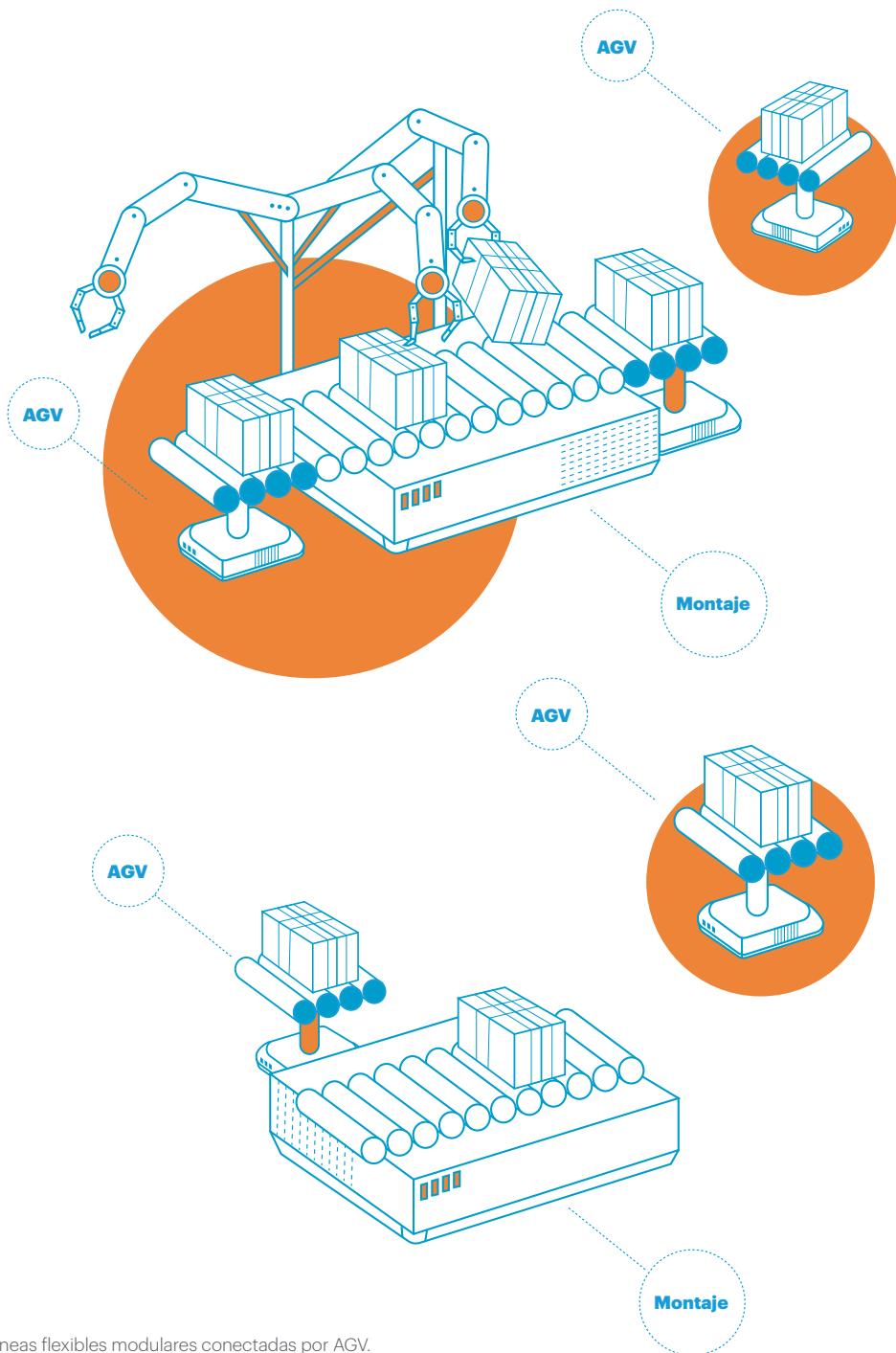


Figura 6. Líneas flexibles modulares conectadas por AGV.

Caso de uso 2: Control de calidad inteligente

El control de calidad constituye una de las tareas fundamentales en cualquier planta de fabricación. La detección anticipada de errores o defectos permite dibujar un escenario libre de averías en los sistemas productivos. Asimismo, estos defectos pueden generar un efecto «bola de nieve» y acabar derivando en series de productos defectuosos que pueden llegar a generar grandes costos económicos, así como posibles retrasos en la entrega de productos acabados.

Podemos distinguir entre tres tipos de control de calidad propios del ámbito de la manufactura: 1) control de calidad del producto, 2) control de calidad del proceso de fabricación y 3) control de calidad del mantenimiento.

En cuanto al producto, la denominada visión artificial es una de las técnicas emergentes que permite automatizar el control de calidad en base a la observación y análisis mediante la aplicación de algoritmos de procesado de imagen. Además, estos sistemas permiten cumplir otras funciones relevantes como pueden ser el posicionamiento de robots móviles en contextos inciertos.

El control de calidad del proceso de fabricación se puede realizar con las técnicas de APC (del inglés, *Advanced Process Control*) y el SPC (del inglés, *Statistical Process Control*). En APC se realizan simulaciones previas y predicciones a las reconfiguraciones de los sistemas de producción debidas a los cambios en la demanda, y se pueden implementar a partir de DM. En SPC se realiza un control estadístico permanente sobre las variables y parámetros durante los procesos productivos en base a los datos obtenidos mediante la IoT, los cuales forman parte de los DS. Por lo tanto, la visión de la Industria 4.0 contempla la posibilidad de realizar controles de calidad de manera automatizada o muy asistida.

El control de calidad del mantenimiento tiene por objetivo eliminar las roturas, averías y reparaciones inoportunas que puedan conllevar costes de todo tipo. La idea es anticiparse a las averías y eliminar su efecto actuando con anticipación sin interferir en la dinámica productiva. Para ello se pueden aplicar técnicas de mantenimiento predictivo, basándose, por ejemplo, en el monitoreo de la condición de los activos, pudiéndose utilizar para el pronóstico modelos analíticos o modelos basados en redes neuronales.

Además del control de calidad en la manufactura, es necesario también implementar un control de calidad de la asistencia de campo y de la formación. Tecnologías como la realidad aumentada o la realidad virtual permiten facilitar acciones de reparación asistida o bien la mejora de los procesos de aprendizaje. Por ejemplo, un técnico de soporte podría recibir, en tiempo real y sobreimpresionadas sobre una maquinaria real, las instrucciones para reparar un fallo de operación. Esto repercutirá en una reducción del tiempo de aprendizaje por parte de los operarios, así como en una reducción del tiempo de reparación de errores. Este tipo de superposición de la realidad con imágenes digitales se muestra en la Figura 7.

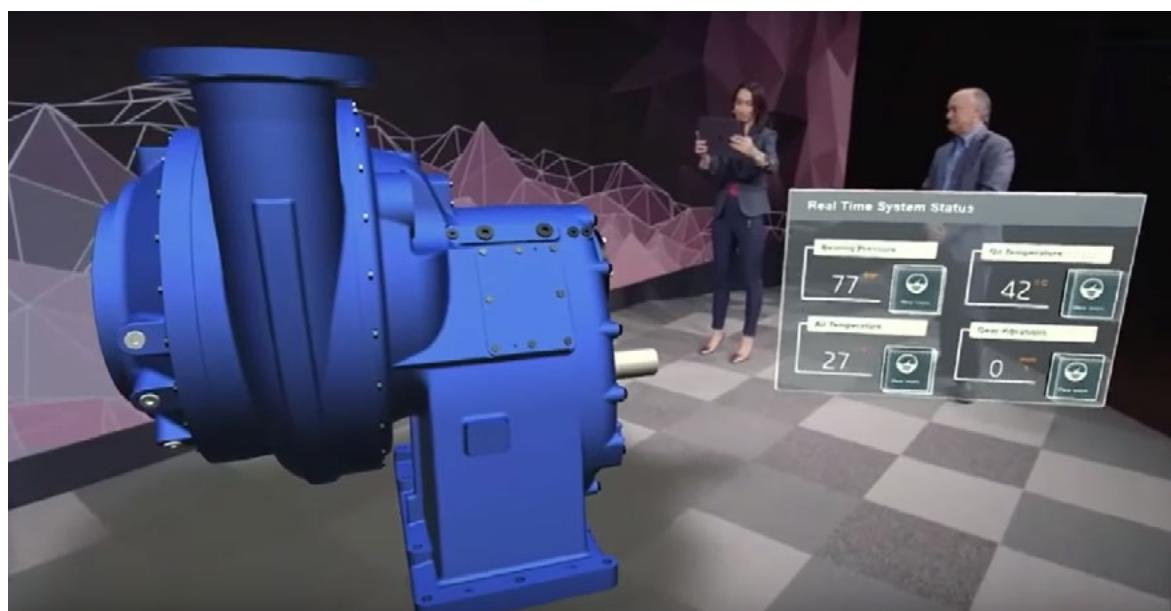


Figura 7. Ejemplo de gemelo digital con realidad virtual.

2

La Industria 4.0, digital y conectada

Marco básico para la Industria 4.0: RAMI 4.0 e IIRA

Existen varios modelos teóricos que definen la arquitectura del concepto de Industria 4.0. De entre los modelos existentes, se pueden destacar dos: la arquitectura de referencia RAMI 4.0 (del inglés, *Reference Architecture Model Industry 4.0*) y la arquitectura IIRA (del inglés, *Industrial Internet Reference Architecture*).

La arquitectura de referencia RAMI 4.0 está definida por la Industrie 4.0 Platform, consorcio de origen alemán para la Industria 4.0. A su vez, la arquitectura IIRA está definida por el Industrial Internet Consortium (IIC), consorcio de origen norteamericano constituido para impulsar la Internet Industrial de las Cosas (IIoT, del inglés, *Industrial Internet of Things*). Por lo tanto, podemos decir que RAMI 4.0 proviene del mundo de las operaciones (OT) e IIRA proviene del mundo de las tecnologías de la información y las comunicaciones (IT).

Por un lado, RAMI define un proceso de digitalización de activos consistente en cubrir, metafóricamente, cada uno de los activos físicos con una «campana digital» (en inglés, *Administration Shell*). Todo flujo de información, tanto de datos como de control, entre el activo y su entorno pasa por dicha campana. La unión lógica de cada activo con su campana digital se define como componente 4.0 (del inglés, *Industry 4.0 Component*). Gráficamente, se representa tal y como se muestra en la Figura 8. Como vemos en la figura, la granularidad de un componente 4.0 puede ir desde una simple válvula a una máquina, pero también podría cubrir una factoría o una organización completa.

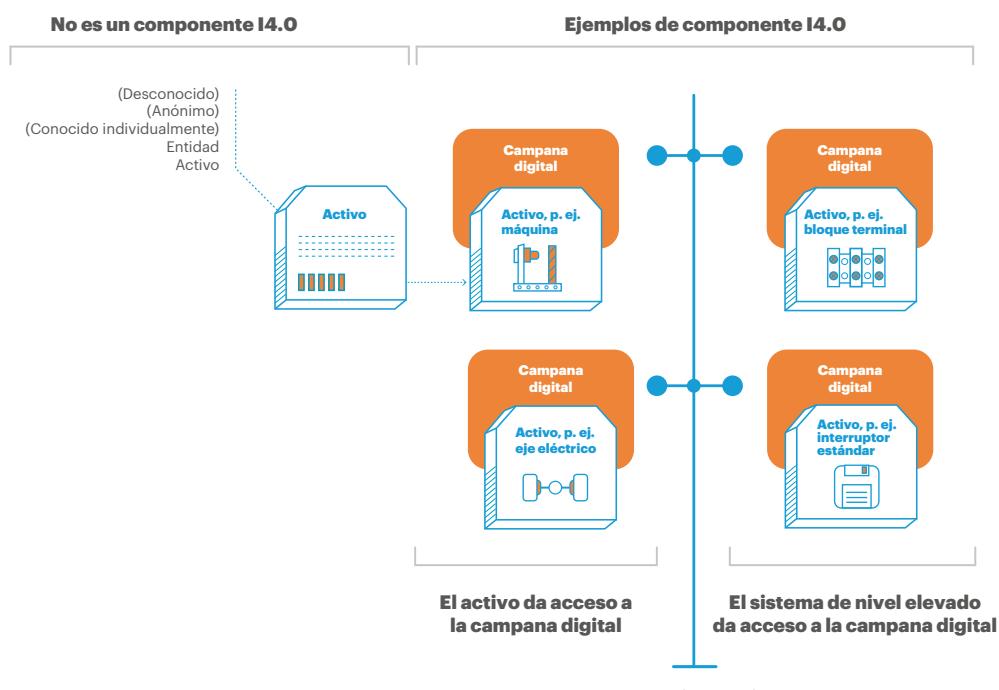


Figura 8. Componentes 4.0 según RAMI 4.0 (IEC PAS 63088).

Así pues, podemos definir un componente 4.0 como un elemento con capacidades de procesamiento y de comunicación en red; en términos informáticos, esta capacidad puede articularse a través de un acceso por terminal remoto, de una interfaz programable (del inglés, *Application Programmable Interface*, API) que provee servicios o mecanismos automatizados de publicación/subscripción de información, los cuales dan lugar a un enfoque emergente denominado PubSub (en inglés, *Publish/Subscribe*).

La relación entre los componentes de la Industria 4.0 y los *Digital Twins* ha sido establecida por el Fraunhofer Institut IOSB en el documento «visit [Industrial IoT - Digital Twin]». En la Figura 9 se muestra la relación entre un componente de la Industria 4.0 y su campana digital con la noción de gemelo digital en una arquitectura de tres capas. Entre la capa del mundo físico y los servicios se encuentra la capa de infraestructura, la cual corresponde a la capa de los sistemas ciberfísicos del modelo planteado en el apartado 1.2.

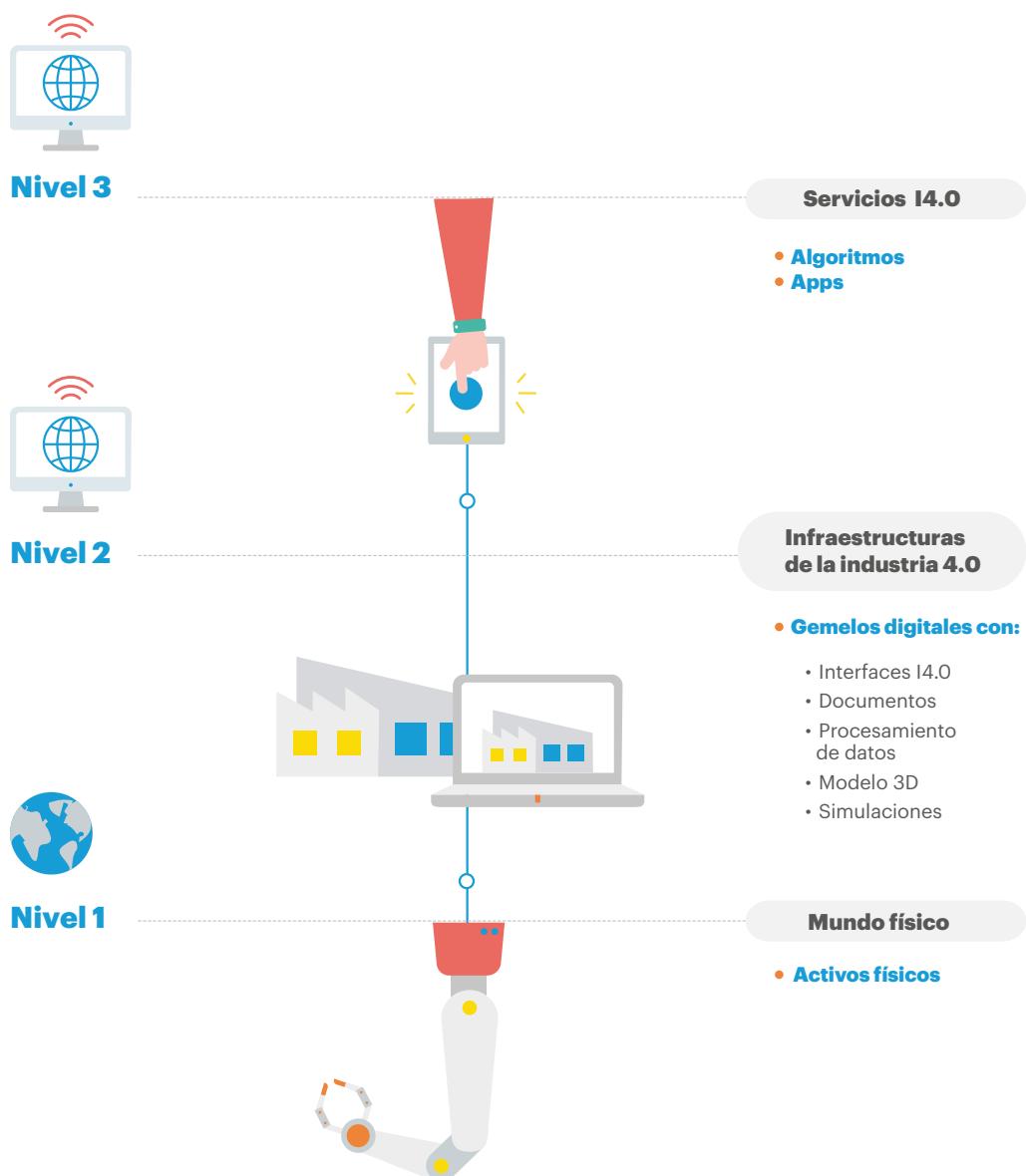


Figura 9. Componentes 4.0 y Digital Twin, entre el mundo real y los servicios.

A su vez, la arquitectura IIRA propone un modelo de la Internet Industrial de las Cosas (del inglés, *Industrial Internet of Things*, IIoT) compuesto por máquinas, computadoras y personas, y que es capaz de facilitar la realización de operaciones industriales inteligentes utilizando análisis de datos avanzados para resultados comerciales transformadores. La arquitectura IIRA define un *endpoint* como un componente con capacidades computacionales y de conectividad a la red de comunicaciones. Sería el equivalente al componente 4.0 del modelo RAMI 4.0.

Las equivalencias entre los modelos RAMI e IIRA se muestran en la Figura 10. Según la arquitectura IIRA, los sistemas edge están en la frontera entre las entidades física y digital delineadas por dispositivos IoT, y tienen la connotación de sistema cercano a lo físico, en contraposición a la noción de *cloud computing*, que se define como paradigma para habilitar mediante acceso a la red a recursos tanto físicos como digitales, escalables, elásticos y compatibles.

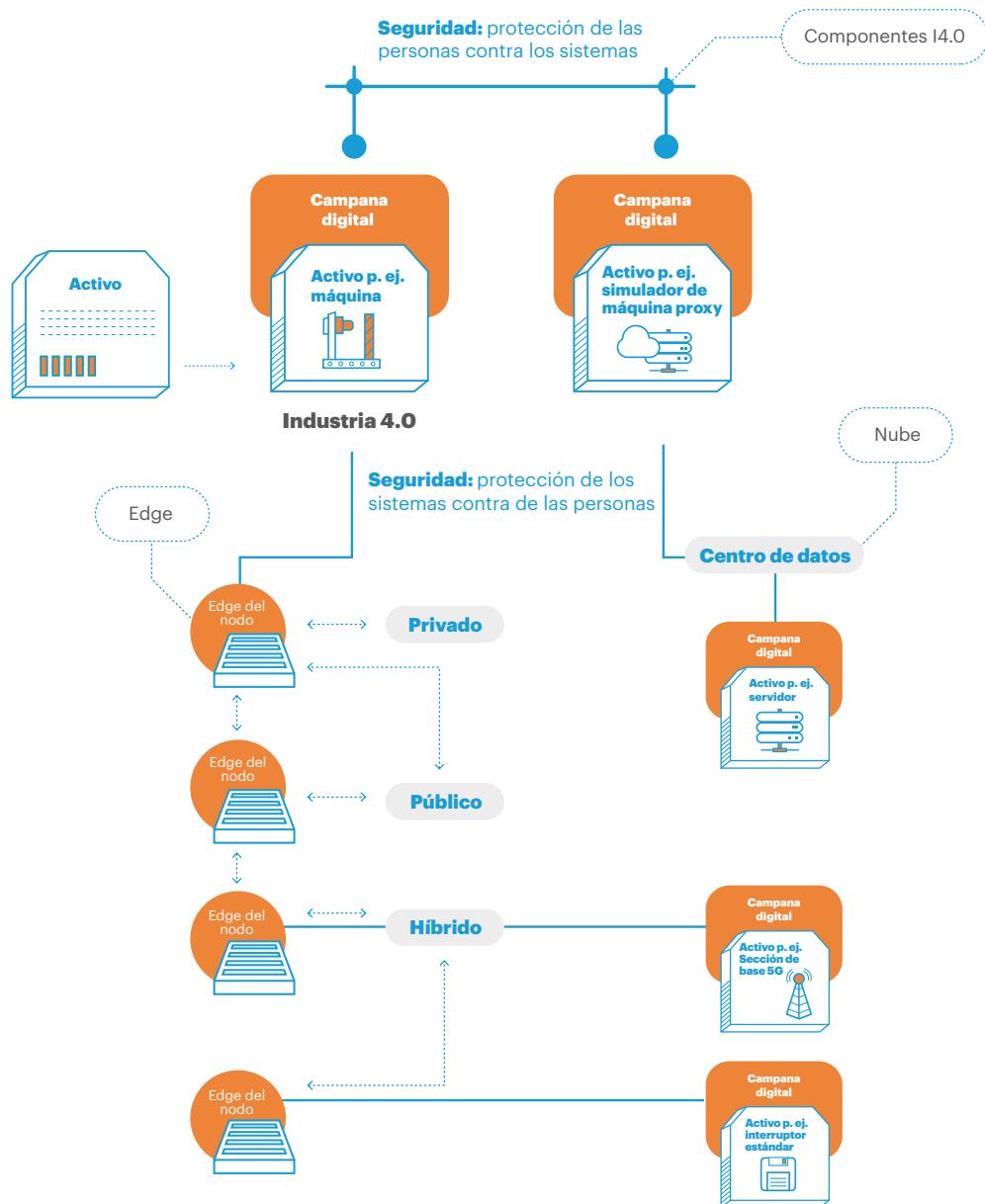


Figura 10. Visión integrada de RAMI 4.0 (IEC/PAS 63088) e IIRA: Componentes I4.0, Edge y Cloud.

Por su parte, los *endpoints* pueden tener la posibilidad de ser virtualizados dentro de otros *endpoints*, de forma que en un mismo equipamiento físico pueden funcionar aparentemente como varios *endpoints* independientes. La técnica utilizada para ello se denomina aislamiento, y las dos variantes emergentes actualmente son el aislamiento por contenedor (aislamiento débil pero muy flexible) y el aislamiento por máquina virtual (aislamiento fuerte con separación de *kernel*, es decir, aislamiento total del hardware subyacente),⁵ tal y como se ilustra en la Figura 11.

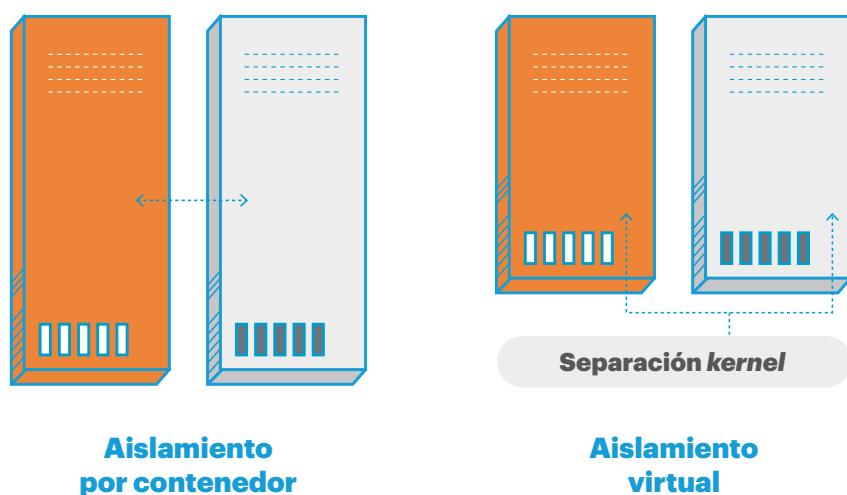


Figura 11. Aislamiento y virtualización de endpoints según IIRA.

Así pues, las comunicaciones industriales son el punto de partida para comunicar tanto los componentes 4.0 de RAMI como los *endpoints* de IIRA (de hecho, un componente 4.0 es un *endpoint*). Teniendo en cuenta esto, en la siguiente sección se describen las principales tecnologías de comunicaciones para entornos industriales desplegadas en la era precedente a la Industria 4.0.



⁵ Sistemas como VMWare o VirtualBox aislan por máquina virtual y, por otra parte, Docker aísula por contenedores

Introducción a las comunicaciones industriales

Como se ha descrito hasta ahora, uno de los pilares de la Industria 4.0 es la conectividad ubicua para permitir que los dispositivos intercambien información. Si bien la conectividad no es un requerimiento nuevo, la cantidad de datos a enviar y los requerimientos de tiempo real que se prevén en esta cuarta revolución industrial suponen un salto tanto cualitativo como cuantitativo respecto a revoluciones anteriores. Teniendo en cuenta esto, en esta sección se presenta una revisión de la evolución de los sistemas de comunicaciones y de gestión automática de procesos industriales.

En la Figura 12 se muestra el modelo de la ISA-95 (en inglés, *International Society of Automation*), donde se definen los diferentes niveles de operación de un proceso productivo (primera) y las tecnologías que se utilizan en cada uno de los niveles (segunda) según los requerimientos de comunicación (ancho de banda, latencia, determinismo, etc.).

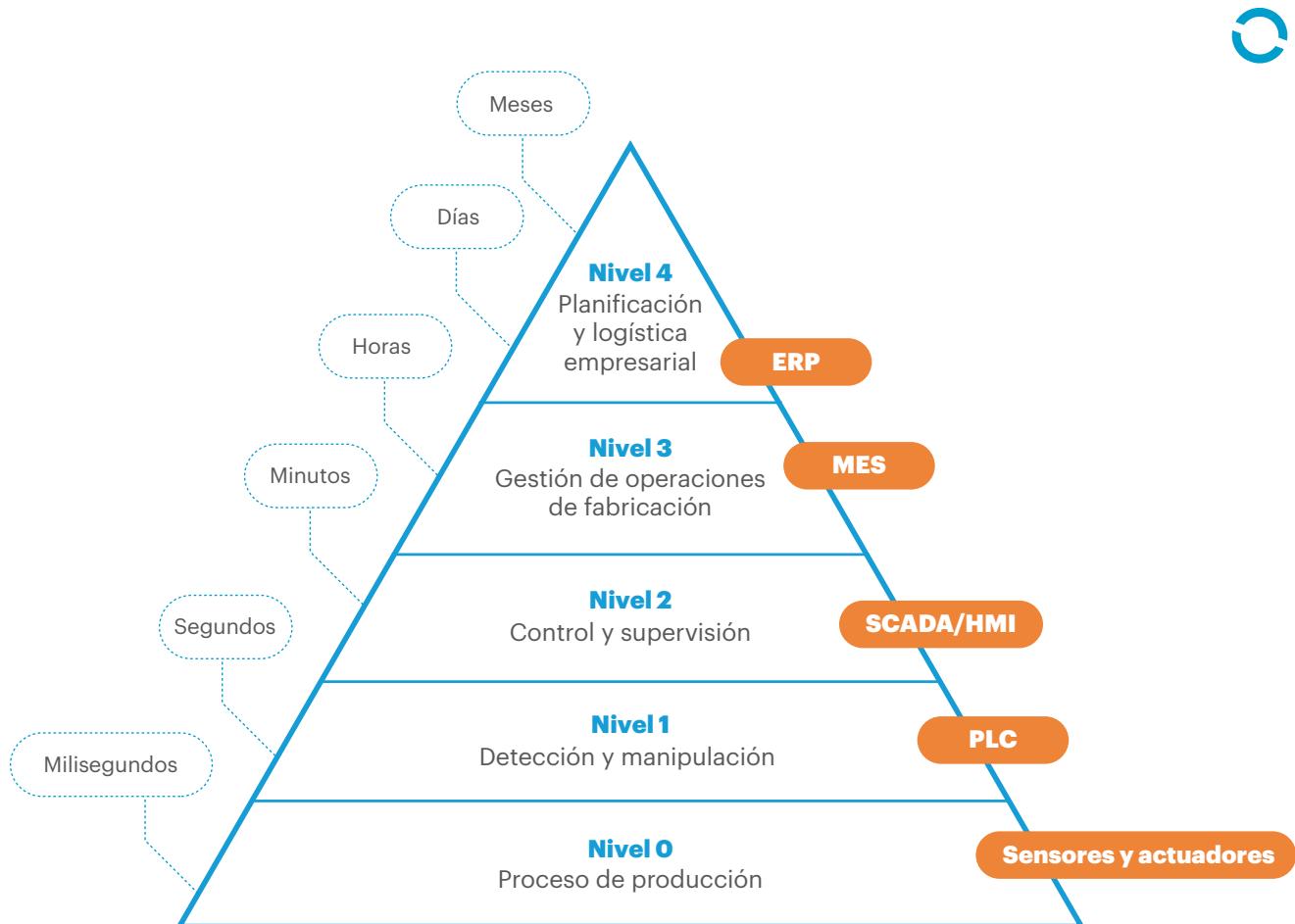


Figura 12.1 Modelo ISA-95.

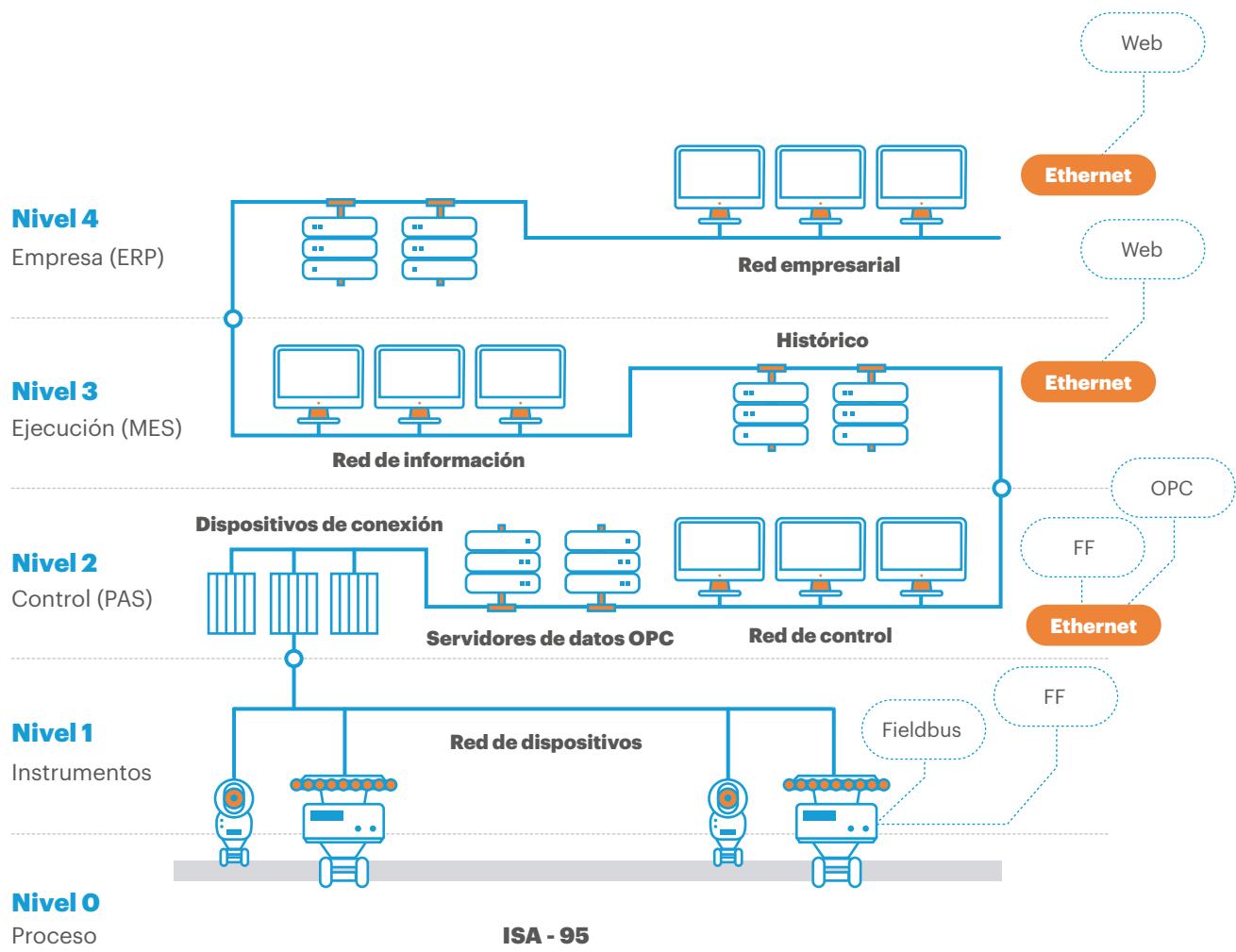


Figura 12.2 Mapeo con las tecnologías de comunicación industrial.

A continuación, se presenta una breve introducción a los sistemas de comunicación usados para la interconexión de sistemas OT, primero, e IT, después.

Interconexión de sistemas OT (operaciones)

Los niveles inferiores de la pirámide ISA-95 están soportados por los llamados buses de campo, estandarizados como IEC 61158 (en inglés, *International Electrotechnical Commission*). Estos buses de campo se utilizan para la interconexión de los diferentes elementos, típicamente PLC (en inglés, *Programmable Logic Controller*), que se encargan de monitorizar y controlar un proceso a tiempo real de una manera flexible, homogénea y escalable. Además, los PLC también conectan los datos del proceso con los niveles superiores de la pirámide, incluyendo los sistemas SCADA (del inglés, *Supervisory Control And Data Acquisition*) y los sistemas HMI (del inglés, *Human-Machine Interface*), que permiten la planificación del proceso y la supervisión del mismo por parte de los operadores humanos.

En general, los buses de campo permiten evitar las conexiones directas punto a punto y mejorar la sincronización de procesos en los que intervienen simultáneamente muchos equipamientos heterogéneos (incluyendo módulos de entrada y salida, servocontroladores, autómatas programables, estaciones de operación y control, sensores, actuadores y módulos de seguridad, etc.), así como aportar una cierta redundancia que mejora la fiabilidad de los procesos. Para su implementación existen varios tipos, entre los que cabe citar AS-i (en inglés, *Actuator Sensor Interface*), EPL (en inglés, *Ethernet Powerlink*), Modbus (en inglés, *Modicon Bus*) y Profibus (en inglés, *Process Field Bus*). A su vez, estos buses se basan en tecnologías de comunicación muy diversas, como pueden ser RS-485 y MBP (Modbus Plus, incluyendo sus versiones IS, que aumentan la seguridad para trabajar en zonas peligrosas; por ejemplo, donde existe riesgo de explosión) o Ethernet.

En cualquier caso, debido a que utilizan tecnologías punto a multipunto con protocolos de acceso al medio aleatorios, los buses de campo no permiten garantizar el ancho de banda ni tener un tiempo de comunicación determinista. Así pues, en los casos donde estos requerimientos son críticos, se opta por realizar una conexión dedicada punto a punto entre dos elementos. Si bien esto permite garantizar los requerimientos de ancho de banda y tiempo real, su uso limita en gran medida la escalabilidad y la ubicuidad de la solución, además de incrementar el coste de la misma.

En este sentido, recientemente han aparecido dos tecnologías que están revolucionando la interconexión de sistemas OT. Por un lado, el grupo de trabajo IEEE 802.1 (en inglés, *Institute of Electrical and Electronic Engineers*) está impulsando la iniciativa TSN (del inglés, *Time-Sensitive Networking*), consistente en un conjunto de estándares abiertos basados en Ethernet con prestaciones de tiempo real determinista. Por otro lado, la OPC Foundation está impulsando el protocolo OPC-UA (del inglés, *Open Platform Communications Unified Architecture*), un estándar abierto de comunicaciones industriales seguras basadas en la pila de protocolos de Internet (TCP/IP).

El interés por parte de la industria en estos protocolos radica en dos factores. En primer lugar, el carácter abierto de las especificaciones, de manera que estas no están ligadas a ningún fabricante concreto. En segundo lugar, las especificaciones cuentan con el apoyo oficial de un amplio número de fabricantes, cosa que garantiza la existencia de productos comerciales que los implementen. Además, ya existen testbeds conjuntos de ambas tecnologías, demostrando las ventajas de combinar la tecnología TSN con el protocolo OPC-UA para reemplazar los buses de campo actuales. Por tanto, estas tecnologías pueden suponer un paso definitivo de la denominada «guerra de los buses de campo», cuyo origen es la incompatibilidad entre los diversos sistemas ligados históricamente a fabricantes específicos.

Pero a pesar de sus ventajas, el uso de TSN sigue limitando la conectividad a equipos industriales que sean fijos. Por tanto, en la línea de la necesidad de flexibilidad de la Industria 4.0, existe un creciente interés por parte de la industria por introducir tecnologías de comunicación inalámbricas que doten los sistemas de movilidad. Pero como veremos más adelante, esta limitación no puede ser salvada con los sistemas de comunicación inalámbricos actuales, ya que estos no garantizan las prestaciones (ancho de banda, retraso, número de dispositivos, etc.) necesarias para las aplicaciones industriales. Por tanto, la tecnología 5G puede jugar un papel clave en el proceso de transformación digital de la industria, aportando comunicaciones ubicuas y movilidad a los sistemas, y garantizando unas comunicaciones con suficiente capacidad y determinismo.

Interconexión de sistemas IT (sistemas de información)

El hecho de no disponer de latencias acotadas en las comunicaciones no suele suponer un problema para los niveles 3 y superiores del modelo ISA-95, donde los procesos pasan de estar controlados por los responsables del ámbito OT (tecnologías operativas) a estar controlados por los responsables del ámbito IT (tecnologías de la información y las comunicaciones). En los niveles 3 y superiores, los tiempos de captura de información, análisis y respuesta están en una escala de tiempo muy superior a los utilizados en las comunicaciones en tiempo real y permiten usar un abanico de tecnologías más amplio. En estos niveles, el uso de tecnologías basadas en Ethernet es perfectamente posible, mucho más cuando esta misma tecnología ha evolucionado de forma significativa en los últimos años y alcanza velocidades de transmisión muy elevadas, en el orden de los Gbps (Gigabits por segundo) con altas capacidades de multiplexación.

Los sistemas ERP (del inglés, *Enterprise Resource Planning*), con todas sus variantes en relación a la gestión de proveedores, clientes, logística, etc., constituyen uno de los pilares de estos niveles superiores. Las herramientas asociadas están claramente centradas en el diseño y la optimización del software, y tratan de ser lo más agnósticas posibles respecto de la tecnología de comunicaciones concreta utilizada en los niveles inferiores. Por tanto, su evolución en la Industria 4.0 se nutrirá únicamente de las nuevas prestaciones que estarán disponibles en dichos niveles, sin entrar en los detalles técnicos de cómo se han alcanzado.

Los sistemas IT, sea cual sea su arquitectura, necesitan de las comunicaciones como algo fundamental para el intercambio de información entre los ordenadores y servidores de almacenamiento y procesado de datos. Cualquier tecnología de transmisión podrá ser utilizada siempre que se adapte al volumen y prestaciones requeridas por la dimensión de la industria correspondiente y sus procesos productivos. Las nuevas prestaciones que aportará la tecnología 5G en los niveles superiores deberán ser aprovechadas por estos sistemas de cara a ofrecer nuevos servicios y también para la optimización de los existentes.

Sistemas de comunicación inalámbricos

En el apartado anterior hemos presentado la arquitectura de comunicaciones que se utiliza para conectar los diferentes elementos de un sistema de producción industrial, desde los sensores hasta los sistemas de gestión de la producción, y las diferentes tecnologías que se utilizan para cada uno de los niveles. Como hemos visto, en el ámbito de la interconexión de sistemas IT, la tecnología más habitual hoy en día es Ethernet; para la interconexión de sistemas OT, las tecnologías más habituales son los buses de campo para la interconexión de los sensores y actuadores con los sistemas de control en tiempo real, y Ethernet para los sistemas de monitorización y supervisión.

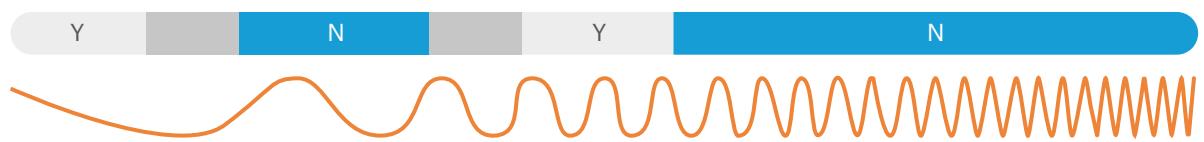
Vemos pues, cómo las tecnologías de comunicación que se han utilizado hasta la fecha en el ámbito industrial son mayoritariamente cableadas. Esto responde a la concepción que los sistemas de comunicación inalámbricos no son adecuados para los sistemas industriales debido a que no ofrecen determinismo (ancho de banda garantizado, latencia y variación de la misma, pérdida de paquetes, etc.). Pero en el marco de la Industria 4.0, los sistemas de producción industrial han evolucionado y, en algunos casos, la movilidad o la facilidad de instalación de los mismos son requisitos indispensables, por lo que las tecnologías de comunicación inalámbricas se vuelven imprescindibles.

Teniendo esto en cuenta, en esta sección se realiza una breve introducción a los sistemas de comunicación inalámbricos y, a continuación, se presentan los dos tipos de sistemas de comunicación inalámbricos más utilizados: los sistemas de comunicación sin cables que utilizan bandas frecuenciales de uso libre o también llamados libres de licencia, y los sistemas que utilizan bandas frecuenciales de uso bajo licencia.

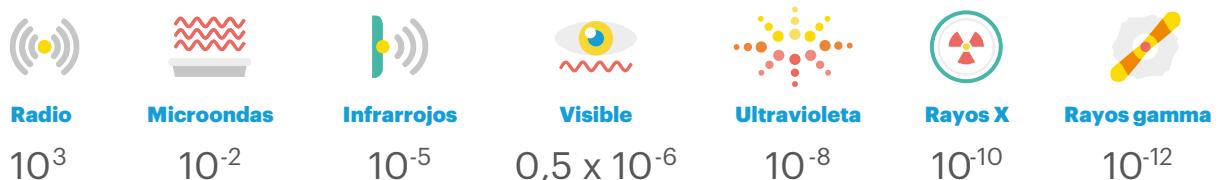
Introducción a los sistemas de comunicación inalámbricos

Los sistemas de comunicación modernos utilizan la radiación electromagnética para transportar información entre dos o más puntos. En el caso de los sistemas de comunicación cableados, el medio de transporte es un cable de cobre o una fibra óptica, que se encarga de facilitar la propagación de las ondas y aislarlas del exterior. En el caso de los sistemas de comunicación inalámbricos, no existe un soporte físico para transportar información, ya que las ondas electromagnéticas también se propagan a través del vacío y el aire. En concreto, los sistemas de comunicación inalámbricos más utilizados en la actualidad usan la banda de las microondas, que se comprenden entre los 300 MHz y los 300 GHz (correspondiente a una longitud de onda de entre 1 metro y 1 milímetro) dentro del llamado espectro radioeléctrico, tal como se muestra en la Figura 13. Estas frecuencias son las más utilizadas debido a que ofrecen unas buenas prestaciones respecto a propagación de la señal a través del espacio, el ancho de banda disponible para la comunicación y el tamaño de las antenas necesario para tener una buena eficiencia tanto en transmisión como en recepción de las señales.

¿Penetra en la atmósfera terrestre?



Tipo de radiación y longitud de onda



Escala aproximada de longitud de onda



Frecuencia (Hz)



Figura 13. Representación gráfica del espectro radioeléctrico.

A la hora de diseñar un sistema de comunicación inalámbrico, es importante tener en cuenta tres parámetros principales: la frecuencia de transmisión, el ancho de banda disponible y la potencia de transmisión. En general, cuanto mayor es la frecuencia de transmisión, mayor es el ancho de banda disponible, de modo que se puede transmitir a más velocidad. Además, es posible utilizar antenas de menor tamaño. Por contra, cuanta mayor frecuencia, mayor es también la atenuación que presenta la señal al propagarse por cada unidad de distancia, de modo que mayor debe ser la potencia de transmisión para tener un rango de cobertura equivalente. En cambio, si reducimos la frecuencia, conseguimos un mayor nivel de cobertura, disminuyendo la potencia necesaria, pero el ancho de banda disponible será menor y se requerirá de antenas de mayor tamaño debido a que estas tendrán una menor eficiencia. Además, al tratarse de un medio de comunicación no guiado, las ondas electromagnéticas se propagan a través del espacio en todas las direcciones, de modo que dos transmisiones simultáneas en la misma banda de frecuencias y en el mismo espacio físico se interfieren, dificultando la recepción de las mismas por parte de los equipos receptores. Además, cualquier obstáculo físico presente en el camino que deba recorrer la señal supondrá, en términos generales, una mayor atenuación cuanto mayor sea la frecuencia utilizada, reduciendo por ejemplo el nivel de cobertura en entornos de interiores o con fuerte presencia de objetos.

El espectro radioeléctrico es un bien público y, como tal, su gestión corre a cargo de la administración de cada país, que se encarga de establecer normas para su uso (bandas disponibles, tipo de uso, potencia y tiempo máximo de transmisión, etc.). Este bien público es, además, escaso, por lo que la regulación debe ser estricta. En el caso de España, el documento que regula el uso del espectro radioeléctrico es el CNAF (Cuadro Nacional de Atribución de Frecuencias), publicado regularmente en el BOE (Boletín Oficial del Estado), donde se especifica la asignación de los diferentes servicios (radiodifusión, radionavegación, radiolocalización, acceso fijo y acceso móvil) a las diferentes bandas de frecuencias. Además, el CNAF se coordina con los organismos internacionales encargados de la regulación a nivel internacional (ITU-T,⁶ ETSI,⁷ etc.) con el objetivo de armonizar y facilitar que los diferentes servicios de radiocomunicación puedan coexistir e interoperar.

Dentro de la regulación⁸ encontramos una clasificación de las diferentes bandas según su tipo de uso: uso común, uso especial, uso privativo, uso reservado para el Estado y, finalmente, uso mixto (combinación del privativo y el reservado). Así pues, las bandas de uso común son aquellas que los usuarios pueden utilizar sin necesidad de una licencia por parte de la administración, ni están sujetas a limitación de número de operadores o usuarios. Por contra, las bandas de uso privativo son aquellas que requieren de una licencia de uso por parte de la administración y, por tanto, están sujetas a control. Estas licencias se asignan directamente en el caso de servicios de interés público (por ejemplo, radio y televisión) o a través de subastas donde los operadores pujan para obtener una licencia de uso durante un tiempo determinado que les permita prestar un servicio (por ejemplo, telefonía móvil). En cualquier caso, es importante destacar que todas las bandas están reguladas a nivel de ancho de banda disponible, potencia máxima de transmisión y tiempo máximo de transmisión, ya que, como hemos comentado antes, se trata de un medio no guiado y las transmisiones simultáneas causan interferencias que pueden afectar negativamente al correcto funcionamiento de los sistemas de comunicación.

⁶ ITU-T, del inglés International Telecommunication Union.

⁷ ETSI, del inglés European Telecommunications Standards Institute.

⁸ Real Decreto 123/2017, de 24 de febrero, por el que se aprueba el Reglamento sobre el uso del dominio público radioeléctrico.

Teniendo en cuenta esto, podemos encontrar sistemas de comunicación móvil basados en bandas de uso común y sistemas de comunicación móvil basados en banda de uso privativo, tal como se describe a continuación.

Sistemas de comunicación inalámbricos basados en bandas de uso común (sin licencia de uso)

A nivel mundial, las bandas de uso común para sistemas de comunicación inalámbricos más habituales son las comprendidas en la banda ISM (del inglés, *Industrial, Scientific and Medical*), tal como se presenta en la Tabla 1. Si bien existen otras bandas de uso común (por ejemplo, 433 MHz, 868 MHz o 915 MHz), estas solo están disponibles en algunas regiones, lo que dificulta la interoperabilidad de los sistemas de comunicación móvil y, por tanto, su uso es más restringido. No es de extrañar, pues, que las tecnologías más utilizadas para sistemas de comunicación móvil, como por ejemplo wifi (basada en el estándar IEEE 802.11) y Bluetooth (basada en el estándar IEEE 802.15.1), utilicen las bandas de 2.4 GHz y 5.8 GHz.



Banda	Frecuencia inicio	Frecuencia fin	Ancho de banda
13.56 MHz	13.553 MHz	13.567 MHz	14 kHz
433.92 MHz	433.05 MHz	434.79 MHz	1.74 MHz
868 MHz	863 MHz	870 MHz	7 MHz
915 MHz	902 MHz	928 MHz	26 MHz
2.45 GHz	2.4 GHz	2.5 GHz	100 MHz
5.8 GHz	5.725 GHz	5.875 GHz	150 MHz
24 GHz	24.25 GHz	24.125 GHz	250 MHz

Tabla 1. Bandas de uso común⁹ para sistemas de comunicación inalámbricos sin licencia. Como se puede observar, a medida que aumenta la frecuencia, aumenta el ancho de banda disponible.

⁹Las bandas 433.92 MHz y 868 MHz solo están disponibles en la Región 1 (Europa y África), mientras que la banda 915 MHz solo está disponible en la Región 2 (América).

Además de la banda de frecuencias en las que operan (que de manera indirecta determinan el alcance de la comunicación y el ancho de banda disponible para el envío de datos), las tecnologías de comunicación por radio se pueden clasificar según la topología de la red y el mecanismo que usan los dispositivos para acceder a Internet (o redes de ámbito superior al local). La topología en redes de comunicaciones por radio suele ser en estrella (en inglés, *star*) o en malla (en inglés, *mesh*), tal como se muestra en la Figura 14. En las redes en estrella existe un dispositivo central que coordina la red y los dispositivos extremos que se comunican únicamente con este. En una red mallada, también existe un dispositivo central que coordina la red pero, a diferencia de la topología en estrella, los dispositivos extremos también pueden comunicarse entre sí, con la posibilidad de formar redes multisalto.

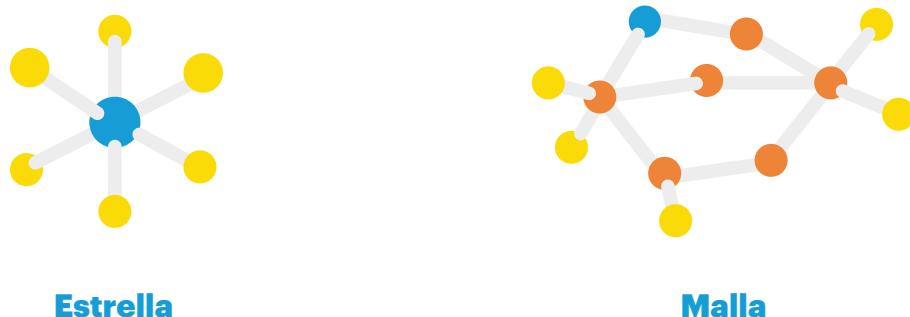
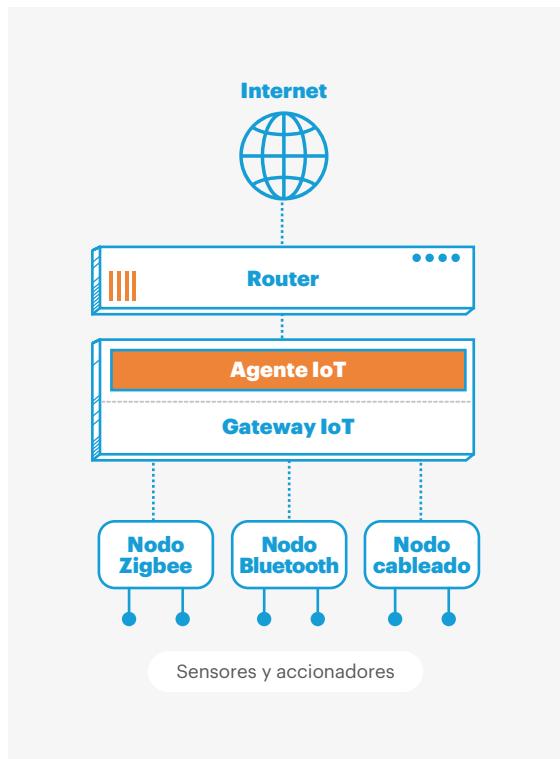


Figura 14. Redes en estrella (izquierda) y malladas (derecha).

En lo que se refiere al acceso a Internet de los dispositivos, las tecnologías se pueden clasificar según si estos acceden directamente a Internet o lo hacen a través de un *gateway*, tal como se muestra en la Figura 15. Si los dispositivos extremos implementan la pila de protocolos de Internet (TCP/IP), se pueden comunicar directamente con Internet. En cambio, si los dispositivos extremos no implementan la pila de protocolos de Internet (TCP/IP), será necesaria la presencia de un *gateway* que les realice las funciones de adaptación de los protocolos entre la red local e Internet.

Conexión mediante gateway



Conexión directa

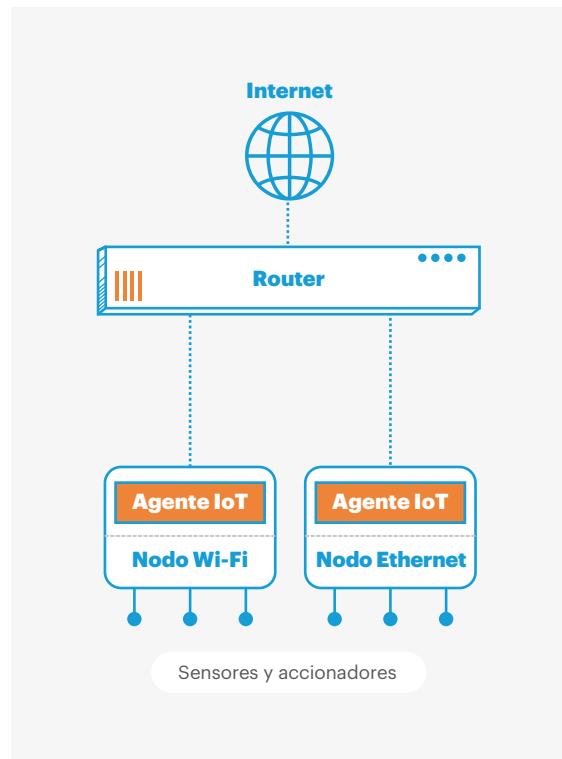


Figura 15. Conexión directa o mediante gateway a Internet.

La tecnología wifi utiliza una topología en estrella donde el punto de acceso (del inglés, *access point*) se encarga de gestionar la red. Además, los dispositivos implementan la pila de protocolos TCP/IP, de modo que no hace falta ningún dispositivo intermedio para acceder a Internet. En cambio, la tecnología Bluetooth utiliza una topología en estrella, pero los dispositivos no implementan la pila de protocolos TCP/IP, de modo que hace falta un proceso en el gateway que realice la conversión bidireccional para permitir el acceso a Internet de los dispositivos.

Además de wifi y Bluetooth, también existen otras tecnologías de comunicación móvil que utilizan las bandas libres y que están enfocadas a la comunicación de dispositivos en un contexto industrial. Por un lado, tenemos tecnologías como LoRa y Sigfox, que utilizan una topología de red en estrella y un modelo de acceso a Internet indirecto, y se caracterizan

por ofrecer un gran nivel de cobertura (mayor a un kilómetro), pero un ancho de banda muy reducido (menor a 10 kilobits/segundo). Por otro lado, tenemos tecnologías como WirelessHART e ISA100.11a, que utilizan una topología de red en malla y un modelo de acceso a Internet directo, y se caracterizan por ofrecer una fiabilidad elevada en las comunicaciones a pesar de funcionar en una banda sin licencia.

Sistemas de comunicación inalámbricos basados en bandas de uso privativo (con licencia de uso)

A diferencia de los sistemas de comunicación que utilizan bandas de uso común, los sistemas de comunicación que utilizan bandas de uso privativo requieren de una licencia para poder operar. Dichas licencias las obtienen los operadores de telecomunicación a través de una licitación organizada por el Estado y la utilizan para prestar un servicio, que puede ser de carácter privado o público. Como hemos visto antes, existen diferentes usos para las bandas de uso privativo, pero uno de los más extendidos son los sistemas celulares que permiten la comunicación de voz y datos a los usuarios, tal como se detalla a continuación.

La tecnología celular se desarrolló a finales de los años 80 para permitir llamadas de voz a través de dispositivos móviles a dispositivos de la red de telefonía fija o a otros dispositivos de la red móvil. A nivel conceptual, en una red celular existen un conjunto de dispositivos móviles (en inglés *Mobile subscribers*) que se conectan a una estación base que se encuentre próxima a ellos, tal como se muestra en la Figura 16. Para dar cobertura global en todo el territorio, el operador móvil despliega un conjunto de estaciones base (BTS, en inglés *Base Transceiver Station*) que se encargan de dar cobertura a cada zona determinada. De este modo, un dispositivo móvil irá cambiando de estación base a medida que se desplace.

A su vez, estas estaciones base están conectadas, mediante radioenlaces o enlaces de fibra óptica, a un controlador de estaciones base (BSC, en inglés *base station controller*) que se encargan de su gestión a nivel territorial. Finalmente, un conjunto de estaciones base se conectan a un centro de conmutación (MSC, en inglés *Mobile Switching Center*) que se encarga de redirigir el tráfico entre los diferentes elementos que conforman la red, permitiendo realizar llamadas a terminales fijos y móviles, así como acceder a Internet.



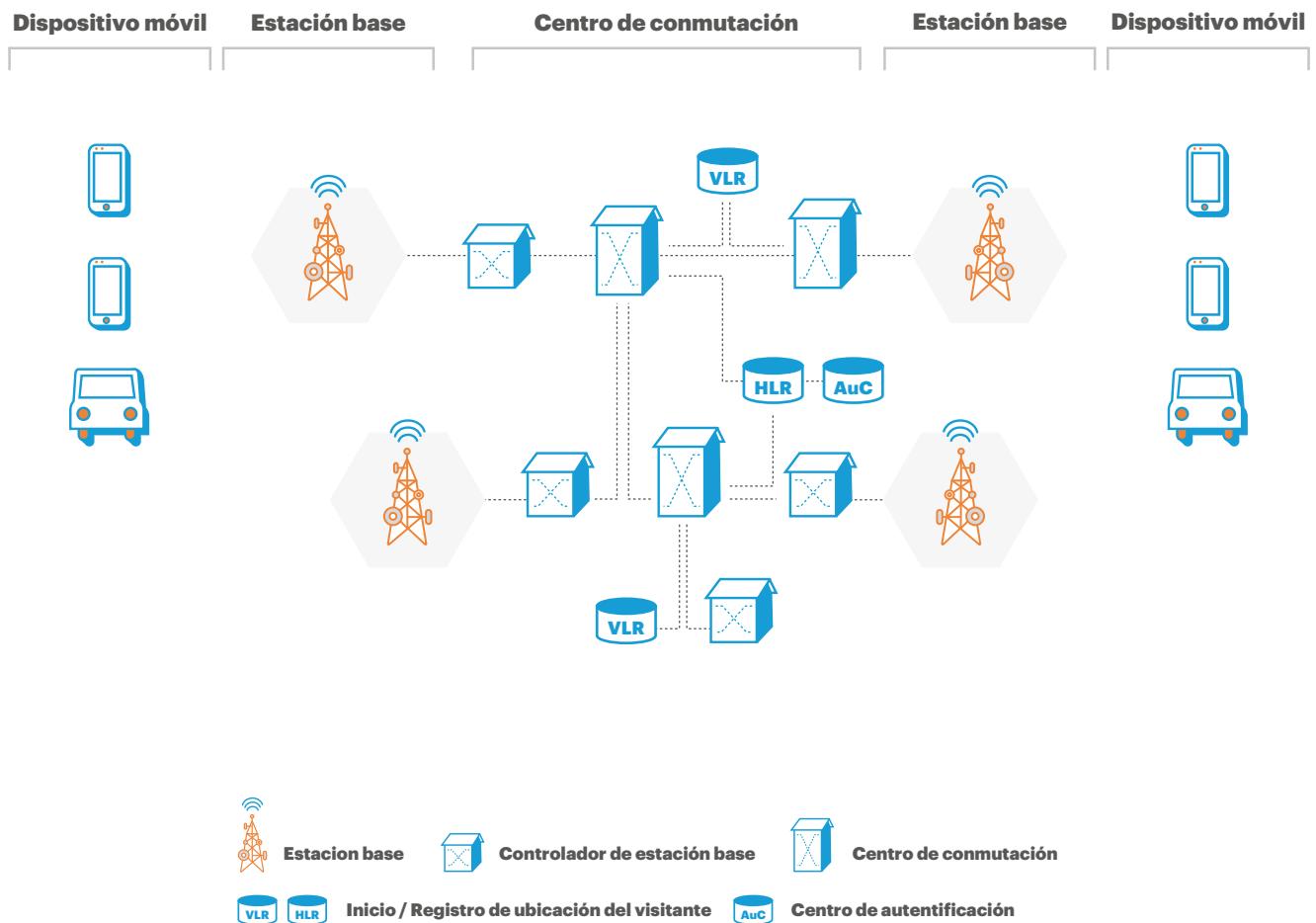


Figura 16. Arquitectura de una red celular.

La creciente demanda del servicio por parte de los usuarios y la voluntad de los operadores de ofrecer nuevos servicios multimedia ha dirigido la evolución de la red de acceso y la red principal, pasando de una red completamente analógica, centrada en la transmisión de voz, a una red completamente digital centrada en la transmisión de datos. Así pues, hemos pasado de accesos de datos de banda estrecha con la tecnología 2G (64 kbps en GPRS) en los años 90, a accesos de banda ancha con la tecnología 4G (hasta 1 Gbps en LTE-A) en el año 2014, tal como se muestra en la Figura 17. Esto supone un incremento del ancho de banda del 55% anual sostenido durante 23 años o, de manera equivalente, a multiplicar por un factor 25 000 la capacidad de la red.

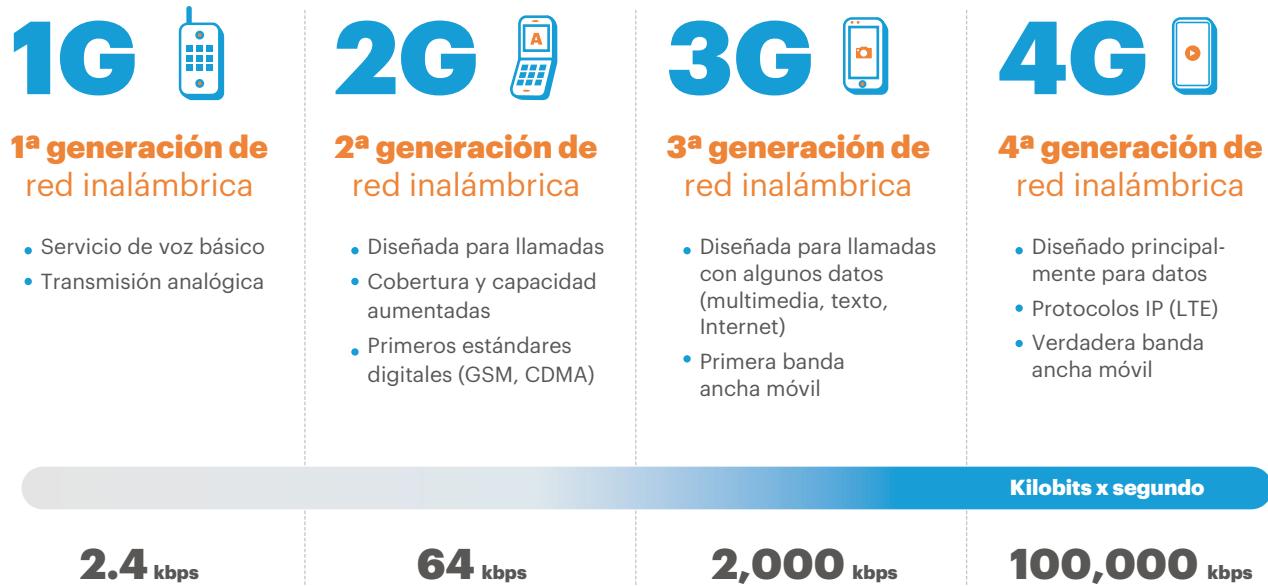


Figura 17. Evolución de la tecnología celular anterior a 5G.

Pero, como hemos visto antes, no todos los casos de uso de la tecnología móvil requieren de un gran ancho de banda por parte de los usuarios para descargar información. Otros casos de uso pueden necesitar conectar miles de dispositivos que envían pequeñas cantidades de información de manera simultánea, o comunicarse con un servidor con baja latencia y de manera determinista. Del mismo modo, en algunos casos de uso también se puede plantear la necesidad de que la red no sea gestionada por la operadora de telecomunicación móvil, y es aquí donde la tecnología 5G supone un cambio de paradigma, como veremos en el siguiente apartado.



3

La tecnología 5G

5G es la primera tecnología de comunicaciones móviles que se ha diseñado, desde su concepción, para satisfacer las necesidades de los diferentes usos que la tecnología puede tener en lo que se han venido a denominar usos «verticales». Para comprender el concepto de **vertical**, tan solo hay que imaginar la red de comunicaciones como un habilitador horizontal, transversal, que es común para diferentes aplicaciones verticales, tales como la industria de la energía, la manufactura, la logística, la industria de la movilidad, las ciudades inteligentes, los sistemas digitales de monitorización y vigilancia de la salud, etc.

La tecnología 5G no se ha diseñado con el único objetivo de ofrecer velocidades de descarga y de subida de datos más rápidas respecto a los sistemas de comunicación anterior (con tecnología 2G, 3G o 4G), sino que se ha diseñado para constituir una tecnología que permita satisfacer las necesidades de 3 grandes grupos de casos de uso, tal y como se representa en la Figura 18 que ilustra el triángulo de 5G:

- 1. eMMB** (del inglés, *evolved Mobile Broadband Communications*), que permite ofrecer velocidades de transmisión muy elevadas. Este tipo de comunicaciones es de gran utilidad cuando la cantidad de datos a transmitir es muy elevada, tanto para, por ejemplo, transmisión de vídeo de muy alta definición (4K, 8K, o lo que esté por venir), como cuando el número de dispositivos a conectar en una misma área de influencia es muy elevado; por ejemplo, maquinaria conectada en una línea transmitiendo información de manera constante sobre el estado de un proceso determinado, agregando información de múltiples sensores de manera simultánea.
- 2. URLLC** (del inglés, *Ultra Reliable Low Latency Communications*), que permite ofrecer comunicaciones de muy baja latencia (por debajo de 1 milisegundo) y de muy alta fiabilidad (99,999% de disponibilidad y fiabilidad de las comunicaciones). Este tipo de comunicaciones permiten equiparar 5G a las prestaciones que hasta hoy solo se podían alcanzar a través de cables. Este tipo de comunicaciones habilita lo que también se conoce como el «Internet de las habilidades» (del inglés, *Internet of Skills*), de manera que se pueden hacer realidad manipulaciones remotas sobre objetos, por ejemplo, tales como vehículos o robots mecanizados. Este tipo de comunicaciones son fundamentales para hacer posibles aplicaciones en tiempo real en las que se utilicen los conceptos de realidad virtual o realidad aumentada, de gran interés de aplicación en la industria. Además, la alta fiabilidad permite ejecutar servicios críticos sobre las redes de comunicaciones, logrando una fiabilidad equiparable a las de un cable.
- 3. mMTC** (del inglés, *massive Machine-Type Communications*), que permite ofrecer conectividad a un número muy elevado de dispositivos conectados de manera simultánea. Este tipo de comunicaciones son necesarias cuando, por ejemplo, un elevado número de sensores se concentra en un área determinada. Aunque cada sensor no transmita una gran cantidad de información de manera individual, todos los sensores de manera agrupada pueden generar una alta demanda de transmisión de datos. En este sentido, no es lo mismo 10 máquinas transmitiendo mensajes de 1 000 000 de bits, que 1 000 000 de máquinas transmitiendo mensajes de 10 bits. Aunque la cantidad de datos agregada es la misma, el impacto sobre la operativa de la red de comunicaciones es diferente; las redes 5G están diseñadas para ser capaces de gestionar de manera eficiente un elevado número de dispositivos conectados de manera simultánea.

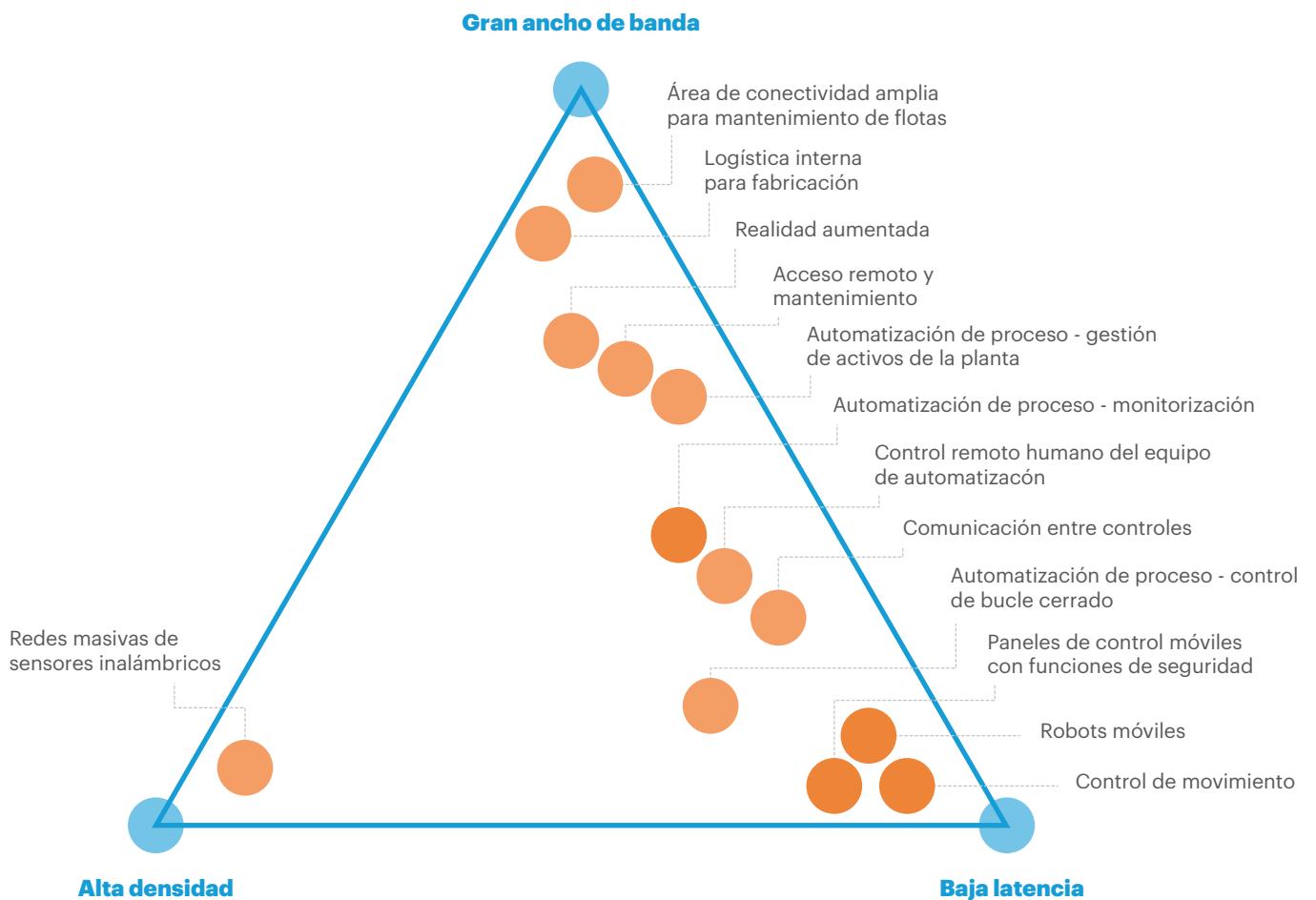


Figura 18. El triángulo del 5G: 3 familias de casos de uso de la Industria 4.0.

¿Qué ofrece la tecnología 5G?

Para poder ofrecer comunicaciones eficaces y eficientes para los 3 tipos de casos de uso descritos anteriormente, la ITU (en inglés, *International Telecommunications Union*) definió los requerimientos de la tecnología 5G en lo que se conoce como IMT (en inglés, *International Mobile Telecommunications*) 2020. En base a estos requerimientos, los sistemas IMT-2020 y, por lo tanto, las tecnologías 5G, serán aquellas que:

- Operen de manera nativa para el protocolo de Internet, conocido por sus siglas en inglés, como el protocolo IP (en inglés, Internet Protocol).
- Multipliquen por 100 la capacidad de transmisión de datos por metro cuadrado y por segundo, pasando de 0,1 Mbps/s/m² en tecnología 4G a 10 Mbps/s/m² en tecnología 5G.
- Aseguren al menos una velocidad media de transmisión de datos por usuario 10 veces superior a 4G, es decir, de al menos 100 Mbps.
- Puedan alcanzar picos de transmisión de datos de al menos 20 Gbps, 20 veces superior a 1 Gbps esperado para la tecnología 4G.
- Mejoren la eficiencia espectral en al menos un factor 3 respecto a 4G; esto quiere decir que se puedan transmitir al menos el triple de datos por hercio de frecuencia utilizado.

- Permitan comunicaciones sin cortes con terminales móviles moviéndose hasta velocidades de 500 km/h (sobre todo, pensando en trenes de alta velocidad).
- Alcancen latencias de 1 ms, es decir, 10 veces menos que en redes 4G. La latencia mide el tiempo que tarda un determinado mensaje en llegar de un origen a un destino.
- Permitan densidades de usuario de hasta 1 millón de terminales por kilómetro cuadrado; esto es, 10 veces más que las redes 4G.
- Mejoren la eficiencia energética de la red en un factor 1000 respecto a las redes 4G, afectando tanto al consumo de la red como al de los terminales.

Conseguir todos estos requerimientos de manera simultánea no es posible. Por ello, la tecnología 5G se ha diseñado de manera flexible; en función de a cuál de los tres tipos de casos de uso se quiere proveer de conectividad, se debe seleccionar algunos de estos requisitos y configurar de manera dinámica la red para asegurar su correcto funcionamiento. Esto se representa en la figura inferior, donde se muestran qué requisitos se pueden asociar, de manera genérica, a cada uno de los 3 tipos de caso de uso.

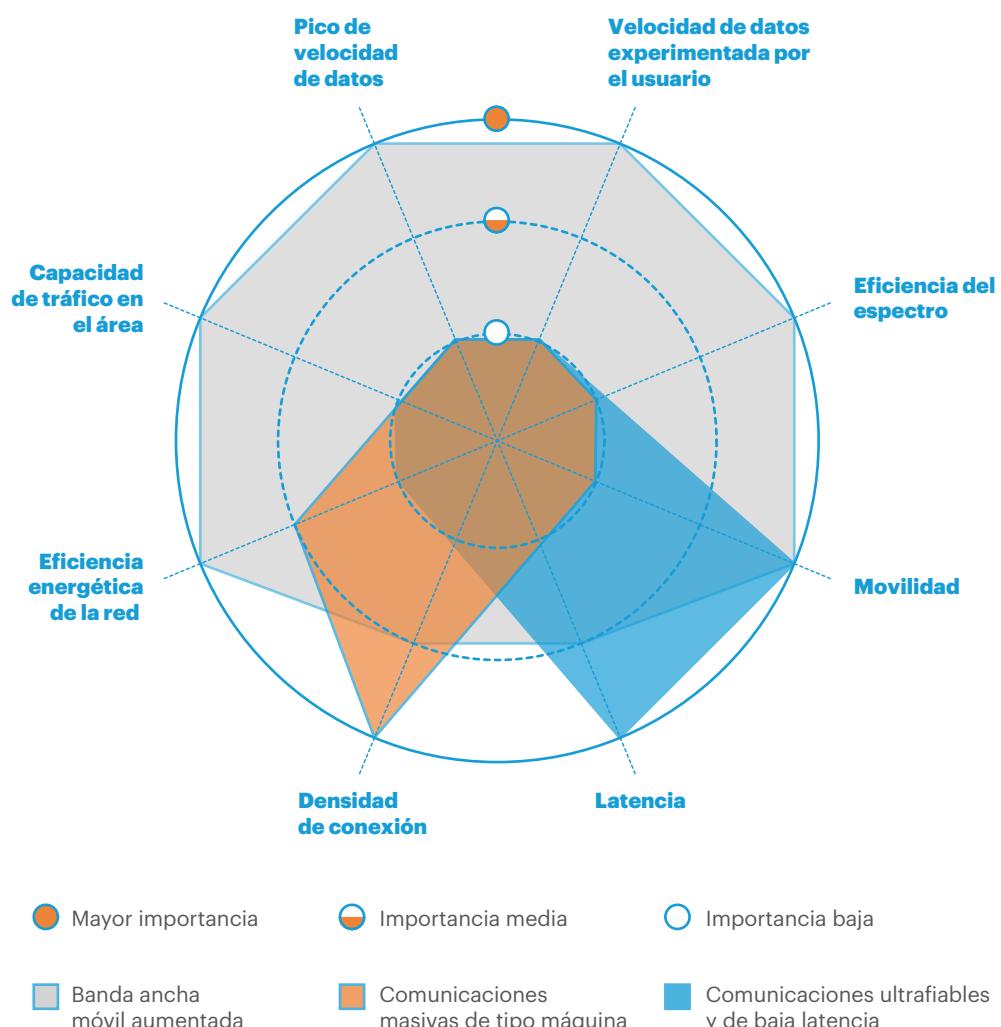


Figura 19. Diferentes familias de casos de uso tienen diferentes requisitos de comunicaciones.



Las expectativas del 5G desde el punto de vista industrial son elevadas. La industria alemana ha creado una alianza denominada 5GACIA (del inglés 5G Alliance for Connected Industries and Automation) para influir en la estrategia de despliegue de 5G. Según un estudio interno de la VDMA de 2019, el 69% de las empresas proveedoras de máquinas y sistemas productivos en planta de Alemania están planeando equipar sus sistemas con interfaces 5G.¹⁰

¿Cómo se hace esto en 5G?

Las redes 5G son redes de comunicaciones celulares. Este tipo de redes están compuestas por dos grandes partes:

- 1. La parte de red de acceso, del inglés Access Network:** que permite comunicar los dispositivos del mundo físico, los endpoints, con el mundo digital. El acceso a la red puede ser sin cables, usando el aire como medio de comunicación, o a través de cables, de hilos de cobre o de fibra óptica como medio de transmisión de información. En el caso de las redes móviles 5G, el acceso puede ser por radio o cableado; en el caso de ser por radio, que es el modo de despliegue que ofrece mayor flexibilidad y versatilidad, esta parte de la red recibe el nombre inglés Radio Access Network (RAN).
- 2. La parte de red principal, del inglés Core Network:** es la que permite que los datos, en forma digital (es decir, bits, ceros y unos), se distribuyan, almacenen, y procesen en el mundo virtual; este mundo virtual está formado por ordenadores con capacidad de almacenamiento y procesado que están distribuidos por el mundo. Dependiendo de lo lejos «físicamente» que estén del usuario final de las comunicaciones, este mundo virtual se clasifica en *edge* y *cloud*, como se ha descrito anteriormente en la arquitectura de referencia, y como se explicará con más detalle más adelante.

El 3GPP (en inglés, *Third Generation Partnership Program*) es el organismo internacional encargado de definir las especificaciones técnicas que luego se transponen en estándares de redes celulares, ya sean a nivel de la ETSI (en inglés, *European Telecommunications Standardization Institute*) en Europa —o los organismos equivalentes en las diferentes regiones del mundo— o de la ITU (en inglés, *International Telecommunication Union*), a nivel global. La industria de las telecomunicaciones participa en este organismo, incluyendo mayoritariamente a operadores de telefonía móvil y fabricantes de equipos de comunicaciones. El 3GPP hace públicas versiones de estas especificaciones públicas que reciben el nombre de *Releases*. Los primeros progresos hacia la tecnología 5G se incluyeron en la *Release 14*, siendo las *Release 15* y *Release 16* las especificaciones formales de la tecnología 5G, descrita en dos fases. De cara al año 2021, el 3GPP plantea elaborar una nueva *Release 17* que constituya una evolución y optimización de las redes 5G.

¹⁰ Estudio VDMA sobre 5G <https://www.vdma.org/en/v2viewer/-/v2article/render/42587492>

La transición del 4G al 5G: Despliegues SA y NSA

La separación de la red en dos partes —red de acceso y red principal— ha dado lugar a lo que se conoce como despliegue de tecnología 5G en modo SA (del inglés, stand alone) o en modo NSA (non stand alone). En los despliegues SA, ambas partes de la red utilizan tecnología 5G. Sin embargo, en los despliegues NSA, la red de acceso es 5G, mientras que la red principal, la core network, se basa en tecnología 4G. Es de esperar que la transición de la tecnología 4G a la tecnología 5G no sea de la noche a la mañana. Se estima que esta transición durará varios años, en los que veremos cómo los primeros despliegues NSA van evolucionando de forma progresiva a despliegues SA, en los que se podrá alcanzar todo el potencial prometido de la tecnología 5G en base a los requerimientos definidos en el IMT-A.

La red de acceso

A diferencia de los sistemas de comunicación que utilizan bandas de uso común, los sistemas de comunicación que utilizan bandas de uso privativo requieren de una licencia para poder operar. Dichas licencias las obtienen los operadores de telecomunicación a través de una licitación organizada por el Estado y la utilizan para prestar un servicio, que puede ser de carácter privado o público. Como hemos visto antes, existen diferentes usos para las bandas de uso privativo, pero uno de los más extendidos son los sistemas celulares que permiten la comunicación de voz y datos a los usuarios, tal como se detalla a continuación.

La red de acceso en 5G puede utilizar tanto el aire como cables como medio de comunicación. Sin embargo, en términos generales, se considera la tecnología 5G como un sistema que permite movilidad y flexibilidad gracias al uso de comunicaciones sin cables. Por lo tanto, en adelante, nos referiremos a la red de acceso principalmente como la red de acceso sin cables; la RAN. El término *radio* hace referencia a las ondas radioeléctricas que se utilizan para transmitir la información a través del aire.

Sin entrar en detalles técnicos sobre la propagación de ondas radioeléctricas por el aire, es importante tener en cuenta que estas ondas se caracterizan principalmente por tener una amplitud (cuánto oscilan las ondas) y una frecuencia (cómo de rápido oscilan estas ondas). En función de cómo varíe a lo largo del tiempo esta amplitud y esta frecuencia, se habla de diferentes tipos de modulaciones, que dan lugar a diferentes maneras de modular la onda y transmitir información por el aire. Gracias a la tecnología de comunicación por radio, es posible recibir de manera independiente información transmitida por el aire que usa frecuencias diferentes, aunque la información se transmita de forma simultánea en el tiempo. Esto es un principio fundamental para los sistemas de comunicación por radio, ya que permiten dar acceso a múltiples usuarios al mismo tiempo repartiéndolos en el espectro radioeléctrico.

A nivel nacional, cada país reserva unas bandas frecuenciales que permiten a los operadores ofrecer servicios de comunicación por radio asegurando que otros servicios no interferirán. Aunque las bandas concretas dependen de las diferentes regiones del planeta, en términos generales se puede decir que la tecnología 5G está diseñada para operar en 3 bandas frecuenciales:

- **Banda por debajo de 1 GHz:** para habilitar grandes rangos de cobertura, permitiendo conectividad en sótanos y en zonas alejadas de núcleos urbanos densos, por ejemplo.
- **Banda por encima de 1 GHz y por debajo de 6 GHz:** para proveer servicios en entornos densos, con alta capacidad de transmisión de datos y sin necesidad de visión directa entre transmisor y receptor. Podríamos decir en lenguaje sencillo, que esta sería la evolución «más natural» de la tecnología 4G.
- **Banda por encima de los 20 GHz:** lo que se conoce como bandas milimétricas, para ofrecer capacidad ultraelevada y servicios innovadores en entornos con rangos de cobertura más pequeños, como pueden ser entornos industriales, empresariales o domésticos. Cuando las comunicaciones se llevan a cabo en estas bandas muy altas de frecuencia, es necesario que haya visión directa entre el origen y el destino de las transmisiones, puesto que cualquier obstáculo bloqueará la propagación de la señal, limitando por lo tanto su aplicación a determinados casos de uso.

Además, la tecnología 5G permitirá la coexistencia y cooperación con otras tecnologías de radio operando en frecuencias libres de licencia, como por ejemplo las bandas ISM, del inglés *Industrial, Scientific and Medical*, en las que operan, por ejemplo, las redes wifi y las redes Bluetooth.

La tecnología 5G contempla, además, la posibilidad de establecer comunicación directa entre dispositivos a través de las comunicaciones D2D (dispositivo a dispositivo), sin necesidad de encaminar los datos a través de la infraestructura. Este tipo de comunicaciones permite reducir la latencia y el retardo de las transmisiones y poder «descargar» en el enlace principal, con el objetivo de aumentar la capacidad del sistema. Un claro ejemplo de la utilidad de este tipo de comunicaciones es para gestionar la comunicación entre vehículos, a través de las llamadas comunicaciones V2V, del inglés, *Vehicle-to-Vehicle*.

La red principal (core network)

Además de mejoras en la red de acceso por radio respecto a tecnologías anteriores como el 4G, la tecnología 5G incorpora mejoras en la arquitectura de red principal para lograr una gran flexibilidad y dinamismo en la manera en que se gestiona la red. No es el objetivo de este documento ofrecer una descripción detallada de la arquitectura de red principal de 5G, sino destacar los factores diferenciales respecto a tecnologías anteriores, y poner el énfasis en aquellos aspectos de su diseño que permiten que la tecnología 5G vaya a ser todo lo disruptiva que se promete.

En términos sencillos, podemos decir que la tecnología 5G implica la «softwarización»

de la red de comunicaciones. En tecnologías celulares anteriores, la red se componía de una serie de equipos de red dedicados, que estaban diseñados para realizar funciones necesarias en la red, tales como la gestión de datos de usuario, autenticación, funciones de gestión de movilidad, sistema de monitorización de uso para el cobro de las tarifas asociadas al servicio de conectividad, funciones de encaminamiento en la red, etc. En la tecnología 5G, todas estas funciones se *virtualizan*. Esto quiere decir que la red está compuesta de equipos informáticos de uso general (no dedicados para una única función específica), que se configuran y reconfiguran de manera dinámica para poder ejecutar unas funciones u otras en función de las necesidades. Este desacople es lo que da lugar al concepto de redes definidas por software o SDN (del inglés, *Software Defined Networks*), que permiten desplegar las funcionalidades de red de manera virtualizada, dando lugar al concepto de NFV (del inglés, *Network Function Virtualization*). Esta virtualización, además de ofrecer flexibilidad y dinamismo a la configuración de la red, permite separar lo que se conoce como el plano de datos y el plano de control. Como datos entendemos toda la información de interés para los *endpoints*. Como control entendemos toda la información necesaria por parte del operador de red para garantizar que la red ofrece servicios de comunicación de un extremo a otro, siendo capaz de garantizar la calidad de servicio esperada por los *endpoints*.

La separación de los planos de datos y control permite que los datos y servicios que finalmente utilice un usuario final puedan desplegarse en cualquier elemento de la red; esta capacidad es la que habilita los conceptos de MEC (en inglés, *Mobile Edge Computing*)¹¹ y *cloud computing*. Con la tecnología 5G ya no es necesario disponer de un servidor de datos o de procesado de información en la nube; la información puede almacenarse y procesarse en cualquier parte de la red, abriendo un enorme abanico de posibilidades tanto a nivel técnico como a nivel de nuevas oportunidades de negocio, tanto para los operadores de red tradicionales como para nuevos operadores de red y proveedores de servicios.

Veamos un ejemplo sencillo: cuando es necesario que un servicio garantice tiempos de respuesta extremadamente cortos, el despliegue de dicho servicio en un nodo MEC, físicamente instalado cerca de los dispositivos, permite reducir el tiempo de respuesta del servicio, además de aplicar técnicas de predicción de datos y de almacenamiento de datos.

Además, esta virtualización de las funciones de red habilita lo que se conoce como *Network Slicing*. Esta técnica permite que, sobre una misma infraestructura de red, se puedan configurar diferentes redes software que se ejecuten en paralelo, sin afectarse la una con la otra. Para cada red, se pueden reservar una serie de recursos de almacenamiento, cómputo y transmisión de datos, de manera que el rendimiento de una «porción» de la red no se vea afectado por el rendimiento de la otra «porción» de la red.

Pongamos un ejemplo; una planta de ensamblaje de motores construida en base a una línea de montaje que está monitorizada por un sistema de sensores que permite observar en tiempo real el rendimiento de la línea y, por lo tanto, realizar tareas de mantenimiento predictivo. En este escenario, gracias al *Network Slicing*, es posible, sobre la misma infraestructura de comunicaciones, tener dos redes de comunicaciones independientes: una

¹⁰ La ETSI usa la terminología más general Multi-Access Edge Computing - MEC - para notar que la computación en el extremo (edge computing) se puede implementar usando diferentes tipos de redes de acceso, no necesariamente una red móvil.

para dar acceso a los trabajadores a los sistemas de información de la empresa y otra para el sistema de sensores de la línea de montaje. De este modo, por ejemplo, se puede garantizar que una demanda momentánea muy elevada por parte de los trabajadores no afecte a los sistemas de monitorización de la línea de montaje que deben trabajar en tiempo real, garantizando una gran fiabilidad y extrema baja latencia.

Tipos de despliegue de la red 5G

Desde sus inicios, las redes de comunicaciones celulares han sido diseñadas y gestionadas íntegramente por los operadores de telecomunicación móvil. Estos se han encargado de pagar por licencias de uso de espectro radioeléctrico a través de las subastas públicas, realizadas por los gobiernos de cada país, así como de realizar la planificación, el despliegue y el mantenimiento de la red de acceso y la red core, optimizando su funcionamiento según la demanda de cada zona. Pero gracias a la virtualización de la red y a la capacidad de *slicing*, explicados en el apartado anterior, la tecnología 5G cambia este paradigma y plantea múltiples formas de despliegue¹² según cómo se gestione la red de acceso y la red core. A continuación, vamos a describir dos alternativas posibles desde el punto de vista de una empresa que decide desplegar propia su red de comunicaciones.

Una primera opción es realizar un despliegue 5G donde la red de acceso se comparte entre uso público y uso privado, y la red core es pública, tal como se muestra en la Figura 20. En este modelo, el operador ofrece un servicio privado (NPN, del inglés *Non-Public Network*) a través de una red pública. Una segunda opción consistiría en un despliegue donde la red de acceso y la funcionalidad de la red core son privadas y están aisladas de la red de acceso público, tal como se muestra en la Figura 21. En este caso, el operador de telecomunicación móvil asigna unos recursos de red e instala una réplica de los diferentes equipos de la red de acceso y core en las premisas del cliente.

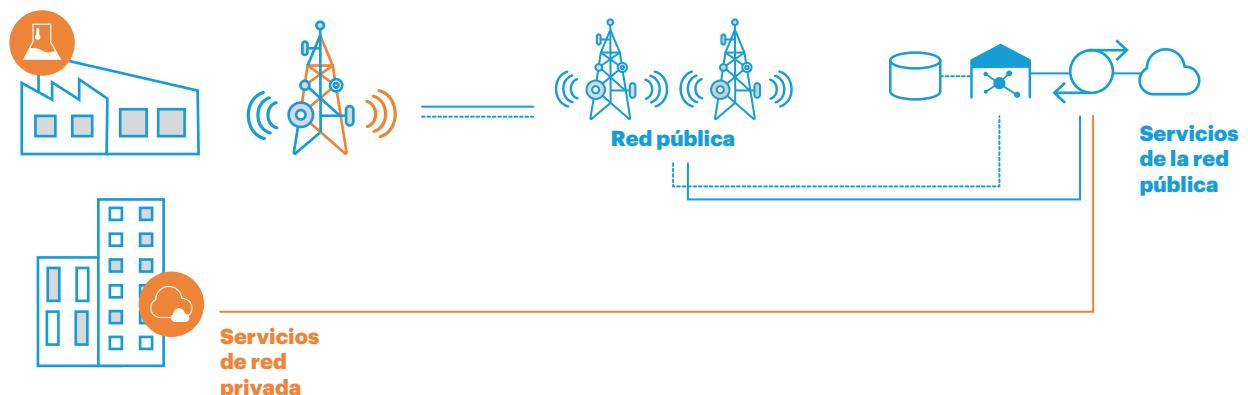
El primer caso es el que resulta más sencillo y tiene un menor coste para la empresa interesada en el servicio, pues el operador de la red móvil es el encargado de realizar el despliegue y la gestión de la red. Por contra, en este tipo de despliegue, el operador puede tener más dificultades para garantizar la calidad del servicio (por ejemplo, ancho de banda, latencia, etc.) ofrecido debido a que los recursos de red son compartidos. Además, también hay que tener en cuenta que los datos generados por los dispositivos de la empresa viajan a través de la red del operador (pública), de modo que no es fácil garantizar la seguridad ni la confidencialidad de los mismos.

En el segundo caso, el operador despliega una réplica de la red de acceso y red core en las instalaciones de la empresa y la conecta directamente a su red corporativa. Lógicamente, esta opción es más costosa debido a los equipos adicionales, pero permite adaptar al máximo las prestaciones de la red a las necesidades del cliente, así como garantizar que los datos que generan los dispositivos de la empresa se mantengan dentro de la misma, ya que la conexión es opcional y pasa por los mecanismos de seguridad de la empresa.

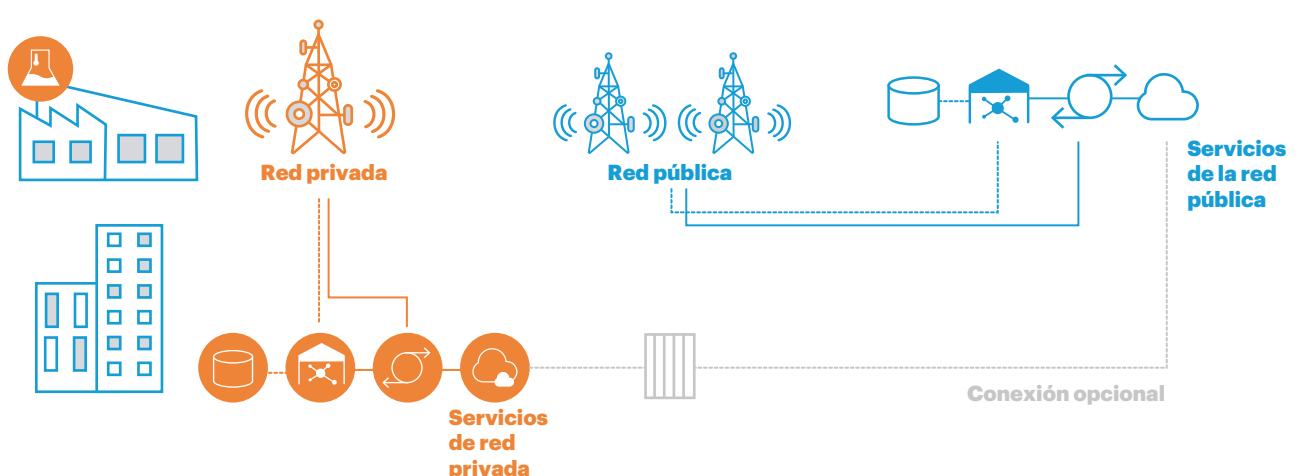
¹² Disponible en el informe de la alianza 5GACIA: https://www.5g-acia.org/fileadmin/5G-ACIA/Publikationen/5G-ACIA_White_Paper_5G_for_Non-Public_Networks_for_Industrial_Scenarios/WP_5G_NPN_2019_01.pdf

Pero gracias a la virtualización de sus elementos y funciones de red, la tecnología 5G permite que existan muchas otras alternativas de despliegue en las que pueden entrar en escena varios operadores móviles de manera simultánea (por ejemplo, unos ofreciendo red de acceso y otros ofreciendo la red core), así como los operadores neutrales, que se ocupan de proveer la infraestructura de red y licenciarla a operadores tradicionales para ofrecer servicios al cliente final. De este modo, la tecnología 5G garantiza mayor competencia en lo que a despliegue y operativa de redes de comunicaciones se refiere, a la vez que mantiene una excelente calidad de los servicios y comunicaciones para los usuarios finales.

NPN implementado en la red pública



Implantación como red aislada



 Infraestructura pública del operador de comunicaciones

 Infraestructura privada de la empresa interesada en el servicio de telecomunicación

Figura 20-21. 5G-ACIA.

Ciberseguridad en la Industria 4.0 y 5G

Introducción a la ciberseguridad en la Industria 4.0

La Industria 4.0 refleja la transformación digital en la industria manufacturera, donde los sistemas ciberfísicos (CPS) se están integrando con componentes físicos y las redes digitales para automatizar procesos e intercambiar información. La introducción de sistemas ciberfísicos, IoT industrial (IIoT), la adopción de computación cognitiva/conductual en la nube y 5G, introducen un nuevo conjunto de desafíos en cuanto a seguridad. Esta hiperconectividad entre dispositivos inteligentes y redes inteligentes prevista por la Industria 4.0 presenta un objetivo atractivo para los cibercriminales, que ahora tienen muchos más puntos de entrada, fáciles e inseguros, en redes y dispositivos.

En la Industria 4.0 existe una gran dependencia entre el flujo de datos y la comunicación entre procesos, componentes y subsistemas. Esta integridad en los datos y sistemas conlleva dimensiones críticas. Supervisar manualmente varios procesos no es factible ni efectivo. Incluso parchear fallos de seguridad de vez en cuando no es práctico, ya que los datos tienen que ser por sí mismos abstractos y seguros a través del uso de diferentes herramientas y técnicas. La práctica más común de seguridad, en la industria manufacturera actual, de tener una red segmentada o completamente desprovista de una conexión a Internet en realidad no se sostiene, como lo demuestra el virus Stuxnet¹³ que, según informaciones, se introdujo en instalaciones «seguras» mediante una memoria USB. Los estándares de seguridad cibernética tienen un papel importante que jugar y los ingenieros de seguridad funcional están comenzando a darse cuenta de que sus sistemas necesitan cumplir unos elevados niveles de seguridad para alcanzar una fiabilidad equivalente a la que tendrían si no estuvieran conectados. Existe un claro desafío para los ingenieros en seguridad, que operan en un mundo determinista, cuando tienen que abordar problemas de ciberseguridad que son inherentemente no deterministas.

Esta nueva ola de ataques cibernéticos contra los CPS ya no se limita a un objetivo aislado, sino que pretenden interrumpir sectores enteros, economías y sistemas políticos. Si un ataque sofisticado como el del malware Triton¹⁴ de 2017, que intentó interferir con el sistema crítico de seguridad de un operador de la fábrica, tuviese éxito, podría representar una seria amenaza para el público y el medio ambiente. Tales ataques a los sistemas de CPS pueden servir como prueba de concepto para ataques más sofisticados y, con múltiples actores peligrosos que se sabe que están investigando métodos similares, parece probable que la aparición y el casi éxito de Triton alentará más incidentes graves.



¹³ <https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html>

¹⁴ https://www.trendmicro.com/vinfo/ph/security/news/cyber-attacks/triton-wielding-its-trident-new-malware-tampering-with-industrial-safety-systems?_ga=2.84375833.1434704139.1571220404-1311567982.1571220404

La Industria 4.0 se postula como el catalizador de la transformación digital en los diferentes sectores críticos como el gobierno, la gestión y administración de ciudades inteligentes y otras aplicaciones. Sin embargo, se enfrenta a un tremendo desafío de seguridad, dadas las tecnologías heterogéneas en las que se basa. En los ataques cibernéticos, ya no es cuestión de «si», sino más bien de «cuándo». Conforme surgen nuevas amenazas técnicas y vectores de ataque, el enfoque de la ciberseguridad se está alejando lenta pero seguramente del enfoque clásico basado en el perímetro, hacia una orientación de 360 grados y, por lo tanto, asegurar la Industria 4.0 requiere un nuevo enfoque holístico.

Panorama de amenazas para la Industria 4.0

La heterogeneidad inherente a la Industria 4.0 hace que su panorama de amenazas (superficie de ataque) aumente exponencialmente. Por ejemplo, se prevé que IIoT sea parte integral de la Industria 4.0, que se estima que tiene miles de millones de dispositivos conectados a Internet y, si algunos de estos dispositivos no están asegurados adecuadamente, los ciberdelincuentes tendrían fácil acceso a la red de IoT y serían capaces de interrumpir los servicios. La superficie de ataque de la Industria 4.0 se puede clasificar principalmente como sigue:

- **Seguridad de los dispositivos:** la tecnología depende de los dispositivos físicos para funcionalidad / procesamiento, recopilación y transmisión de datos. Una vulnerabilidad en un dispositivo puede comprometer toda la red de las cosas conectadas.
- **Privacidad y protección de datos:** la confidencialidad de extremo a extremo de los datos es vulnerable debido a la falta de una arquitectura de seguridad adecuada, especialmente en entornos heterogéneos interconectados, como el de la Industria 4.0. El desafío es garantizar que se mantenga el nivel requerido de privacidad y confidencialidad en las diferentes tecnologías del ecosistema de la Industria 4.0.
- **Riesgo de aplicación:** las aplicaciones proporcionan otra área de superficie para el ataque; los atacantes pueden explotar cualquier debilidad en la seguridad de la aplicación para interrumpir el servicio.
- **Cloud y edge computing:** proporciona la plataforma de procesamiento para dispositivos, almacena una gran cantidad de datos y se conecta de forma remota para lograr la funcionalidad requerida, por lo tanto, la seguridad informática se vuelve crítica.
- **Seguridad de la comunicación (5G):** La Industria 4.0 depende de diferentes redes de comunicación (cableadas e inalámbricas), por lo tanto, las vulnerabilidades colectivas de estas redes representan una amenaza de seguridad para la Industria 4.0.



Figura 22. Industria 4.0 Panorama de seguridad.

Enfoque de ciberseguridad para la Industria 4.0

La superficie de ataque de la Industria 4.0, como se describió anteriormente, es bastante amplia y diversa y requiere de un enfoque integral a varios niveles para garantizar la seguridad. La seguridad cibernética ya no debe verse como una función de la tecnología de la información o la seguridad de la información sola. Debe considerarse como una parte integral de la cultura y la estrategia de la organización. Debe reflejarse en todas y cada una de las facetas de la organización, desde la estrategia hasta el comportamiento de un empleado individual. El consorcio industrial de Internet presentó un informe exhaustivo sobre puntos de vista empresariales, funcionales y de implementación para abordar los desafíos de seguridad y privacidad en IIoT.¹⁵ ENISA (en inglés, *European Network and Information Security Agency*) también presentó un enfoque integral de seguridad cibernética para la Industria 4.0.¹⁶ El enfoque de seguridad se puede clasificar en tres grupos principales; i) Políticas, ii) Prácticas organizativas, y iii) Prácticas técnicas.

Las políticas se refieren a las directivas y procedimientos que establecerá la Industria 4.0 para lograr un alto nivel de ciberseguridad. Estas políticas incluyen seguridad por diseño, privacidad por diseño, gestión de activos, gestión de riesgos y amenazas. Seguridad o privacidad por diseño son un enfoque para desarrollo de software y hardware en el cual seguridad o privacidad se integran desde el principio, y no como una adición tardía a raíz de un incidente de piratería. La necesidad de seguridad o privacidad por diseño se ha vuelto crucial a medida que las compañías tecnológicas continúan produciendo una miríada de objetos de IoT para consumidores y empresas.

Las prácticas organizacionales proveen una guía para las compañías que adoptan tanto *Smart Manufacturing* como las que adoptan modelos vinculados a Industria 4.0, las cuales deben operar entre ellas y con otros miembros de su ecosistema para abordar incidentes de ciberseguridad. Los principios organizacionales deben de tener en cuenta los puntos finales del ciclo de vida, la arquitectura de seguridad, el manejo de incidentes, la gestión de vulnerabilidades, así como la capacitación y gestión de terceros.

Las políticas y prácticas de la organización deben estar respaldadas por fuertes capacidades técnicas de IIoT. Las medidas de seguridad técnicas necesarias para permitir a las empresas de Industria 4.0 y *Smart Manufacturing* mejorar el nivel de seguridad incluyen: gestión de confianza e integridad, seguridad en la nube, continuidad y recuperación del negocio, seguridad de máquina a máquina, protección de datos, actualizaciones de software / firmware, control de acceso, red, protocolos y encriptación, monitorización y auditoría, y gestión de configuración.

Seguir una visión de ciberseguridad tan integrada como la que propone ENISA, alinea las funciones comerciales de las organizaciones con las necesidades de las partes interesadas, a la vez que tener en consideración los puntos fuertes de las capacidades técnicas constituye una buena estrategia de ciberseguridad para abordar los desafíos de seguridad en la Industria 4.0.

¹⁵ https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

¹⁶ <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot>

Seguridad de las comunicaciones 5G

La Industria 4.0 requiere un sistema de comunicación seguro y resistente en su red troncal para cumplir con la promesa de una hiperconectividad de confianza entre los miles de millones de dispositivos conectados. La tecnología 5G (redes móviles de próxima generación) parece un encaje natural para la Industria 4.0, ya que las comunicaciones masivas de máquina a máquina y la comunicación ultra segura de baja latencia son algunos de sus principales casos de uso, como hemos ido desgranando en este documento. La tecnología 5G abarca la convergencia de múltiples tecnologías heterogéneas y, como resultado, tiene una superficie de ataque sin precedentes, como se identificó en la subsección anterior. Sin embargo, una gran ventaja de 5G, en comparación con su predecesor (4G), es el enfoque holístico para la seguridad. El enfoque de seguridad 5G no solo se focaliza en partes individuales de forma aislada, sino que también considera los principales riesgos y su rectificación apropiada, al analizar el alcance del daño de una amenaza en comparación con el costo de su remediación.

Como hemos visto antes, la organización encargada de definir la tecnología 5G a nivel de red de acceso y red principal es la 3GPP. Pero existen otras organizaciones internacionales dedicadas a la estandarización que complementan el funcionamiento de la tecnología 5G a otros niveles, como es el caso de la ETSI y la IETF (en inglés, *Internet Engineering Task Force*). Cada uno de estos organismos considera a fondo la seguridad bajo su alcance específico, así como desde un punto de vista de extremo a extremo del sistema 5G. Por ejemplo, el grupo de trabajo 3GPP SA3 produjo el estándar de seguridad 5G R15¹⁷ en 2018, definiendo arquitecturas y estándares de seguridad para escenarios eMBB, que cubren arquitecturas independientes (SA) y no independientes (NSA). Basado en la arquitectura de seguridad 5G R15, los estándares 5G R16 y R17 cubrirán la optimización de seguridad para escenarios mMTC y URLLC.

5G es inherentemente diferente de cualquiera de sus predecesores y ofrece medidas de seguridad mejoradas, algunas de las relevantes para las redes 3GPP se enumeran a continuación:

- **Mayor seguridad de la interfaz radio:** para evitar la manipulación de datos del usuario, los estándares 5G brindan protección adaptativa de la integridad de los datos del usuario además del cifrado de datos de extremo a extremo.
- **Privacidad del usuario mejorada:** a diferencia de su predecesora, la red 4G, la información de identificación del usuario, las identidades internacionales de suscriptor móvil (IMSI), no se transmiten en texto plano, sino que se encriptan en la interfaz radio.
- **Marco de autenticación mejorado:** el procedimiento de autenticación de acceso 5G está diseñado para admitir el protocolo de autenticación extensible (EAP) especificado por el IETF. EAP acepta diferentes tipos de credenciales y, por lo tanto, es clave para diversos casos de uso de 5G.

¹⁷ <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169>

- **Seguridad de roaming mejorada:** la arquitectura basada en servicios (SBA) 5G define el proxy de protección de borde de seguridad (SEPP) para implementar la protección de seguridad E2E para la señalización entre operadores a nivel de transporte y aplicación. Esto impide que los dispositivos de operadores terceros puedan tener acceso a datos confidenciales como claves, ID de usuario y SMS, intercambiados entre redes centrales.

Las mejoras de seguridad mencionadas anteriormente y otras, junto con el inherente enfoque de seguridad holístico, permiten a 5G cumplir con los diversos requisitos de seguridad de los diferentes sectores verticales, como la Industria 4.0.



4

Aplicaciones representativas de 5G en el ámbito industrial

En este apartado se exponen diversos escenarios de implementación de los casos de uso expuestos en el apartado 1.3, combinando los conceptos introducidos en este documento respecto a la Industria 4.0 y las comunicaciones 5G.

La fábrica flexible basada en AGV

Para ilustrar la implementación de este caso de uso, vamos a contemplar dos escenarios de aplicación de los sistemas AGV, ambos en el contexto de un polígono industrial, tal como se muestra en la Figura 23. El primer escenario (izquierda) corresponde a una planta de grandes dimensiones de una empresa multinacional, mientras que el segundo (derecha) corresponde con dos plantas colindantes de pymes (pequeñas y medianas empresas) independientes.

En el caso de la multinacional, esta dispone de una gran cantidad de AGV (miles) que deben cubrir una gran superficie. Además, los diferentes AGV transmiten una gran cantidad de información y deben estar coordinados en tiempo real. Finalmente, por política de seguridad de la empresa, se requiere que toda la información generada por los AGV se mantenga dentro de la red corporativa. Así pues, en este caso se opta por realizar el despliegue de una red 5G privada, que permite conectar directamente los AGV con los sistemas de información de la empresa, garantizando las propiedades antes descritas.

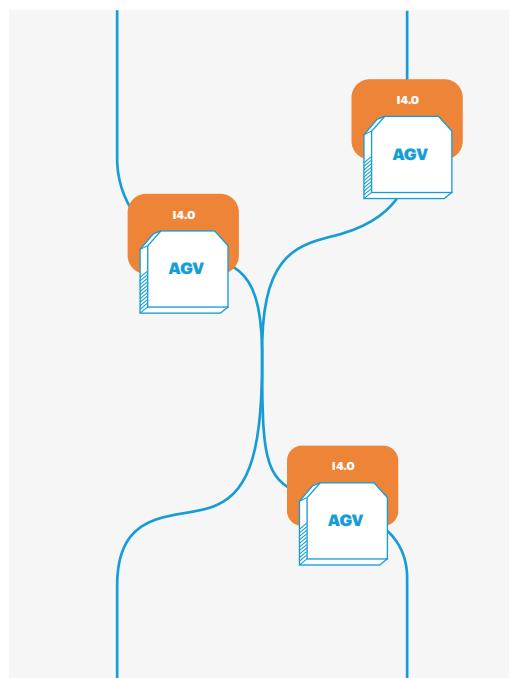
En cambio, para el caso de las pymes el parámetro a optimizar es la facilidad de despliegue y el coste del servicio, por lo que se utilizará la red 5G pública. De este modo cada pyme podrá contratar cualquiera de los operadores móvil que presten el servicio 5G en el polígono utilizando la infraestructura de red y computación compartidas gracias a las capacidades de slicing y virtualización. Es importante destacar que esta elección no irá en detrimento de las capacidades de comunicación de la red, ya que será cada operadora la encargada de optimizar su funcionamiento para prestar el servicio adecuado.



Despliegue de un sistema AGV basado en red 5G privada



Estación base
de uso privado

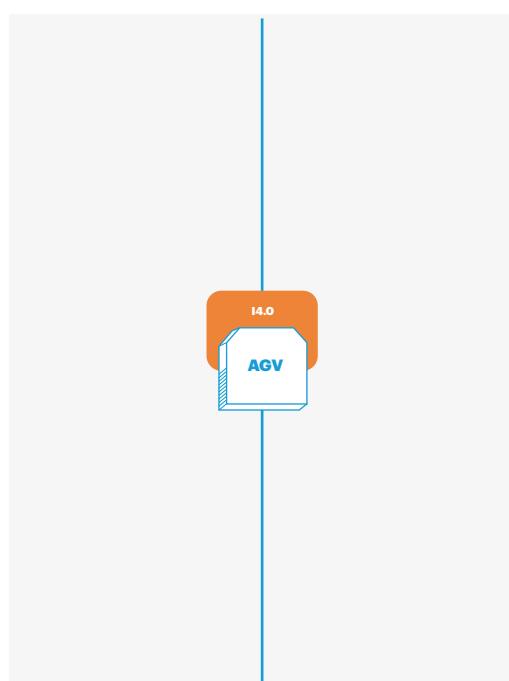


Planta empresa X

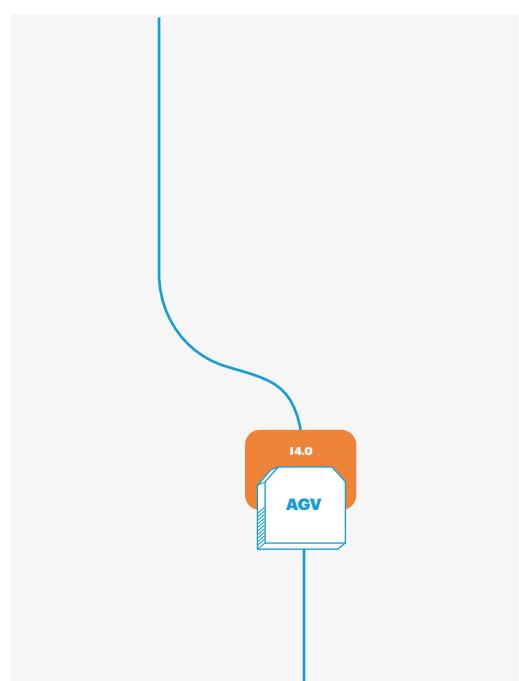
Red público-privada



Estación base
de uso público/
privado



Planta empresa Y



Planta empresa Z

Figura 23. Despliegue de un sistema AGV basado en red 5G privada (izquierda) y red público-privada (derecha).

Una variante del escenario propuesto es el caso en que dos pymes tuvieran que cooperar muy estrechamente para realizar un proceso coordinado, por ejemplo, que los AGV de cada una de ellas tuvieran que circular por ambas plantas. En este caso, las empresas podrían optar por un servicio privado desplegado de manera conjunta (igual que en el caso de la empresa multinacional), o bien que ambas empresas utilizaran el mismo operador de la red 5G para facilitar el intercambio de datos y minimizar la latencia de las comunicaciones.

Por último, también se puede dar el caso de una empresa pyme que requiera incrementar o disminuir su capacidad productiva en función de la demanda puntual. Hasta ahora la conectividad de las máquinas era un factor limitante, ya que requería de un proceso propio de planificación y despliegue, con el tiempo y los costes asociados. En cambio, gracias a la llegada de la tecnología 5G, la conectividad móvil pasará a ser un servicio ubicuo y fácilmente accesible, lo que facilitará el despliegue de nuevas actividades y flexibilizará el ajuste de las existentes.



Control de calidad inteligente

Supongamos un sistema dotado de la capacidad de controlar de forma inteligente la calidad de los productos fabricados, así como la calidad de los propios procesos de fabricación.

El control de calidad de la producción se basa en el análisis de imágenes de los productos realizado mediante un sistema de visión artificial, para el cual se utiliza el sistema mostrado en la Figura 24. La máquina dispone de un sistema de visión artificial que identifica defectos de fabricación. Para ello, debe ser previamente entrenada. El controlador edge del aprendizaje gestiona los modelos entrenados, los cuales pueden ser ejecutados por él mismo o por un procesador de la propia máquina. Por otra parte, el controlador de aprendizaje gestiona los juegos de datos de entrenamiento, los envía al *cloud* y recoge los sistemas entrenados.

Para transferir juegos de datos de entrenamiento de gran volumen, se precisará de prestaciones eMBB (ancho de banda elevado). Si el sistema entrenado se ejecuta en el controlador edge del aprendizaje, serán necesarias prestaciones uRLLC (baja latencia) para que la máquina pueda reaccionar en tiempo real.

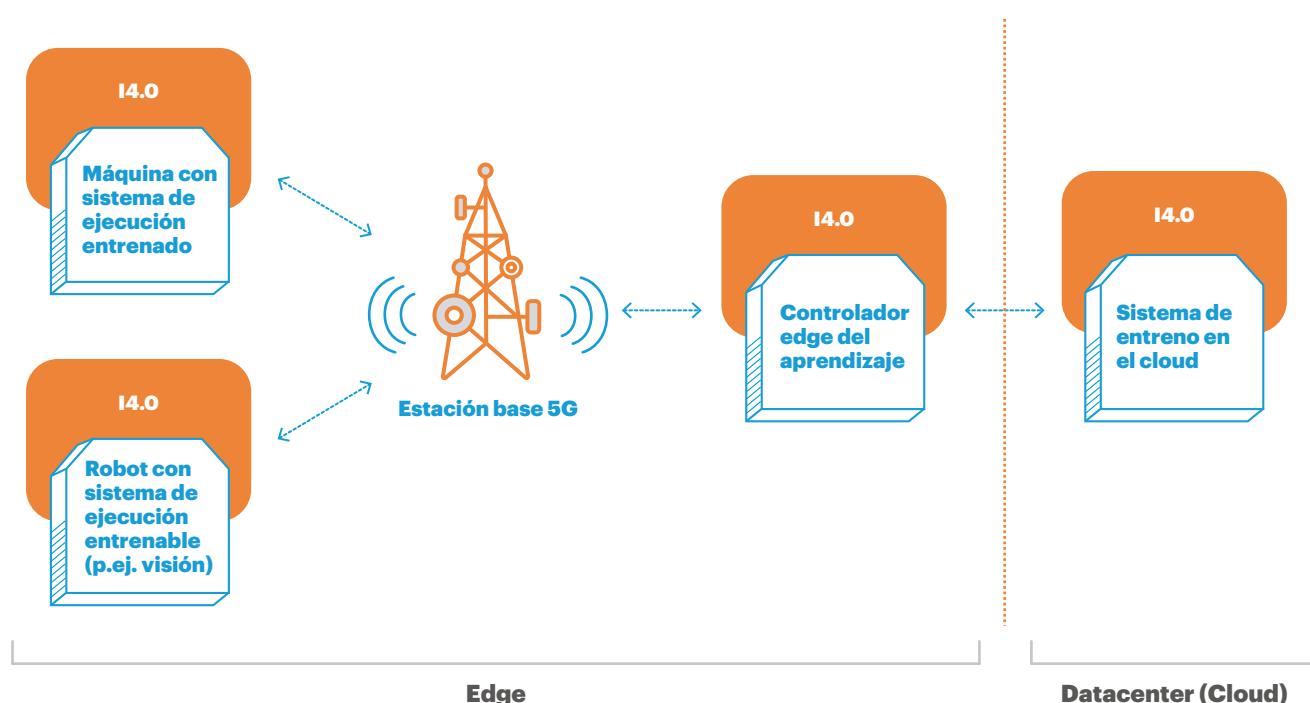


Figura 24. Despliegue con 5G de sistemas ciberfísicos con machine learning.

La implementación del sistema APC se basa en la ejecución de modelos de simulación, que en general requerirá prestaciones en el cloud y no en el edge. No obstante, puede requerir sistemas de visualización de alta calidad, y en el límite de realidad virtual, pudiendo requerir eMBB.

Por otra parte, el sistema de SPS requiere el acceso al DS, el cual puede estar alimentado por miles de sensores, lo que puede requerir mMTC (alta densidad).

Finalmente, los sistemas de asistencia técnica de campo basados en realidad aumentada pueden requerir eMBB si se utilizan imágenes de alta calidad. La situación es similar si se quieren utilizar sistemas de formación inmersiva basados en realidad virtual, los cuales pueden requerir eMBB y uRLLC.



Conclusiones

Tal como hemos explicado desde el punto de vista técnico en este documento, la tecnología 5G es algo más que una nueva generación de comunicaciones inalámbricas, que abre un amplio abanico de servicios que sobrepasa la visión para el gran público, basada en el incremento de velocidad de descarga. Para la Industria 4.0, el 5G es el catalizador tecnológico que permite alcanzar atributos impensables hasta ahora como: adaptabilidad, resiliencia, capacidad de proceso, bajas latencias y seguridad. No quiere decir que tecnologías anteriores no dispongan de estos atributos, pero ahora cobran una nueva dimensión que puede actuar como generador de confianza para el impulso definitivo de la Industria 4.0.

Por lo tanto, el desarrollo de la tecnología 5G, que todavía requerirá de algunos años para mostrar todo su potencial, puede actuar como elemento que acelere la adopción de la Industria 4.0 y favorezca el desarrollo de una cultura digital, pero puede actuar también de freno si no se ofrece a precios competitivos. En este sentido, resulta imprescindible que las subastas públicas del espectro 5G garanticen los ingresos adecuados a los estados, pero permitan a los operadores ofrecer los servicios a precios razonables.

Uno de los objetivos fundamentales de la Industria 4.0 es lograr la flexibilidad tanto en los productos como en el proceso de fabricación. Al mismo tiempo, una de las características principales que ofrece la tecnología de comunicaciones 5G es, precisamente, la flexibilidad.

Además, tanto la Industria 4.0 como la tecnología de comunicaciones 5G realizan una apuesta estratégica por el concepto de virtualización. Los nuevos sistemas de producción flexibles, basados en elementos móviles, robotizados y conectados, podrán desplegarse en tiempos reducidos en espacios articulados en polígonos industriales equipados con 5G, los cuales permitirán la adaptación de los sistemas productivos y su capacidad a la demanda de los mercados prácticamente en tiempo real.

Para garantizar el correcto funcionamiento de las comunicaciones inalámbricas implicadas, el espacio radioeléctrico asignado a 5G será custodiado por operadoras de telecomunicaciones, donde los equipos conectados estarán identificados con su correspondiente tarjeta SIM formando parte de una red gestionada por equipos humanos altamente especializados, para garantizar su fiabilidad y su seguridad.



Glosario

Diversas organizaciones juegan un papel importante en la estructuración del discurso, tanto de la Industria 4.0 como de 5G, las cuales se relacionan en la siguiente lista:

3GPP: (3rd Generation Partnership Project). Organización que elabora estándares para la telefonía móvil, integrado en el ETSI.

5GACIA: (5G Alliance for Connected Industries and Automation). Alianza de las industrias conectadas y automatización para el 5G, creada por la industria alemana.

ACATECH: Academia de las ciencias y la ingeniería alemana.

CNAF: (Cuadro Nacional de Asignación de Frecuencias). Instrumento legal, dependiente del Ministerio de Industria, Energía y Turismo de España, utilizado para asignar a los distintos servicios de radiocomunicaciones las diferentes bandas de frecuencias.

ENISA: (European Union Agency for Cybersecurity). Agencia europea focalizada en seguridad informática, cuya denominación original era European Network and Information Security Agency.

ETSI: (European Telecommunications Standards Institute). Organismo internacional europeo independiente y sin ánimo de lucro de estandarización de sistemas de telecomunicaciones.

GSMA: (Global System for Mobile Communications Association). Asociación global de los operadores de telecomunicaciones.

IEEE: (Institute of Electrical and Electronics Engineers). Asociación profesional global de ingenieros eléctricos y electrónicos. Fundada en 1963, es la más importante del mundo en su campo.

IETF: (Internet Engineering Task Force). Organización que promueve y desarrolla estándares abiertos relacionados con las tecnologías de Internet como el TCP/IP.

IIC: (Industrial Internet Consortium). Consorcio internacional de origen norteamericano de empresas y organizaciones para desarrollar e impulsar la Internet industrial de las cosas.

ITU: (International Telecommunication Union). Agencia de Naciones Unidas focalizada en lo relativo a las telecomunicaciones. Fundada en 1865, es la organización internacional global más antigua del mundo.

OPC Foundation: (Open Platform Communications Foundation). Organización de estandarización de comunicaciones para sistemas de automatización como OPC-UA.

Plattform Industrie 4.0: Organización de origen alemán constituida por empresas, sindicatos, asociaciones profesionales, mundo académico y administración pública que tiene por objetivo estandarizar y difundir la Industria 4.0.



