Internet de la Cosas. Aplicaciones, Tecnologías y Seguridad.

Autor: Pablo Hallado Medina

Tutor: Amadeus Albos.

Profesor:

Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones

Grado en Ingeniería Informática

Fecha de entrega

El presente cuadro de texto tiene solamente finalidades informativas y no tiene que ser incluido en la memoria del estudiante. Asimismo, esta página tampoco tiene que ser incluida.

SOBRE LOS CONTENIDOS DE ESTE DOCUMENTO

Este documento incluye estilos predeterminados de texto, ejemplos de citas bibliográficas, notas a pie de página e inserción de figuras (imágenes y gráficos) y tablas, así como sección de bibliografía e índices automatizados listos para usar.

SOBRE LOS CAPÍTULOS DE ESTE DOCUMENTO

Aquellos apartados (i.e. capítulos, apartados, subapartados, etc.) con el título en color negro son obligatorios para todos los TFP, mientras que aquellos en color gris son opcionales, es decir, susceptibles de ser incluidos en la memoria según el tipo de TFP realizado. Es recomendable adaptar el orden de los capítulos a la naturaleza del TFP a realizar, e incluso combinar dos o más capítulos en uno si se considera oportuno.

Tened en cuenta que el número máximo de páginas que puede tener la memoria es 90, incluyendo anexos y bibliografía.

Créditos/Copyright

Una página con la especificación de créditos/copyright para el proyecto (ya sea aplicación por un lado y documentación por el otro, o unificadamente), así como la del uso de marcas, productos o servicios de terceros (incluidos códigos fuente). Si una persona diferente al autor colaboró en el proyecto, tiene que quedar explicitada su identidad y qué hizo.

A continuación, se ejemplifica el caso más habitual y una lista de posibles alternativas:

Esta obra está sujeta a una licencia de Reconocimiento- NoComercial-SinObraDerivada 3.0 España de CreativeCommons.

Licencias alternativas (elegir alguna de las siguientes y sustituir la licencia anterior)

A) CreativeCommons:

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial - SinObraDerivada 3.0 España de CreativeCommons.

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial- CompartirIgual 3.0 España de CreativeCommons.

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial. 3.0 España de CreativeCommons.

Esta obra está sujeta a una licencia de Reconocimiento- SinObraDerivada 3.0 España de CreativeCommons.

B) GNU Free Documentation License (GNU FDL)

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Internet de las Cosas. Aplicaciones y Seguridad*
Nombre del autor:	*Pablo Hallado Medina*
Nombre del colaborador/a docente:	*Amadeus Albos Raya*
Nombre del PRA:	*Nombre y dos apellidos*
Fecha de entrega (mm/aaaa):	*12/2019*
Titulación o programa:	*MISTIC*
Área del Trabajo Final:	*TFM*
Idioma del trabajo:	*Español*
Palabras clave	*IoT, Seguridad, IIoT*

Resumen del Trabajo (máximo 250 palabras):

El avance del IoT en los últimos tiempos ha sido imparable abarcando un amplio espectro de entornos de aplicación, desde la domótica domestica más sencilla, como puede ser una bombilla, hasta el control de grandes plantas industriales de todo tipo. Este gran avance ha traído consigo no solo la posibilidad de tener control e información en tiempo real de los que antes no se disponía, sino que también una serie de nuevos problemas de seguridad y privacidad específicos de estos entornos.

Las peculiares características de estos dispositivos, sus diferentes localizaciones fuera de los tradicionales centros de datos y la gran variedad de fabricantes hace que la seguridad de IoT presente un gran reto para los actuales departamentos de IT de las empresas.

Los ciberataques que han sufrido grandes empresas en los últimos tiempos han puesto el foco en la seguridad, provocando la reacción de estas y el incremento de manera significativa de los recursos, tanto económicos como de personal, de cara a fortalecer sus sistemas ante estos ataques.

A lo largo de este TFM daremos un repaso al mundo IoT, desde sus orígenes hasta su estado actual, poniendo el foco en aquellos riegos de seguridad, las medidas de que se pueden tomar y como mediante el uso de nuevos enfoques podemos dar solución a este heterogéneo entorno.

Abstract (in English, 250 words or less):

The progress of the IoT in recent times has been unstoppable covering a wide spectrum of application environments, from the simplest home automation, such as a light bulb, to the control of large industrial plants of all kinds. This breakthrough has brought not only the possibility of having real-time control and information that was not available before, but also a series of new security and privacy issues specific to these environments.

The peculiar characteristics of these devices, their different locations outside the traditional data centers and the great variety of manufacturers makes IoT security a great challenge for the current IT departments of the companies.

The cyberattacks that have suffered large companies in recent times have put the focus on security, causing their reaction and the significant increase in resources, both economic and personal, in order to strengthen their systems in the face of these attacks.

Throughout this TFM we will review the IoT world, from its origins to its current state, putting the focus on those security risks, the measures that can be taken and how through the use of new approaches we can solve this heterogeneous environment.

Índice

Figuras y tablas

Índice de figuras

1. Introducción

1.1. Introducción/Prefacio

Actualmente hay millones de dispositivos de IoT que recopilan todo tipo de información tanto en entornos particulares como industriales. Esta información debe ser analizada para comprobar si podemos extraer de ella resultados que puedan ser de utilizad para la persona que los van a consumir.

IoT se ha extendido en diferentes áreas como el mundo de la salud, los deportes, las ciudades inteligentes, la domótica, la automoción, etc. Su éxito radica en que sus principales características como son la recogida de datos, el procesamiento y su análisis pueden ser realizados desde cualquier lugar, siendo habitual su realización desde plataformas cloud.

El flujo de información se inicia en el elemento IoT que recopila la información hasta el servicio encargado del procesamiento de esta información llegando, finalmente, al usuario final que realiza la explotación de la misma.

La disponibilidad de esta información desde cualquier sitio hace a la misma vulnerable a diferentes amenazas de seguridad y a ataques. Durante este TFM trataremos acerca de cuáles son los principales problemas, retos y soluciones de seguridad aplicables a los entornos de IoT como de IIoT.

Figura 1 – Ecosistema IoT

1.2. Descripción/Definición

Con el gran avance de los ecosistemas de IoT que vemos en la actualidad, tenemos que hacernos la pregunta de si sabemos realmente que son y para que se utilizan estos nuevos dispositivos, así como ver de qué manera nos pueden ser útiles tanto a nivel particular como empresarial.

A lo largo de este TFM intentamos dar a conocer más en profundidad los principales componentes que conforman este nuevo ecosistema, centrándonos fundamentalmente en cuales son los retos en términos de seguridad a los cuales se enfrentan y como mediante el diseño de arquitecturas seguras podemos mitigar los riesgos existentes.

En lo que respecta a IIoT veremos cuáles son sus principales diferencias con un entorno de IoT, sus principales áreas de aplicación, su estructura, los mecanismos de seguridad a aplicar y crearemos una prueba de concepto de un entorno industrial en el que podamos ver los distintos elementos en funcionamiento.

1.3. Objetivos generales

A continuación, se detallan los objetivos que se persiguen en este trabajo.

1.3.1. Objetivos principales

Objetivos de la redacción del trabajo:

- Definir los principales elementos que componen IoT.
- Conocer los riesgos a nivel de seguridad que presenta este entorno.
- Definir las medidas de seguridad a aplicar para maximizar la seguridad.
- Aplicar de IoT en entornos industriales.
- Integrar plataformas de IoT con los servicios cloud.

Objetivos personales del autor del TF:

- Conocer el mundo de IoT y sus aplicaciones.
- Conocer las aplicaciones en entorno industriales para su aplicación en el entorno laboral.
- Conocer la interacción de los dispositivos IoT con el mundo cloud.
- Conocer cómo se segurizan de entornos IoT.

1.3.2. Objetivos secundarios

Objetivos adicionales que enriquecen el TF.

- Despliegue de una plataforma de IIoT en una plataforma cloud.
- Finalización de Master.

1.4. Metodología y proceso de trabajo

A lo largo de este trabajo la metodología que se utilizara en la realización de este TFM está compuesta por las siguientes tareas:

Tarea 1: Definición del ámbito del Proyecto. – El primer paso consiste en el establecimiento del ámbito del Proyecto y la selección de los recursos que son considerados importantes para el desarrollo del trabajo.

Tarea 2: Búsqueda de información – Durante este paso se realizará una búsqueda extensa de aquellos documentos relevantes en el contexto que el trabajo ha sido definido. Las fuentes identificadas servirán como referencia para el desarrollo de los puntos que se tratarán en el trabajo.

Tarea 3: Análisis del material recogido y desarrollo del trabajo – Los documentos recogidos en el punto anterior servirán para la redacción de trabajo.

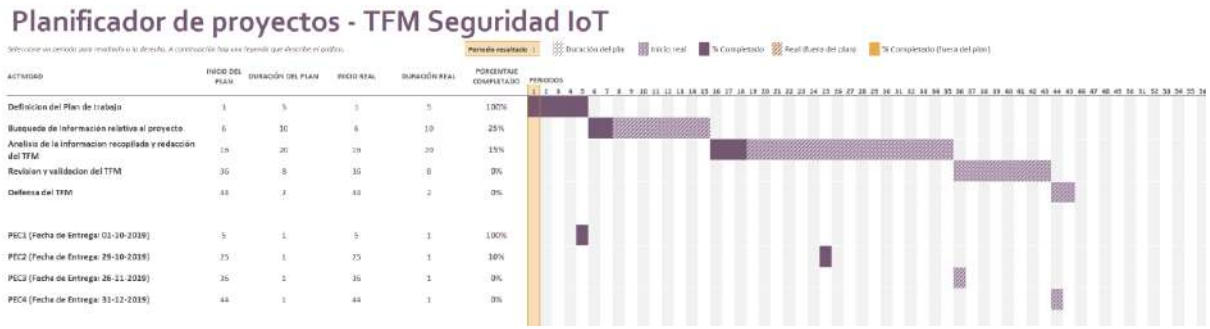
Tarea 4: Revisión y validación del trabajo: Una vez que el trabajo esté redactado se remitirá al tutor del mismo para la obtención de sus opiniones y comentarios.

El uso de esta metodología permite destacar aspectos de interés en el tema tratado y que puede resultar de interés a aquellas personas interesadas en el tema desarrollado, entre los que podemos destacar:

- Definición de la terminología (IoT, IIoT, por ejemplo)
- Activos implicados en los aspectos de seguridad
- Identificar los posibles riesgos, las amenazas y los escenarios de ataque que puedan sufrir los entornos de IoT / IIoT.
- Lista de las medidas de seguridad relacionadas con el uso de IoT en los entornos industriales.

1.5. Planificación

A continuación, se muestra en un diagrama de Gantt la planificación estimada para la realización de este trabajo.



Se han agregado las referencias relativas a cada una de las entregas a realizar en la plataforma online de la universidad.

1.6. Estructura del documento

El trabajo estará compuesto por los siguientes capítulos:

Capítulo 2 – Introducción al mundo IoT. Orígenes y Aplicaciones.

Capítulo 3 – IoT. Seguridad en IoT. Riesgos y Retos.

Capítulo 4 – IoT. Elementos de una Arquitectura.

Capítulo 5 – IoT. Arquitecturas y seguridad en entornos industriales.

Capítulo 6 – Ejemplo de planta conectada.

Capítulo 7 – IoT. Despliegue de un modelo conceptual de IIoT en cloud.

Capítulo 8 - Nuevos enfoques de la seguridad. SDP. ZeroTrust. Azure Sphere.

Capítulo 9 – Conclusiones.

Capítulo 10 – Bibliografía y fuentes consultadas.

1.7. Estado del arte

La definición de IoT hace referencia a aquellos dispositivos que están conectados a internet de manera permanente, como puede ser un teléfono móvil o un reloj inteligente, pero actualmente también podemos englobar dentro de la misma objetos que hasta hace poco tiempo no disponían de esa conectividad.

Dentro de esta nueva categoría se encuentran televisores, lavadoras, coches, enchufes, etc. los cuales disponen de una conexión a Internet.

Pero no solo es en el ámbito doméstico donde estos nuevos dispositivos están comenzando a tener un gran auge. Los entornos industriales están comenzando a utilizarlos para recopilar información acerca del funcionamiento de sus máquinas de manera que puedan utilizar los datos recopilados de la misma para, por ejemplo, predecir posibles averías o ajustar los periodos de mantenimiento de determinados elementos de manera que puedan maximizar su duración.

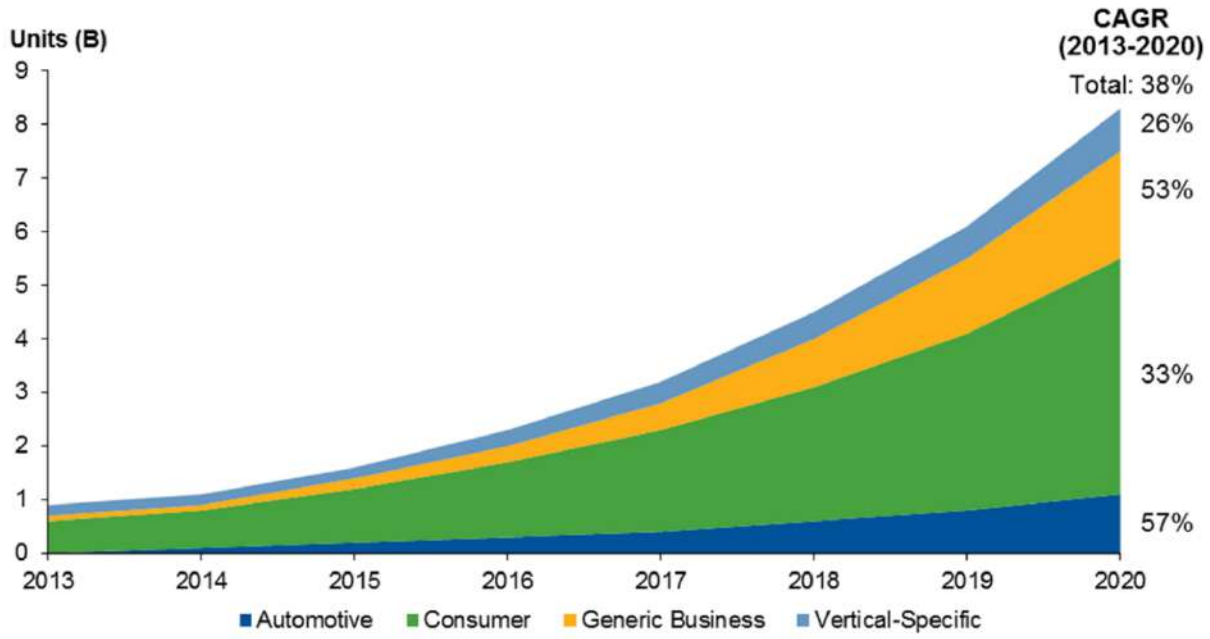


Figura 2 – Evolución de los IoT en los últimos años

Como en todo sistema informático, y más en la actualidad, la seguridad es un factor que cada vez es de una mayor importancia. Aunque podamos pensar inicialmente que estos dispositivos no tienen una funciona critica imaginemos, por ejemplo, que un intruso pudiera tomar el control de los sensores que controlan el funcionamiento de una maquina critica dentro de un proceso productivo. Esto podría provocar graves pérdidas económicas e incluso de seguridad para el consumidor final en función de la actividad de la empresa.

Hay diversos informes que indican que un alto porcentaje de estos dispositivos tienen fallos en los sistemas de control de acceso y también sufren problemas de seguridad en sus interfaces de acceso.

Mediante el uso de un buscador como *Shodan*, el cual está diseñado para la búsqueda en Internet de dispositivos conectados como pueden ser cámaras de seguridad, podemos encontrar muchos dispositivos los cuales suelen disponer de un servicio http para su gestión, el cual está configurado con un usuario y contraseña tan simples como Admin y 1234.

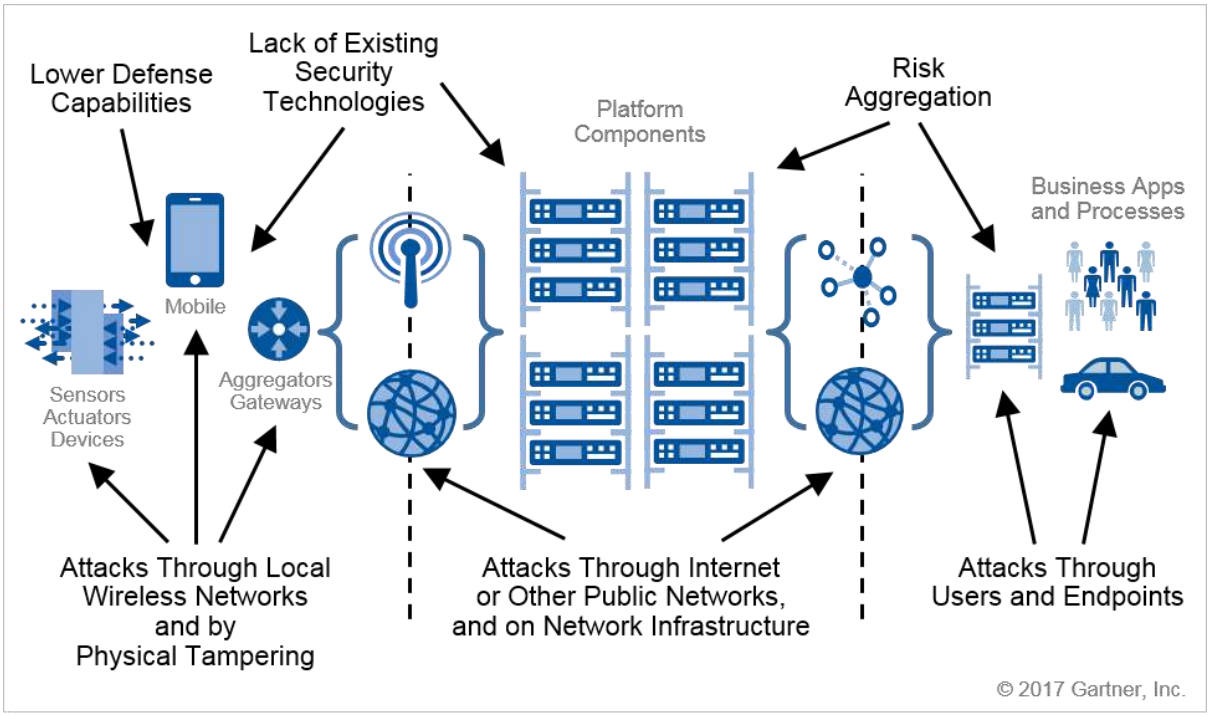


Figura 3 – Riesgos de Seguridad en IoT

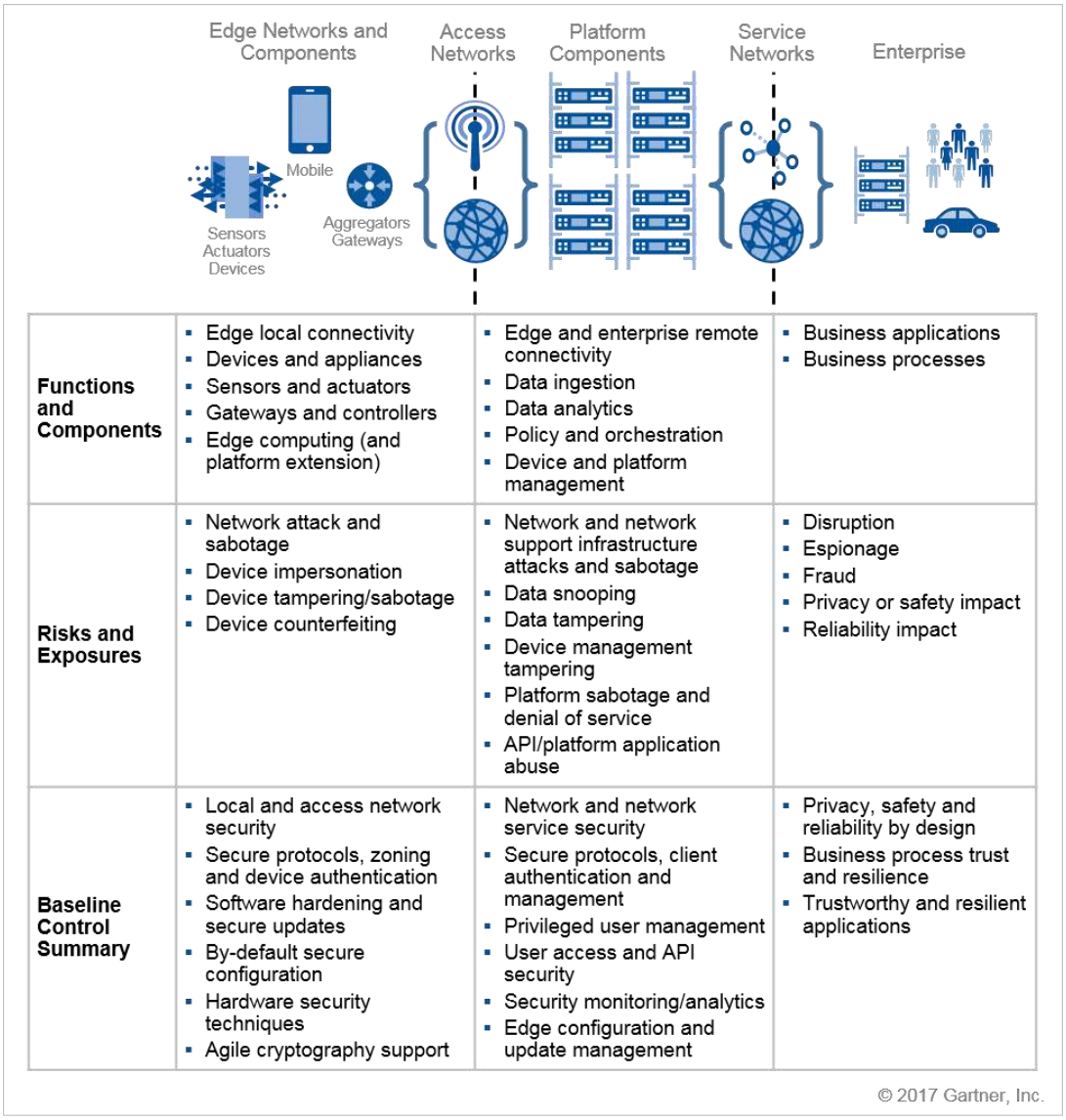
El crecimiento de los dispositivos IoT y el alto grado de interconexión entre los mismos les convierte en un objetivo muy atractivo para los hackers. La cantidad de malware existente junto a la diversidad en los tipos de vectores de ataque que pueden sufrir obliga a tener en cuenta diferentes aspectos de manera que podamos protegerlos de una manera segura. Entre los vectores de ataque que existen podemos destacar:

- Ataque por fuerza bruta.
- Ataques por denegación de servicio.
- Utilización como plataforma de ataque hacia otros dispositivos.
- Obtención de datos de carácter personal de los usuarios.

Aunque a alto nivel, la seguridad en IoT desde un punto de vista técnico no difiere de otras áreas dentro de una empresa, las compañías pueden mejorar ampliamente la seguridad de sus soluciones de IoT en las siguientes áreas:

- Inseguridad en el software, la configuración y la autenticación en los dispositivos edge.
- Seguridad insuficiente en las redes edge y de acceso.
- Carencia de privacidad, Seguridad y fiabilidad.

Es importante la creación de patrones y pruebas de cara a identificar los controles a aplicar y establecer los niveles de riesgos asociados.



Functions and Components	▪ Edge local connectivity ▪ Devices and appliances ▪ Sensors and actuators ▪ Gateways and controllers ▪ Edge computing (and platform extension)	▪ Edge and enterprise remote connectivity ▪ Data ingestion ▪ Data analytics ▪ Policy and orchestration ▪ Device and platform management	▪ Business applications ▪ Business processes
Risks and Exposures	▪ Network attack and sabotage ▪ Device impersonation ▪ Device tampering/sabotage ▪ Device counterfeiting	▪ Network and network support infrastructure attacks and sabotage ▪ Data snooping ▪ Data tampering ▪ Device management tampering ▪ Platform sabotage and denial of service ▪ API/platform application abuse	▪ Disruption ▪ Espionage ▪ Fraud ▪ Privacy or safety impact ▪ Reliability impact
Baseline Control Summary	▪ Local and access network security ▪ Secure protocols, zoning and device authentication ▪ Software hardening and secure updates ▪ By-default secure configuration ▪ Hardware security techniques ▪ Agile cryptography support	▪ Network and network service security ▪ Secure protocols, client authentication and management ▪ Privileged user management ▪ User access and API security ▪ Security monitoring/analytics ▪ Edge configuration and update management	▪ Privacy, safety and reliability by design ▪ Business process trust and resilience ▪ Trustworthy and resilient applications

Figura 4 – Áreas de IoT, Riesgos y Controles de Mitigación

Por todo lo anterior es de vital importancia comprender los riegos y aplicar las medidas apropiadas para que estos potenciales peligros no afecten a las infraestructuras de IoT / IIoT que despleguemos en nuestro entorno.

2. IoT. Antecedentes. Definición y Aplicaciones

En los últimos años, el mundo de IoT se ha convertido en un tópico viral en el mundo digital, el cual ha sido discutido, debatido y analizado en multitud de diferentes contextos. Esto es normal cuando se trata de nuevas tecnologías. Expertos en las distintas áreas, como desarrolladores, arquitectos, etc., debaten acerca de las capacidades e impacto de estas nuevas tecnologías en los diferentes congresos, blogs, y medios especializados. Podemos pensar en ejemplos recientes como Dockers y Kubernetes, los cuales están cambiando la forma en la que se diseñan, implementas y despliegan las

aplicaciones. Están teniendo un gran impacto en el mundo digital en diferentes aspectos, como el ciclo de vida del software, capacidades y coste. A pesar de esto, permanecen dentro de sus campos especializados, lo cual no es el caso de IoT.

Esto es así debido a que IoT no es solo una tecnología que impacta a un grupo determinado de personas, sino que nos impacta a todos nosotros, lo cual cambiara y creara nuevos mercados. El mundo de IoT está cambiando nuestras vidas y las percepciones que tenemos del mundo físico, cambiando la forma en la que interactuamos con él. El desarrollo de las tecnologías de IoT es un momento crucial de en nuestro mundo debido a que está contribuyendo a cambiar la formas en la que pensamos, nuestra cultura y la forma en la que vivimos. La era de IoT no va a ser una transición instantánea, sino que será gradual a lo largo de los próximos años.

A día de hoy nos encontramos en el principio de este cambio, pero el cual ya ha empezado. Estamos avanzando hacia un mundo en el que interactuaremos no con objetos físicos sino con sus imágenes digitales que residen en el cloud y se comunican con otras imágenes, dotadas de inteligencia artificial, lo que las dota de nuevas capacidades, como por ejemplo la sugerencia de acciones, la toma de decisiones autónomas o proporcionar nuevos servicios.

Actualmente podemos regular la temperatura de nuestro sistema de calefacción de manera remota, pero si estuviera en el cloud podría recibir información adicional de otras fuentes, como nuestro coche, el calendario, nuestra posición y el tiempo, podría regular la temperatura de manera autónoma. Es esta interacción con otras imágenes en el cloud lo que convierte a un objeto en un objeto inteligente.

Aunque estos avances puedan ser vistos como un avance hacia un mundo perfecto, también tiene sus inconvenientes. Hay gran cantidad de información almacenada en el cloud acerca de nosotros, la cual puede ser utilizada no solo para mejorar nuestras vidas, sino también para fines maliciosos como influencias políticas y económicas a gran escala.

La historia de la tecnología ha demostrado que la tecnología no es buena o mala en sí misma, si no que esto viene dado por el uso que los humanos hacemos de la misma, lo cual también es aplicable al mundo de IoT.

2.1. Historia y definición

Fue durante el año 1999 cuando fue utilizado por primera vez el concepto de IoT. Como uno de los primeros ejemplos podemos destacar una máquina expendedora de bebidas la estaba conectada a Internet para comprobar si había o no bebida disponible en la misma.

Figura 5 – Primer dispositivo IoT – Maquina de bebidas

Durante una conferencia, Kevin Ashton (experto en innovación digital) fue en primero en describir el concepto de IoT, pero no fue hasta el año 2005 en el que el concepto fue añadido por la ITU (international Telecommunication Union) en el ITU Report. A lo largo de los años esta definición ha cambiado.

Según el informe de la IEEE del año 2014, podemos definir IoT como "*Una red de elementos dotados de sensores los cuales están conectados con Internet*". Esto incluye casi cualquier cosa que podamos pensar, desde teléfonos móviles, mantenimiento de edificios o el motor de un avión, dispositivos médicos como marcapasos, sensores en una granja de animales, calzado, ropa, etc.

2.2 Aplicaciones

Como hemos visto anteriormente, IoT no solo es una innovación tecnológica si no que engloba un cambio radical en que impactara en la sociedad tal y como la conocemos actualmente, lo que significa que afectara a casi todos los aspectos de nuestras vidas, tanto en el ámbito personal como en el profesional, así como en el ámbito de la economía, en los que podemos destacar:

- Industria y manufacturas
- Cadenas de suministro
- Marketing y Finanzas
- Salud
- Transporte y Logística
- Agricultura
- Energía
- Ciudades inteligentes
- Casas y edificios inteligentes
- Fuerzas de seguridad
- Educación
- Deporte

Todas estas áreas ya están involucradas en la transformación digital que ha sido provocada por la llegada de IoT y jugara un papel aún más importante en ellas a lo largo de los años.

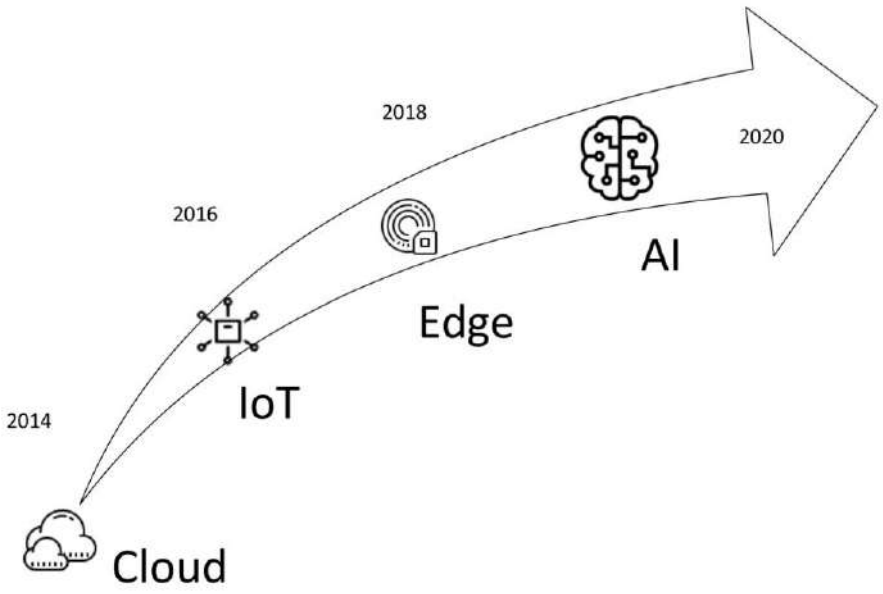


Figura 6 – Evolución de IoT

Como se puede apreciar las aplicaciones son casi infinitas. A continuación, vamos a comentar algunos ejemplos tanto en el mundo doméstico como en el entorno empresarial.

Imaginemos el frigorífico de nuestra casa. Éste podría estar conectado a Internet y nos podría avisar a nuestro teléfono móvil de las fechas de caducidad de nuestros productos, ver si alguno de ellos se está acabando, si se produce algún problema técnico en ella o el consumo eléctrico que estamos teniendo.

Sin salir de nuestra casa, el mundo de la domótica podría ser otro ejemplo donde ya hay numerosos dispositivos que están conectados a Internet, como altavoces inteligentes, alamas, persianas, iluminaciones, piscinas, sistemas de climatización, los cuales permiten ser controlados remotamente desde nuestros móviles, por ejemplo.

Ya dentro del mundo industrial, IoT se utiliza en muchos entornos productivos para la monitorización de la cadena de producción, maquinaria y demás elementos que intervienen en la producción de cara a generar alamas y mensajes que se envían a los administradores de los sistemas para que tomen las medidas oportunas o, en un paso más allá, actuar de manera automática ante las mismas.

Otros términos que estas muy relacionados con IoT pueden son "Smart Cities" y "Smart Buildings", los cuales se aplican a dispositivos que se utilizan para un mejor del control del tráfico, el control del transporte público, control de servicios en edificios (climatización, puertas, etc.)

3. IoT. Seguridad en IoT. Tecnologías, Riesgos y Retos.

La seguridad que engloba a todos los elementos que componen una red IoT es vital. Los protocolos actuales utilizados en IoT trabajan con protocolos IP como su columna vertebral, pero están orientados a trabajar en diferentes capas y proporcionar seguridad en múltiples campos. Los mayores retos en términos de la seguridad de una red de IoT es la ausencia de una estandarización lo cual expone tanto el hardware, como el software y los datos a diferentes amenazas y ataques. Los protocolos de IoT tienen que tratar con brechas de seguridad en un entorno heterogéneo y distribuido.

3.1. Problemas de Seguridad en IoT

Los problemas que afectan a la seguridad de IoT no están únicamente relacionados con el medio inalámbrico, sino que afectan también a aspectos como el control de acceso, autenticación y privacidad. Podemos destacar entre todos ellos los siguientes:

Dispositivos con recursos de proceso limitados: los recursos de que disponen estos dispositivos en lo que respecta a nivel de procesamiento y almacenamiento son bastante escasos lo que dificulta la ejecución de algoritmos pesados en ellos.

Gestión de la confianza: este mecanismo es necesario para los diversos procesos como la criptografía y el cifrado de firmas.

Heterogeneidad: IoT es una integración de redes heterogéneas de dispositivos lo cual provoca la aparición de problemas de compatibilidad y seguridad, dificultando la identificación de los nodos de confianza en el entorno.

Control de acceso seguro: este problema es uno de los mayores retos en una red de IoT. Es habitual que la información ubicada en el cloud sea accedida por varias entidades y procesos, por lo cual, la definición de una política de control de acceso y un acceso seguro son un reto en este entorno.
Gestión de las identidades: es una condición requerida la identificación de cada dispositivo de manera univoca. Mediante la autenticación se valida el flujo de datos a través del dispositivo y con la autorización aseguramos el control de acceso. En un entorno de IoT, los dispositivos puedes ser añadidos de manera dinámica, lo cual dificulta aún más este proceso.

Privacidad: es un tema importante proporcionar privacidad para la gran cantidad de dispositivos que se encuentran en una red IoT. El anonimato del usuario debe ser mantenido en todo momento, siendo un punto importante en todo el ciclo de vida de IoT.

Red distribuida de IoT: el flujo de información desde los dispositivos hasta el centro de recopilación sigue un patrón jerárquico, lo cual proporciona un control centralizado de la seguridad mejor, pero si uno de los dispositivos en una red IoT se ve comprometido, todo el sistema puede están comprometido también.

3.2. Tecnologías en el ámbito de la seguridad IoT

El problema de la seguridad ha de ser tratado durante el ciclo de vida de cada uno de los dispositivos IoT. Estas tecnologías en materia de seguridad deben ser comprobados en cada una de las etapas del ciclo de vida de manera que nos permita protegernos ante un ataque a nuestro entorno de IoT.

Como principales tecnologías podemos señalar las siguientes:

Algoritmos criptográficos: utilización de algoritmos de clave pública que proporcionan gestión de claves, autenticación de los nodos escalabilidad y seguridad.

Técnicas de gestión de claves: este punto es una importante característica de seguridad en IoT. La utilización de protocolos de distribución de claves ligeros es obligatoria para asegurar las comunicaciones. El principal objetivo en la gestión de las claves es reducir la complejidad, el consumo energético y la seguridad.

Protocolos de enrutamiento seguros: los protocolos de enrutamiento tradicionales no pueden ser usados para una red IoT. El protocolo de comunicación ha de garantizar la autenticidad de la información enrrutada y evitar las escuchas no autorizadas mientras la comunicación se realiza por un medio inalámbrico.

Clasificación de la información: los datos que se encuentran en una red de IoT pueden ser de distinto tipo y en función del mismo, el grado de protección ha de ser mayor cuanto mayor es la sensibilidad de la misma, por lo que ésta ha de ser clasificada en función de este parámetro.

Protección de los dispositivos en producción: los dispositivos de producción han de estar protegidos, teniendo todos sus puertos el correspondiente control de acceso. Aquellos dispositivos que se encuentren en localizaciones expuestas dispondrán de protecciones adicionales que los protejan de accesos físicos no autorizados.

Secuencia de arranque por etapas: Una secuencia de arranque por etapas confiable asegurará la seguridad de un dispositivo IoT. Sin embargo, la primera secuencia es vital y, por lo tanto, debería ser iniciado por código seguro. El uso de un módulo seguro donde los algoritmos criptográficos y las claves se almacenan es recomendado. En cada etapa del código de arranque, se recomienda verificar la confiabilidad del código de arranque, validez de hardware y finalización del código anterior.

Sistema operativo seguro: un sistema operativo en IoT debería tener unos derechos de acceso limitados con una reducida visibilidad del sistema. Debería estar diseñado para tener solo aquellos elementos indispensables para que el dispositivo pueda funcionar. Durante el ciclo de vida del dispositivo se le han de proporcionar actualizaciones. Todos aquellos puertos, protocolos y servicios que no se utilicen deberán estar deshabilitados.

Seguridad de aplicación: las consideraciones de seguridad deben ser parte integral del diseño de las aplicaciones y no debería ser añadido a posteriori. Las credenciales deben estar almacenadas de manera separada en un almacenamiento seguro.

Conexiones de red: el número de interfaces de conexión de un dispositivo de IoT hacia el exterior ha de mantenerse al mínimo posible. Solo los puertos, interfaces o servicios necesarios han de estar

habilitados. El uso de conexiones SFTP y HTTPS ha de ser el medio usado para el acceso a los dispositivos.

Actualizaciones de software: Antes de proceder a cualquier actualización de software, la fuente de la misma ha de ser verificada mediante el uso de certificados emitidos por una entidad certificadora reconocida. El paquete de actualización ha de estar firmado adicionalmente.

Registro seguro de eventos: el sistema de registro de eventos ha de estar protegido de accesos no autorizados que puedan modificar o eliminar su contenido. Este sistema se encuentra normalmente almacenado en un registro central alejado de los dispositivos IoT. Estos logs han de ser comprobados periódicamente para la detección de posibles fallos y las acciones a tomar en cada caso. En ellos no se deben almacenar ningún tipo de credencial del sistema.

3.3. Retos de la seguridad de IoT

Podemos agrupar la lista de los retos a los que se enfrenta IoT en tres grandes grupos: Limitaciones hardware, limitaciones software y limitaciones de conectividad. Dentro de las limitaciones hardware podemos destacar las limitaciones de procesamiento, memoria y la resistencia de su cobertura. En lo relativo al software éstas hacen referencia a las limitaciones del software embebido y las actualizaciones dinámicas de seguridad. Por último, la movilidad, escalabilidad, diversidad de dispositivos, medios de comunicación, protocoles y topologías de red descantan en las limitaciones de conectividad.

IoT hardware: en esta categoría podemos encontrar sensores, dispositivos wereables, dispositivos digitales y otros microcontroladores como, por ejemplo, las Raspberry Pi. Los fabricantes de estos dispositivos están más preocupados por los aspectos de diseño de los dispositivos que en su seguridad. La reducida capacidad de cálculo de los mismos inhibe los mecanismos de seguridad que ha de tener un dispositivo de IoT. También debido a la falta de estandarización estos están más expuestos a amenazas de seguridad. De cara a proteger estos dispositivos hemos de tratar asuntos como el ciclo de vida del hardware, las actualizaciones de software, el control de acceso y la autenticación. Dentro del entorno empresarial, se ha de verificar la configuración de estos dispositivos, realizar escaneos de vulnerabilidades y comprobar las conexiones de red.

IoT Firmware y software: los dispositivos IoT conectados a Internet suelen disponer de sistemas operativos embebidos como firmware, los cuales no están diseñados bajo unos estándares que prioricen la seguridad lo cual los hacen vulnerables a ataques de malware.

Inseguridad en las comunicaciones de red: debido al gran número de dispositivos conectados, las medidas de seguridad tradicionales son muy difíciles de implementar. La monitorización y aislamiento de los dispositivos en vlans privadas ayuda a reducir las amenazas de seguridad. Es difícil proporcionar seguridad a todos los dispositivos IoT conectados tras un firewall porque el ataque de un hacker a solo nodo puede comprometer de manera lateral todo el sistema.

Amenazas y vectores de ataque: los vectores de ataque son vías que utilizan los hackers para acceder a sistemas seguros. Éstos vectores aumentan diariamente debido al incremento de las conexiones globales lo cual nos lleva a incrementar las medidas de tolerancia a fallos disponibles. Los datos y metadatos de IoT pueden ser usados como vectores de ataque por los hackers. Dentro de las amenazas actuales, podemos destacar las siguientes:

- Denegación de servicio
- Escuchas ilegales
- Control de un dispositivo IoT
- Ramsomware

3.4. Ataques de seguridad en IoT

Los usos de mundo de IoT nos están proporcionando más ventajas cada día que pasa. Esta tecnología hace a las cosas inteligentes mediante la incorporación de sensores, lo cual les dota de conectividad y de nuevos servicios. Este aumento de la información generada hace que este más expuesta a ataques de seguridad.

El ataque, por ejemplo, a una cámara de seguridad ubicada en nuestra casa puede revelar información a los posibles atacantes de la presencia o no de personas en casa de cara a planear un robo. Tenemos que ver cuáles son las vías en las cuales nuestros dispositivos pueden ser atacados. A continuación, comentaremos varios de estos posibles ataques.

Ataques a nivel de firmware: el firmware no es más que un software encargado de controlar los dispositivos. En general este software es almacenando en una zona de memoria no volátil. Los hackers intentan añadir código a esa zona de la memoria de manera que pueden hacerse con el control del dispositivo. Estas intrusiones son difíciles de identificar ya que suelen ejecutarse con anterioridad a antivirus del sistema. Otras razones de su preferencia en este tipo de ataques son:

- Persistencia: estas zonas no pueden ser borradas con facilidad.
- Protección: pueden mantenerse ocultos con mayor facilidad.
- Autorización: el código añadido en el firmware puede permitir a un usuario el control del dispositivo.

No es extraño encontrarse con dispositivos cuyo firmware es obsoleto, incluso en equipos de reciente aparición, a lo que podemos añadir que muchos usuarios suelen actualizar este componente en sus dispositivos. De cara a minimizar estos peligros es aconsejable tener siempre los dispositivos a su ultimo nivel de firmware, exigiendo a los fabricantes actualizaciones de los mismos si éstas se dilatan mucho en el tiempo.

Ataques en los datos

El gran volumen de información que el mundo de IoT genera va desde el dato más inocuo hasta el más sensible, lo cual hace de esta variedad un entorno muy atractivo para aquellos que quieran sustraer información. Todos los elementos en la cadena de conexión, desde el dispositivo hasta el usuario son susceptibles de ser atacados pudiendo robar información a través de ellos. Si fuera sencillo el acceso a estas informaciones no tendría sentido la conexión de estos dispositivos. IoT nos permite que las cosas estén conectadas entre sí, pero también aumenta el número de problemas de seguridad.

Figura 7 – Objetos conectados al mundo IoT

Ataques basados en Telnet: el comando telnet es un viejo conocido dentro del mundo de la informática y está de nuevo en primera línea debido a que muchos de los dispositivos utilizan puertos explotables mediante telnet para el acceso remoto a sus configuraciones, pudiendo explotar vulnerabilidades del mismo, obtener accesos no autorizados, controlar el flujo de la información o la obtención de contraseñas, entre otros.

Es habitual encontrarnos con dispositivos que, aun recomendando el cambio de sus credenciales de fábrica, los usuarios no las han cambiado, lo cual en combinación con los puertos telnet, son una brecha importante en la seguridad de los mismos. Es, por lo tanto, recomendable el bloqueo de estos puertos y el establecimiento de credenciales distintas a las definidas por el fabricante para protegernos de estos ataques.

Ataques de DDOS: este tipo de ataque es importante dentro de IoT, ya que puede convertir a estos dispositivos en miembros de bonets que sirvan como atacantes contra otros servicios de Internet. Varios de estos ataques están documentados en la web.

Malware: la mayor parte de los ataques a los que se enfrenta el mundo de IoT viene dado por este tipo de ataques. Los dispositivos IoT son más vulnerables a sufrir este tipo de ataques debido a, entre otros, su débil autenticación, numerosas vulnerabilidades de seguridad o sus limitadas capacidades de actualización.

3.5. Soluciones de seguridad en IoT

Anteriormente hemos visto cuales son los posibles ataques que pueden ser sufridos por un dispositivo IoT. Como podemos observar en la imagen, la pila IP del mundo IoT es diferente a la que conocemos tradicionalmente, lo cual es debido a las peculiares características de estos dispositivos.

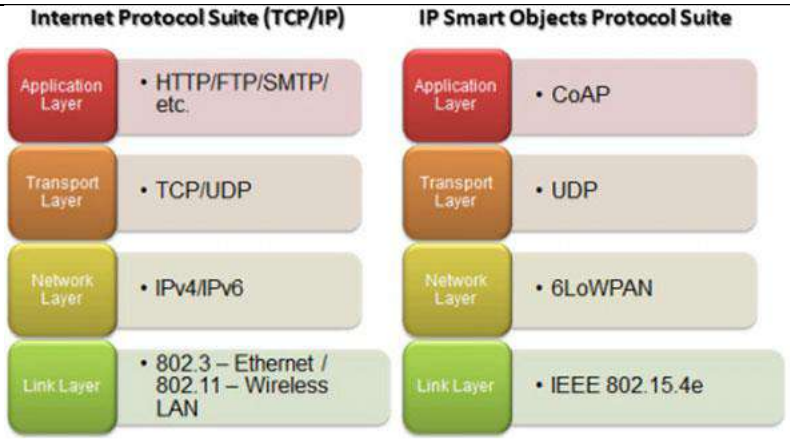


Figura 8 – Estructura de protocolos en IoT

Dada la diversidad de dispositivos que pueden componer estos entornos, es importante adaptarla para que pueda trabajar de una manera convencional con Internet. Muchos de estos dispositivos no son lo suficientemente potentes para la ejecución de algoritmos complejos. Tampoco es fácil actualizarlos de una manera global debido a que se conectan mediante conexiones no del todo fiables. Por último, la aplicación de la seguridad requerida en ellos a veces no es del todo trivial para los usuarios, lo que disminuye el grado de implantación de estas medidas.

Vamos a ver diferentes protocolos que nos permiten avanzar en estas tareas en distintas capas, como la de transporte, la de aplicación y la de red.

Capa de transporte

Dentro de esta capa, el protocolo UDP juega un importante papel ya que es el que se utiliza preferentemente en entornos IoT debido a sus características como, por ejemplo, un overhead mínimo. Hay entornos en los que esta propiedad es de vital cuando lo comparamos con TCP.

UDP es *conectionless* y, por lo tanto, sin un estado de conexión que mantener, por lo que el tamaño / uso de la memoria no es un gran problema. Una transacción UDP requiere solo dos datagramas UDP, uno en cada dirección, la carga en la red se minimiza, lo que reduce aún más tiempos de respuesta.

Capa de aplicación

El uso de HTTP en Internet está muy extendido hoy en día. Pero en el mundo de IoT, este protocolo no es el que mejor se adapta a las necesidades que tienes estos dispositivos. Es por esto por lo que dos nuevos protocolos se han diseñado, los cuales están más adaptados a las peculiaridades de este mundo, como son MQTT y CoAP.

COaP (Constrained Application Protocol)

Como indica su nombre, es un protocolo ubicado en la capa de aplicación, la cual está justo encima de la capa de transporte, donde TCP y UDP son los protocolos básicos. Los protocolos de la capa de aplicación se basan en cualquiera de estos protocolos de capa de transporte (TCP o UDP). Básicamente, TCP es complejo cuando se compara con UDP. El problema con UDP es que no es estable. Dado que HTTP es no es adecuado para dispositivos de baja potencia y bajo ancho de banda, CoAP fue diseñado para solventar estos inconvenientes.

CoAP nació en el año 2014. Los desarrolladores de CoAP lo diseñaron de tal manera que debía incluir las características de HTTP y también ser aplicable para dispositivos que tienen recursos limitados. Para su funcionamiento utiliza UDP, estando basado en la arquitectura REST.

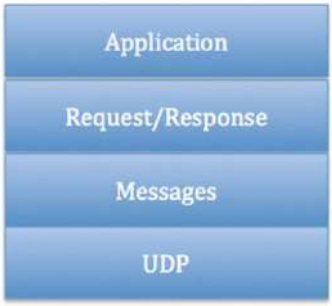


Figura 9 – IoT Estructura de mansaje CoAP

Para la protección de las transmisiones CoAP, DTLS (Datagram TLS) ha sido la tecnología seleccionada como protocolo de seguridad principal.

MQTT (Message Queue Telemetry Transport)

MQTT es un protocolo ligero basado en TCP que utiliza un patrón de mensajes de publicación-suscripción. Cualquier fuente, como un sensor, puede publicar sus datos y el cliente puede suscribirse a esos datos. MQTT está diseñado para dispositivos de recursos limitados cuyo ancho de banda es mínimo. MQTT consta de tres componentes, el broker, editor y suscriptor. El broker realiza un seguimiento de todas las publicaciones y suscripciones. El editor publica información a todos los suscriptores a través del broker. El broker securiza el intercambio al verificar la autorización de los editores y los suscriptores. El broker también garantiza la entrega de un mensaje, es decir, es entregado al menos una vez o exactamente una vez.

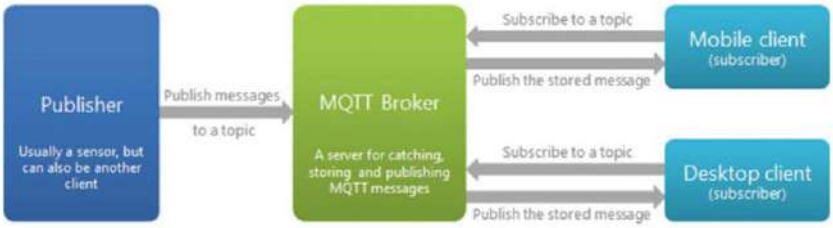


Figura 10 – MQTT Componentes

MQTT usa un formato binario que requiere un mínimo de ancho de banda. El encabezado tiene solo dos bytes. El mensaje tipo puede variar entre CONECTAR, CONECTAR, PUBLICAR Y SUSCRIBIRSE. El campo DUP indica si el mensaje está duplicado y si el receptor puede haberlo recibido antes. El campo QoS es utilizado para garantizar la entrega. MQTT admite tres niveles de QoS, "Fire and Forget", "entregado al menos una vez" y "entregado exactamente una vez". El campo RETENER informa al servidor para retener el último mensaje de publicación recibido.

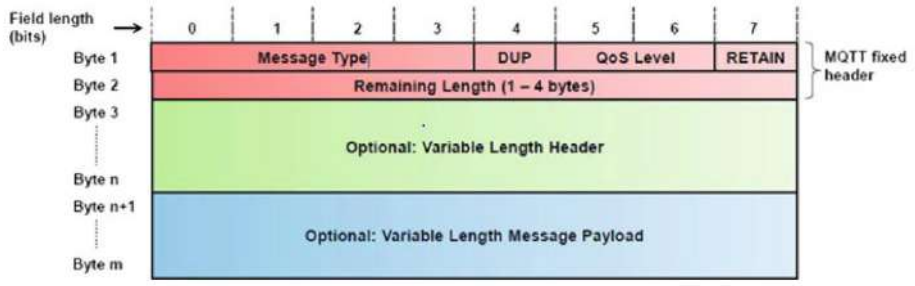


Figura 11 – MQTT Formato del mensaje

Creado originalmente en 1999 para sensores remotos, ahora se usa de forma segura y confiable para la comunicación entre dispositivos. MQTT se basa en TCP en combinación con TLS para la seguridad.

Aunque MQTT está diseñado para ser ligero, tiene dos inconvenientes para dispositivos muy limitados. Cada cliente MQTT debe ser compatible con TCP y, por lo general, tendrá una conexión abierta al broker en todo momento. Para algunos entornos donde la pérdida de paquetes es alta o los recursos informáticos son escasos, esto es un problema. También, MQT utiliza nombres cuya longitud es elevada. Ambos inconvenientes son abordados por el MQTT-SN (MQTT: redes de sensores), que define una asignación UDP de MQTT y agrega al broker soporte para la indexación de estos nombres (topic names)

Capa de red

Los dispositivos en el Internet de las cosas tienen recursos limitados, lo que significa que el tamaño del dispositivo, la energía y la memoria limitan sus posibilidades. En esta sección, hablaremos sobre los protocolos IPv6 y 6LowPAN. IPv6 soporta un espacio de direcciones suficiente para todos los dispositivos IoT involucrados. 6LoWPAN está especialmente diseñado para baja potencia dispositivos.

IPv6

IPv4 es el direccionamiento de red utilizado más ampliamente. Es una dirección de 32 bits y puede admitir hasta 4 mil millones de dispositivos. En el mundo de Internet de las cosas, cada dispositivo está conectado a Internet, pero IPv4 no es suficiente con un número tan grande de dispositivos. IPv6 utiliza direcciones de 128 bits y puede asignar hasta 2^{128} rangos de direcciones. Esto hace que sea posible asignar una dirección IP a todos los dispositivos que están conectados en el mundo de IoT.
Las principales características que lo hacen ventajoso sobre IPv4 son las siguientes:

- Escalabilidad: dado que es una dirección de 128 bits, podemos asignar direcciones IP a cada dispositivo.
- Se puede lograr una verdadera conectividad de extremo a extremo.
- Las tasas de utilización del espacio de direcciones son pequeñas en IPv6.
- IP Sec es un requisito en IPv6, lo que permite que dos o más hosts se comuniquen de manera segura autenticando y encriptando cada paquete IP en cada sesión de comunicación.

6LoWPAN

Aunque IPv6 proporciona la plataforma de direccionamiento, esta no es adecuada para los dispositivos de poca potencia involucrados en IoT. Para admitir estos dispositivos necesitamos otro protocolo. WPAN (Wireless Personal Area Networks) es utilizado en muchas comunicaciones en los entornos IoT, teniendo algunas características especiales como el tamaño de paquete limitado (por ejemplo, máximo 127 bytes para IEEE 802.15.4), varias longitudes de dirección y bajo ancho de banda.

El grupo de trabajo de IETF 6LoWPAN desarrolló dicho estándar en 2007. 6LoWPAN es la especificación de los mapeos de servicios requeridos por el IPv6 sobre dispositivos de baja potencia de cara a mantener una red IPv6. Este estándar proporciona compresión de encabezado para reducir la sobrecarga de la transmisión, fragmentación para cumplir con el requisito de MTU y reenvío a la capa de enlace para admitir la entrega a múltiples saltos.

4. IoT. Elementos de la arquitectura

En el mundo de los dispositivos IoT, podemos encontrar principalmente 3 tipos de dispositivos:

- Los de menor tamaño que incluyen un controlador del tipo SOC (8-bit System on a Chip), entre los que podemos destacar los Arduinos Uno, los cuales no disponen de sistema operativo.

- En un siguiente nivel nos encontraríamos con los sistemas basados en chips ARM con una arquitectura de 32 bastante limitada, en los cuales se ejecutan versiones reducidas de Linux o sistemas operativos dedicados.

- En el escalón más alto nos encontramos con plataformas de computación, tanto en 32 como en 64 bits, como pueden ser las Raspberry Pi, las cuales ejecutan versiones completas de Linux o Windows. Estos dispositivos pueden hacer de medio de conexiones para otros dispositivos menos potentes, dotándoles de acceso de Internet a través de conexiones Bluetooth por ejemplo entre ellos.

La forma en la que los dispositivos se comunican entre ellos y el mundo de Internet puede seguir diferentes modelos, como, por ejemplo:

- Conectividad directa mediante Ethernet o red inalámbrica
- Near Field Communication (NFC)
- Bluetooth Low Energy

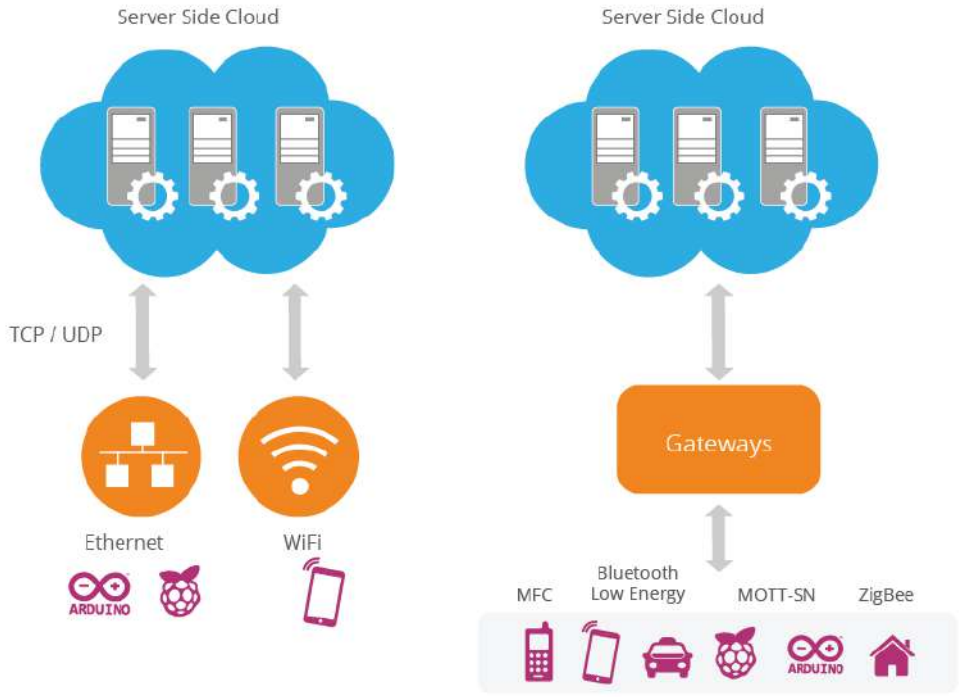


Figura 12 – IoT Vías de conexión de los dispositivos

4.1. Requerimientos para una arquitectura de IoT

Hay determinados requerimientos específicos los cuales son propios de la casuística de los dispositivos IoT, muchos de los cuales surgen de sus limitaciones a nivel de tamaño y energía.
Los principales requerimientos los podemos agrupar en las siguientes categorías clave, de las que comentaremos más en detalle alguna de ellas:

- Conectividad y comunicaciones
- Gestión de dispositivos
- Escalabilidad
- Seguridad.
- Alta disponibilidad
- Analísis predictivo
- Integración

Conectividad y Comunicaciones

Los protocolos que existen actualmente, como puede ser HTTP, tienen un lugar muy importante para el mundo IoT. Un controlador de 8 bits puede crear solicitudes GET y POST simples. También HTTP proporciona una conectividad unificada y uniforme. Sin embargo, la sobrecarga que este protocolo y algunos otros protocolos tradicionales pueden originar problemas en el mundo de IoT.

En primer lugar, es importante que el tamaño de los programas ha de ser lo más pequeña posible dado el escaso espacio que estos dispositivos tienen. Otro problema viene relacionado con sus requisitos de energía. De cara a cumplir con estos dos requisitos se necesita protocolo adaptado a este mundo.

Gestión de Dispositivos

A lo largo del tiempo hemos visto como el número de ordenadores, móviles y otros dispositivos que son gestionados de manera activa ha aumentado de manera importante y este mismo camino es el que debería seguir el mundo de IoT. Los requerimientos para poder afrontar esta función podrían ser:

- La capacidad de desconectar un dispositivo extraño o robado
- La capacidad de aplicar actualizaciones a los dispositivos
- Actualización de las credenciales de seguridad.
- Capacidad de habilitar y deshabilitar funciones de manera remota.
- Capacidad de localizar un dispositivo perdido.
- Borrado remoto de dispositivos perdidos
- Reconfiguración remota de los parámetros de red del dispositivo

Escalabilidad

Como requerimiento importante de una arquitectura de IoT está el tema de su escalabilidad, es decir, la capacidad de escalar desde un entorno de pequeño tamaño a uno compuesto por un gran número de dispositivos. Su elasticidad y la capacidad del uso de plataformas cloud es una característica esencial.

Seguridad

No cabe duda de que este aspecto es crucial en el entorno de IoT. Los dispositivos muy a menudo recopilan datos de carácter personal lo cuales pueden ser expuestos a Internet sin nuestro consentimiento. Los riesgos los podemos clasificar en:

- Aquellos propios de cualquier dispositivo conectado a Internet.
- Los que son específicos del mundo de IoT.

En la primera categoría podríamos ubicar cosas sencillas como el bloqueo de los Puerto que no están en uso. En el segundo grupo colocaríamos aquellos propios de IoT, como la falta de recursos para la utilización de un sistema de encriptación adecuado.

4.2. Arquitectura

Las arquitecturas típicas de IoT suelen estar agrupadas bajo dos conceptos como son los *tiers* y los *layers.* Los tiers donde un dispositivo IoT, función o proceso opera dentro de un entorno de IoT. Los layers definen que características un dispositivo IoT, función o proceso han de tener. En las siguientes imágenes podemos ver en detalle ambos elementos.

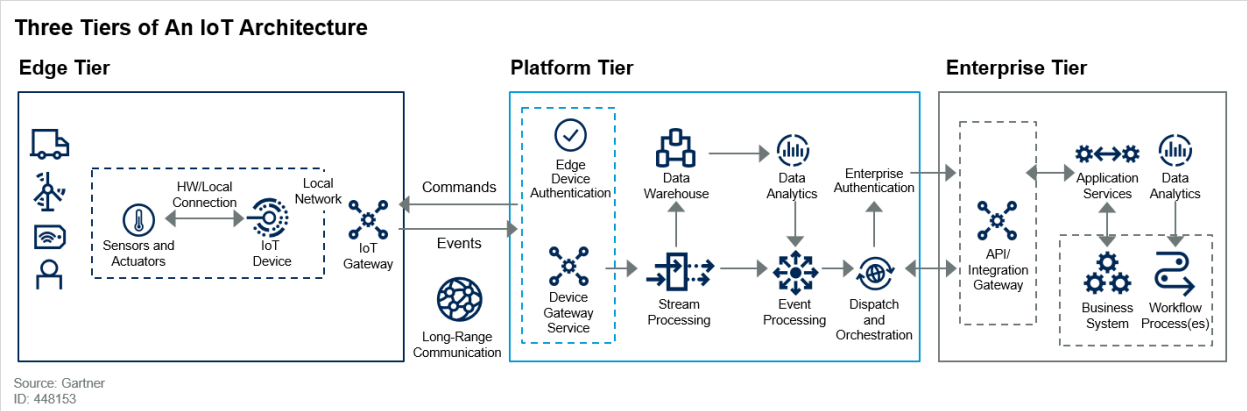


Figura 13 – IoT Arquitectura de Tiers

El *edge tier* es el lugar donde los datos son generados y recopilados desde el entorno a través de los dispositivos IoT. Dentro de estos dispositivos podemos encontrar aquellos destinados al consumo doméstico (como una bombilla wifi) o aquellos pertenecientes al mundo industrial, como un sistema de control de una cadena de montaje, la cual contiene sensores para la recopilación de datos. Dentro de este tier también se encuentran los gateways usados por IoT que pueden proporcionar análisis de los datos localizados, procesamiento de eventos y almacenamiento, así como ayudar a la integración de dispositivos antiguos dentro de la plataforma IoT.

La *platform tier* es donde los sistemas IoT agregan los datos y eventos que provienen de diferentes ubicaciones. A menudo proporciona servicios de stream processing y event processing para múltiples localizaciones edge. En ella también se realizan tareas de orquestación o llamada a aplicaciones empresariales.

La *enterprise tier* es donde los sistemas IoT se integran con un conjunto de aplicaciones, procesos o servicios que son requeridos para la consecución de los objetivos de negocio., como pueden ser la gestión del inventario, por ejemplo. Muchas de las plataformas de IoT incluyen sus propias API´s que pueden ser utilizados por las aplicaciones empresariales para sus propios propósitos.

En cuanto a los layers, estos los podemos dividir en los siguientes niveles:

- Accesos mediante los portales web, Dashboard o APIs de cliente
- Procesamiento y análisis de eventos
- Nivel de agregación – ESB y message broker
- Comunicaciones (MQTT/HTTP/XMPP/CoAP/AMQP)
- Dispositivos.

Como layers que aplican de manera transversal a las anteriores tenemos:

- Gestión de dispositivos.
- Identificación y gestión de acceso.

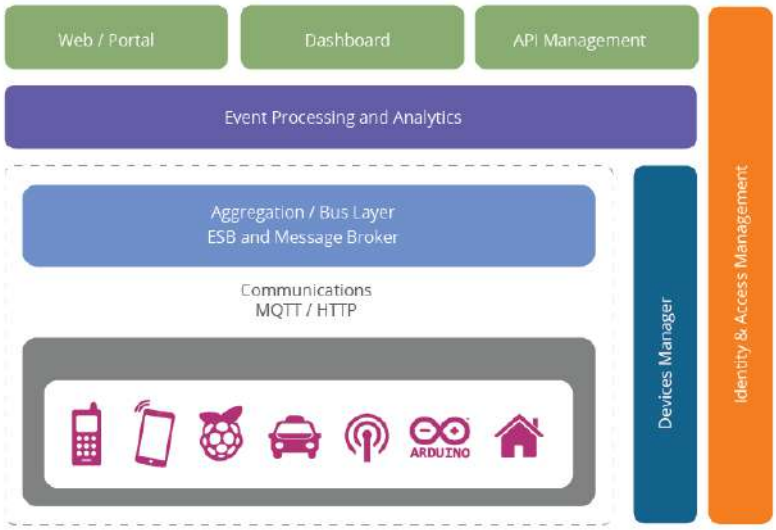


Figura 14 – IoT Arquitectura de Layers

Capa de dispositivos

Es la capa situada en el fondo de la arquitectura. Los dispositivos, como hemos indicado anterior mente, pueden ser de diferente tipo, pero a la hora de considerarlo uno del mundo IoT, ha de disponer de conexión, ya sea de manera directo o indirecta a Internet.
Cada dispositivito ha de tener un ID que lo identifique de manera univoca. Esto puede lograrse, por ejemplo:

- Con un UUID que forme parte de un chip en el mismo.
- Un UUID proporcionado por el Sistema de comunicaciones (MAC por ejemplo)
- Un identificador almacenado en una zona no volátil de la memoria.

Capa de comunicaciones

En esta capa es donde se soportan las comunicaciones de los dispositivos. Hay mucho protocoles potenciales que pueden ser usados, pero los más conocidos son:

- HTTP/HTTPS
- MQTT 3.1/3.1.1
- Constrained application protocol (CoAP)

El protocolo HTTP es un viejo conocido de Internet, el cual tiene muchas librerías que lo soportan. Dado que es un protocolo sencillo basado en texto los dispositivos con menos capacidades de proceso pueden realizar parte de sus funciones, como puede ser un post o un get.

Existen también protocolos especialmente optimizados para el mundo IoT. Los dos más conocidos son MQTT y CoAP. MQTT fue creado en el año1 999 para resolver los problemas que se presentaban en los ciertos dispositivos. MQTT tiene un tamaño de mensaje muy reducido y fue diseñado para el soporte de redes de conexiones intermitentes y con pérdidas utilizando TCP.

CoAP es un protocolo diseñado por la IETF pensado con la intención de proporcionar un protocolo de aplicación RESTful modelado bajo la semántica HTTP, pero con el objetivo de generar un mensaje de un tamaño menor que los diseñados basados en texto. Ésta pensado para ser usado utilizando UDP.

La capa de agregación/bus

En esta capa es donde las comunicaciones se agregan y se realizan las funciones de bróker. Las principales características que hacen esta capa importante son:

- La capacidad de soportar un servidor HTTP y/o un servicio de broker MQTT para comunicarse con los dispositivos.
- La capacidad de agregar y combinar comunicaciones de diferentes dispositivos y enrutar las comunicaciones a través de un dispositivo especifico.
- La capacidad de enlazar y transformar entre diferentes protocolos.

Procesado de eventos y capa analítica

Dentro de esta capa se recogen los eventos provenientes del bus y nos proporciona la capacidad de procesamiento de los mismos y actuar en base a ellos. Una característica principal en ella es la capacidad de almacenar la información en una base de datos, lo cual puede llevarse a cabo de tres maneras diferentes. La manera tradicional seria mediante una aplicación del lado del servidor.

Sin embargo, existen diferentes caminos que nos proporcionan una mayor agilidad. El primero sería el uso de una plataforma de analítica de bigdata, basada en cloud y altamente escalable como Apache Hadoop, la cual nos da una alta capacidad analítica sobre los datos que provienen de los dispositivos. El segundo camino consiste en un soporte complejo del procesamiento de los eventos que nos permitan ejecutar actividades y acciones casi en tiempo real tomando como base los datos que recibimos de los dispositivos y el resto de sistemas.

Capa de comunicación externa

En este punto de la arquitectura se proporciona una vía para que los dispositivos puedan comunicarse con el mundo exterior, fuera de los sistemas de dispositivos. En ella podemos distinguir tres principales puntos a destacar.

El primero de ellos es la capacidad de crear front-ends de tipo web que nos permitan interactuar con los dispositivos y con la capa de gestión de los eventos. El segundo es la capacidad de crear cuadro de mandos que nos ofrezcan vistas dentro los procesos analíticos. Como último debemos ser capaces de comunicarnos con el mundo exterior mediante el uso de diferentes API´s.

Gestión de dispositivos

Esta tarea es realizada mediante la utilización de dos componentes. Un sistema ubicado en el lado del servidor que se comunica con los dispositivos utilizando diferentes protocolos, proporcionado un control individual o conjunto de los dispositivos, permitiendo, por ejemplo, el control de las aplicaciones desplegadas en ellos o el bloqueo o borrado de uno de ellos si fuera necesario.

Este sistema trabaja en conjunto con los agentes de gestión de dispositivos. Existen diferentes agentes para cada tipo de plataforma y dispositivo.

El gestor de dispositivos ha de mantener una lista con la identidad de todos los dispositivos, así como de sus propietarios. Es también vital que se comunique con la capa de identificación y acceso para controlar el acceso a los dispositivos. La gestión de los mismos se puede agrupar en tres niveles principales: no gestionados, semi-gestionados y completamente gestionados.

Los pertenecientes a esta última categoría disponen dentro de ellos de un agente que permite está completa gestión.

- Gestión del software del dispositivo
- Control de características del dispositivo
- Gestión de los controles de seguridad
- Monitorización de la disponibilidad del dispositivo
- Control de la localización de los dispositivos
- Bloqueo y borrado de los dispositivos comprometidos.

Capa de Identidad y control de acceso

Los servicios que se han de proporcionar en esta capa son, entre otros:

- Gestión y validación de los tokens de seguridad.
- Directorio con los usuarios con acceso (servidor LDAP, por ejemplo).
- Gestión de políticas de control de acceso.

4.3. Zonas de confianza y fronteras

En toda solución de IoT se utilizan para su construcción diferentes tipos de componentes (dispositivos, field Gateway, etc.) los cuales son aislados de las dentro de las zonas de confianza y las fronteras. Estas separaciones proporcionan un aislamiento tanto físico como software de los distintos elementos de cara a proporcionarnos un mayor grado de protección ante problemas como:

- Ataques de robo de identidad
- Manipulación de eventos
- Robo de información
- DDOS
- Exploit por elevación de privilegios

Las principales zonas de confianza a tener en cuenta cuando diseñamos una arquitectura de seguridad en el mundo de IoT son las siguientes:

- Zona local
- Zona de dispositivos
- Zona del field gateway
- Zona del cloud gateway
- Zona de los gateways y los servicios
- Zona de los usuarios remotos

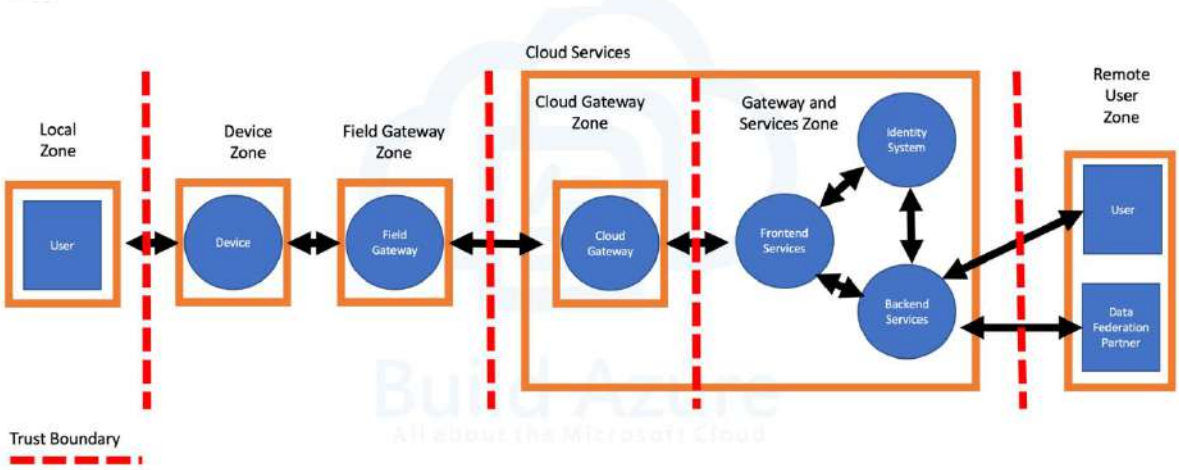


Figura 15 – IoT Zonas de confianza y boundaries

Como regla general, se debe tener una frontera entre cada una de las zonas de confianza. Esto nos permite ayudar a proteger cada zona creando un nivel de aislamiento entre ellas, lo cual repercute en el aumento de la seguridad en cada una de ellas y en las siguientes dado que el flujo de información va desde las zonas ubicadas más abajo hacia el cloud.

Zona local

Es la zona en la que se encuentran los usuarios locales, ya sea en la red local o la ubicada en on-premises, donde se encuentran los ordenadores de los usuarios. También puede ser la zona física más próxima a los dispositivos. Desde un punto de vista de la seguridad física, puede llevar consigo el despliegue de accesos controlados o biométricos a estas zonas.

Zona de Dispositivos

La zona del dispositivo es el área donde se encuentran los dispositivos IoT. Esto incluye el espacio físico alrededor de los dispositivos, así como la red local (o red local) a la que están conectados los dispositivos. La red local proporciona la conectividad digital para que los dispositivos se comuniquen con el resto del sistema, y puede incluir la conectividad a Internet. Debido al alcance físico y virtual de la conectividad y el acceso a los dispositivos, la arquitectura de seguridad de los dispositivos garantiza medidas de protección tanto físicas como digitales.

Desde un punto de vista virtual, la protección de la zona del dispositivo abarcaría la seguridad de los dispositivos en la red local a la que están conectados; incluida la conectividad cableada e inalámbrica que podría integrarse en los dispositivos. Esto incluye el uso de claves de cifrado para la comunicación, como el uso de SSL / TLS para comunicaciones seguras, entre otras técnicas de cifrado y validación.

Desde un punto de vista físico, asegurar la zona del dispositivo abarcaría asegurar los dispositivos encerrándolos en una caja segura o asegurando el acceso a las habitaciones o instalaciones donde se encuentran los dispositivos. Tenga en cuenta que cada dispositivo podría estar en una ubicación diferente, por lo que cada dispositivo puede necesitar su propio diseño de seguridad que difiere de otros dispositivos utilizados en el sistema.

Zona Field Gateway

La zona del field gateway es donde residirán los field gateway utilizados en el sistema. Podrían estar contenidos dentro del mismo límite de confianza que los dispositivos o en uno separado.

Como muchos dispositivos diferentes pueden estar ubicados en instalaciones o ubicaciones físicamente diferentes, puede haber múltiples field gateway en uso al mismo tiempo. Como resultado, puede haber múltiples zonas de gateway en una arquitectura de seguridad IoT para acomodar la conexión y facilitar las comunicaciones entre los dispositivos IoT y los componentes de la nube de la solución IoT.

Desde un punto de vista virtual, la protección de la zona de field gateway abarcaría la seguridad de los dispositivos de field gateway de una manera similar a la forma en que se asegura la conectividad inalámbrica o por cable de los dispositivos IoT. Esto incluiría comunicaciones encriptadas SSL / TLS, o alguna otra validación segura de los otros dispositivos y componentes que se comunican con los dispositivos field gateway.

Desde un punto de vista físico, la protección de la zona se realizaría de manera similar a la forma en que se aseguran los dispositivos IoT dentro de la zona de dispositivos, con medidas como acceso biométrico a los lugares donde se encuentran ubicados.

Zona del Cloud Gateway

La zona del cloud gateway es donde reside el intermediario de mensajes o la cola de mensajes. El agente de mensajes para una solución de IoT facilitará las comunicaciones entre los diversos dispositivos de IoT y los componentes de servicio del sistema. El cloud gateway no es una base de datos, almacenamiento o servicio de procesamiento específico, sino que proporciona la comunicación para obtener datos hacia / desde los servicios de fondo y los dispositivos en la solución.

Esta zona podría ubicarse en la nube pública; como Microsoft Azure o Amazon AWS. Sin embargo, también podría ubicarse en una red y ubicación separadas de cualquiera de los otros dispositivos en la solución IoT. El término "nube" en este contexto se está utilizando para referirse a la práctica de proporcionar medidas operativas para evitar el acceso físico dirigido a la zona. En el panorama actual de IoT, esto generalmente significará que la solución de IoT se creará con los componentes de la nube que residen en Microsoft Azure, Amazon AWS u otro proveedor de la nube, pero es importante recordar que esto podría significar un entorno local u otro entorno híbrido también.

Asegurar la conectividad virtual para la zona cloud gateway es, generalmente, la primera tarea a realizar en esta zona, especialmente si la arquitectura depende de un proveedor de la nube, como Microsoft Azure o Amazon AWS, para proporcionar servicios de broker de mensajes de IoT. Las encriptaciones de comunicación apropiadas y la validación de identidad del dispositivo deberán establecerse dentro de esta zona. La configuración de cada servicio particular de agente de mensajes de IoT tendrá sus propios requisitos y documentación sobre cómo configurar su seguridad.

Desde un punto de vista físico, esta zona es realizada por el proveedor de la nube, como Microsoft Azure o Amazon AWS. Sin embargo, si los componentes de la nube están alojados en un entorno local o en algún otro entorno híbrido, las medidas de seguridad física habituales de asegurar un centro de datos físico u otro dispositivo deberán tenerse en cuenta en la arquitectura de seguridad de IoT.

Zona de Gateway y Servicios

Aquí es donde residen todos los demás servicios de backend. Esto incluirá bases de datos, API REST, conectividad híbrida a sistemas locales y cualquier otro componente de backend del sistema. En general, habrá múltiples zonas dependiendo de cómo se distribuya la arquitectura general del backend entre los proveedores de la nube y las redes locales.
Además, esto contendrá principalmente servicios, pero podría incluir intermediarios de mensajes / puertas de enlace adicionales según sea necesario para desarrollar la arquitectura del sistema necesaria para el IoT y el escenario empresarial dados.

La seguridad en esta zona variará según los diferentes servicios, componentes y sistemas locales integrados en el sistema. Cada componente puede tener su propia seguridad implementada. Como resultado, puede haber uno o incluso múltiples límites de seguridad dentro del contexto.

Zona de Usuario Remoto

La zona de usuario remoto es una especie de depósito genérico que contiene partes de la solución que proporcionan algún tipo de acceso remoto o externo a usuarios o incluso socios externos. Esto también podría incluir la integración entre la solución IoT y los servicios de terceros integrados para proporcionar capacidades adicionales como parte de la arquitectura general de IoT.

Está menos predefinida que otras zonas. Las conexiones de usuarios remotos pueden incluir el uso de Escritorio remoto (RDP) para conectarse a una máquina virtual de Windows, el uso de SSL / TLS para acceder a algún tipo de aplicación web de usuario final o algún otro método de acceso seguro a terceros.

Realmente, la zona de usuario remoto proporciona esa zona de backend para la comunicación e integración en cualquier otro sistema que pueda necesitar integrarse en la solución IoT. Esto podría incluir las API o servicios de terceros, las aplicaciones web de acceso de usuario final o algunos otros escenarios de federación de datos.

Si enlazamos los conceptos de los que hemos hablado en este punto relativos a las zonas de confianza y las capas en las que se divide la arquitectura de un entorno de IoT, podemos ubicarlas de la siguiente manera:

- **Edge Tier**: contendría la Local Zone, Device Zone y la Field Gateway Zone.
- **Platform Tier**: contendría la Cloud Gateway Zone y la Gateway and Services Zone.
- **Enterprise Tier**: contendría la Remote User Zone

5. Arquitecturas y seguridad en entornos IIOT

5.1. Definición

Después de la invención de la máquina de vapor en 1760, el vapor fue utilizado para proporcionar energía a toda maquinaria industrial, desde la agricultura hasta las manufacturas. Esto fue el origen de la primera revolución industrial.

Con la llegada de la energía eléctrica a finales del siglo 19, nuevas formas de organización del trabajo y la producción en masa originaron la segunda revolución industrial.

En la segunda mitad del pasado siglo, con la llegada de controladores electrónicos se produjo el comienzo de la hora de la automatización y la llegada de la tercera revolución industrial.

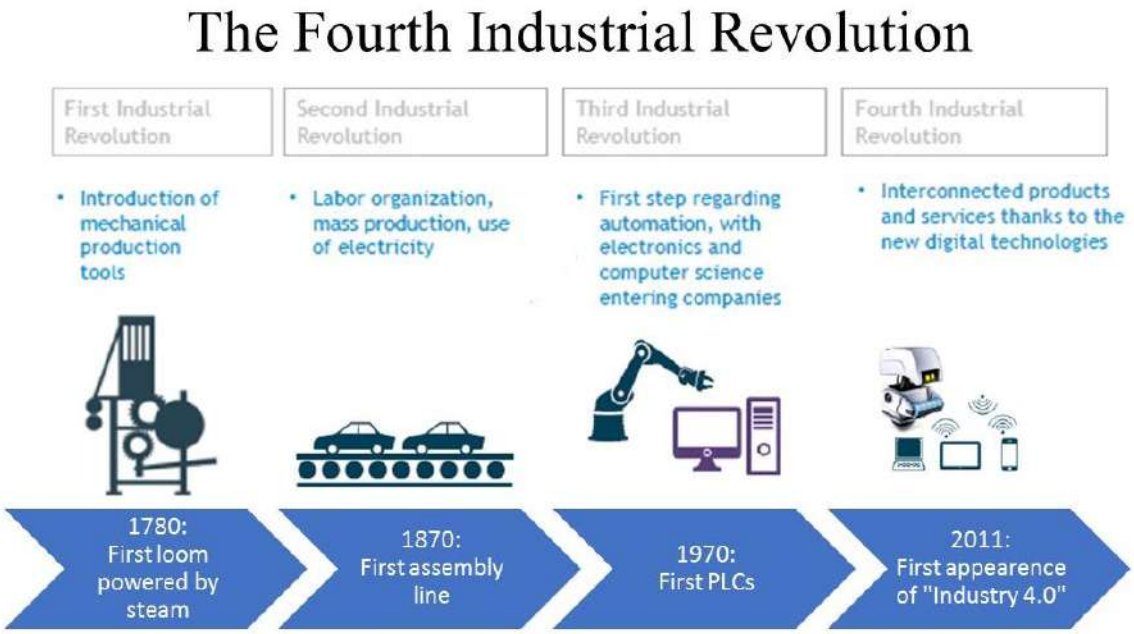


Figura 16 – Evolución Industrial

Fue en una convención en el año 2011 fue cuando se introdujo el concepto de Industria 4.0. De este nuevo concepto se esperan las siguientes cosas:

- Conectar y mezclar la producción con la tecnología de la información y la comunicación
- Mezclar los datos del cliente con los datos de las maquinas
- Aprovechar la capacidad de las máquinas para comunicarse con las maquinas
- Gestionar la producción autónomamente de una manera flexible, eficaz y con economicidad de recursos

El mundo de IoT es casi, por definición, la clave para el avance en el desarrollo de la industria de las manufacturas mediante la inclusión de tecnologías como el big data, el cloud, robots y como punto más importante, la integración y la convergencia entre IT y OT.

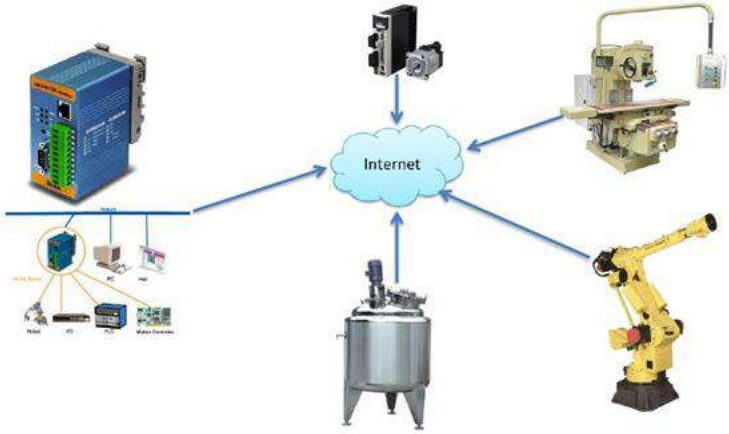


Figura 17 IIoT – Industrial IoT

Objetos, sensores, actuadores y controladores que alguna vez fueron diseñados para operación independiente ahora están cada vez más conectados por medio de software y redes inteligentes, formando el base de la Internet industrial de las cosas (IIoT).

IIoT no es solo una nueva tecnología si no que se refiere a la cadena de valor de un producto completo impactando en todos los sectores del mundo industrial modificando de manera significativa los procesos en cada etapa del ciclo de vida de un producto, incluyendo como es diseñado, hecho entregado, vendido y mantenido. De igual manera que en IoT, estamos en las primeras fases del IIoT.

5.2. IoT y IIoT Similitudes y diferencias

Hay muchas similitudes entre ambos mundos, sin embargo, en el caso de IIoT, está estrictamente relacionado con el mundo industrial, debido a lo cual lo hace tener una serie de características especiales, entre las que podemos destacar:

- La ciberseguridad es un asunto critico en cualquier solución digital, pero su aplicación en el sector industrial requiere especial atención. Esto es debido a que los dispositivos y sistemas OT en la industria tienen un ciclo de vida mucho mayor y, en muchas ocasiones, con hardware antiguo y sistemas operativos que no están diseñados para su conexión a Internet. Esto implica que estén aislados en una red protegida mediante un firewall del mundo exterior.

- Es critico asegurar que los dispositivos industriales se mantengan en funcionamiento ya que cualquier caída del servicio puede suponer importantes costes económicos.

- Las soluciones IIoT deben coexistir en un entorno en la que hay mucha cantidad de tecnologías de operación antiguas, diferentes dispositivos que actúan como fuentes de datos (SCADA, PLC, etc.), varios protocolos y los sistemas corporativos de back office.

- Las redes industriales están especializadas y soportan miles de controladores, robots y diferente maquinaria. Las soluciones de IIoT deben ser capaces de escalar a ese número de elementos de manera transparente.

- Los dispositivos físicos en el mundo industrial son más complejos y tienen un mayor rango de tipologías en comparación al mercado de consumo general.

- La robustez, resistencia y fiabilidad tienen un mayor peso en este sector que en el sector de consumo, donde la usabilidad y la experiencia de usuario tienen una gran importancia.

- Los sistemas industriales han de ser muy flexibles y son reprogramados y reconfigurados con frecuencia para adaptarse a los nuevos procesos, lo cual obliga al mundo IIoT a tener esta misma característica.

- La propiedad intelectual tiene un peso capital en el sector industrial, siendo el punto diferenciador de muchas compañías en el mercado, la cual no puede ponerse en peligro.

5.3. IT/OT

Históricamente, las áreas de IT (Information Technology) y OT (Operational Technology) eran consideradas como segmentos de mercado distintos, aunque en los últimos años la interacción entre ambos ha aumentado considerablemente. Los entornos SCADA (Supervisory Control and Data Acquisition), los dispositivos PLC (Programmable Logic Control), los sensores y actuadores recopilaban datos dentro de un fabrica dentro de una red protegida. Estos datos se mantenían en formatos propietarios, con unos casos de uso muy limitados y siempre tenían una función reactiva.

La integración de ambas áreas proporciona unas nuevas oportunidades de beneficio para las empresas, entre los que podemos destacar:

- Optimización de los procesos de negocio: las decisiones pueden ser tomadas en tiempo real dado que se dispone de la información detallada al respecto.
- Reducción de costes operativos.
- Nuevas posibilidades de beneficio: esta integración proporciona un amplio rango de oportunidades para la creación de oportunidades de beneficio.

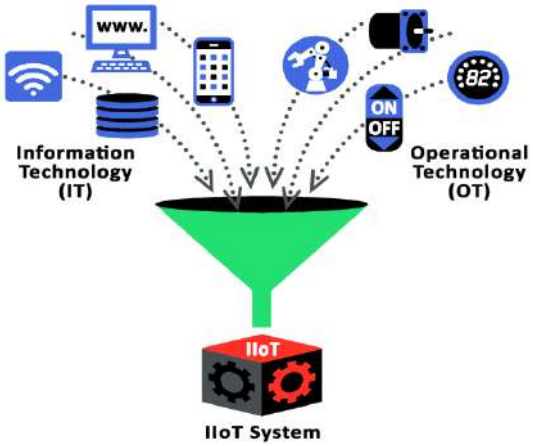


Figura 18 – Integración IT/OT

No obstante, esta integración también se enfrenta a diversos retos en áreas como la seguridad, la integración y la producción. Entre estos retos destacamos:

- Integración compleja de dispositivos para despliegue masivo
- Transmisión de datos inestable en entornos extremos: el rendimiento inalámbrico y la estabilidad se ven afectados significativamente por factores ambientales, así como por el exceso de calor generado por equipos e infraestructura.
- Mantenimiento del tiempo de actividad en ubicaciones remotas: las plataformas informáticas perimetrales desplegadas por empresas de servicios de comunicación y de servicios públicos pueden estar ubicados en sitios remotos, lo que hace muy costoso los mantenimientos rutinarios.
- Aumento de las amenazas de ciberseguridad: un ciberataque puede provocar pérdidas significativas causadas por tiempo de inactividad o interrupción de la producción

5.4. Riesgos de seguridad en IIOT

Según varios estudios más del 25% de los ataques que se producen contra las empresas tendrán como destino las infraestructuras de IoT de las mismas, pero dentro de los presupuestos de las mismas apenas un 10% es dedicado a la seguridad de estos entornos. El espionaje o el sabotaje y demás motivaciones están a la orden del día. Es importante destacar también que los ataques ejecutados por entes como los países pueden tener un impacto muy superior al inicialmente previsto.

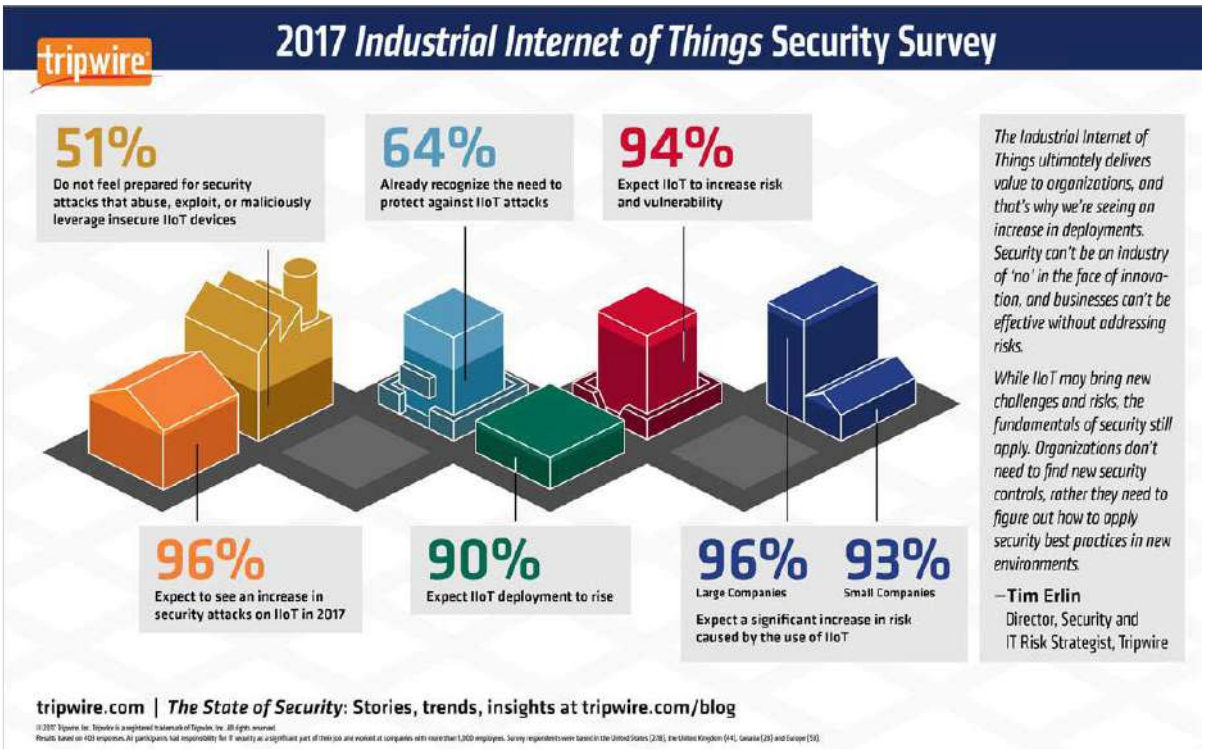


Figura 19 – Evolución de la seguridad en IIoT

El objeto principal de estos ataques son los sistemas de control industrial (ICS), PLC y sistemas SCADA. La adopción de la conectividad IP entre los dispositivos ha aumentado los riesgos de seguridad, lo cual hace de los sistemas ICS uno de los objetivos más vulnerables. Entre los ataques más comunes están:

- Ataques Man-in-the-middle
- Ataques de control de dispositivos
- Ataques de denegación de servicio
- Denegación de servicio permanente

5.5. Requisitos de seguridad en IIoT

La infraestructura IIoT debe estar protegida por una solución de seguridad integral (desde el dispositivo a la nube) que no interrumpa las operaciones, la confiabilidad o la rentabilidad del servicio. Una solución práctica y simple, pero segura, que permita su fácil implantación en el entorno productivo puede ser más eficaz que una más compleja cuya gestión y despliegue sea compleja de llevar a cabo.

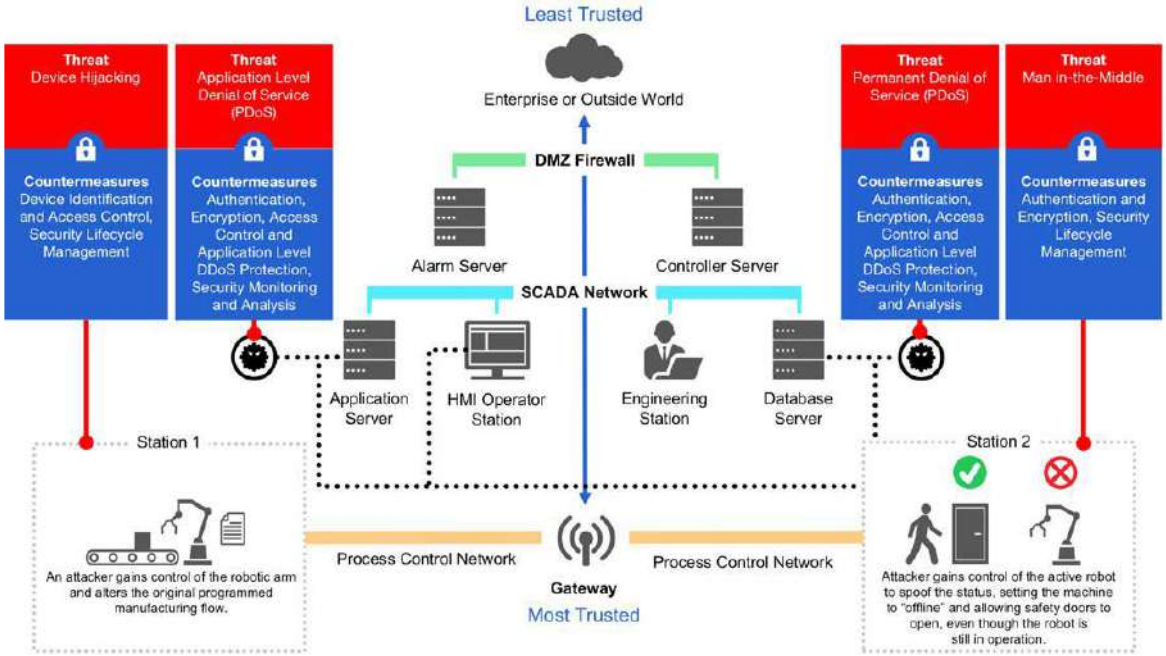


Figura 20 IIoT – Visión de la arquitectura

Cualquier solución que se aplique en este entorno ha de tener, al menos las siguientes características:

Integridad del firmware y arranque seguro: el arranque seguro utiliza técnicas de firma de código criptográfico, asegurando que un dispositivo solo ejecute el código generado por el OEM del dispositivo u otra parte confiable. El uso de la tecnología de arranque seguro evita que los piratas informáticos reemplacen el firmware con conjuntos de instrucciones maliciosas, evitando así los ataques. Desafortunadamente, no todos los conjuntos de chips IIoT están equipados con capacidades de arranque seguro. En tal escenario, es importante asegurarse de que los dispositivos IIoT solo puedan comunicarse con servicios autorizados para evitar el riesgo de reemplazar el firmware con conjuntos de instrucciones maliciosas.

Autenticación mutua: cada vez que un dispositivo se conecta a la red se debe autenticar antes de recibir o transmitir datos. Esto asegura que los datos se originen de un dispositivo legítimo y no en una fuente fraudulenta. La autenticación segura mutua, donde dos las entidades (dispositivo y servicio) deben probar su identidad mutua ayuda a proteger contra ataques maliciosos. Los algoritmos criptográficos utilizando claves simétricas o claves asimétricas pueden utilizarse para la autenticación bidireccional.

Comunicación segura (cifrado de extremo a extremo): las capacidades de comunicación segura protegen los datos en tránsito entre un dispositivo y su infraestructura de servicio (la nube). El cifrado garantiza que solo aquellos con una clave de descifrado secreta puedan acceder a los datos transmitidos.

Figura 21 IoT – Protección End To End

Monitoreo y análisis de seguridad: el monitoreo de seguridad captura datos sobre el estado general de un sistema industrial, incluidos los dispositivos el tráfico de conectividad. Luego, los datos se analizan para detectar posibles violaciones de seguridad o posibles amenazas al sistema. Una vez detectado, se debe ejecutar una amplia gama de acciones formuladas en el contexto de una política general de

seguridad del sistema, como revocar las credenciales del dispositivo o poner en cuarentena un dispositivo IoT basado en un comportamiento anómalo. Este ciclo automático de monitoreo, análisis y acción puede ejecutarse en tiempo real o en una fecha posterior para identificar patrones de uso y detectar posibles escenarios de ataque. Es fundamental asegurarse de que los dispositivos estén protegidos contra posibles manipulaciones, tanto de los dispositivos como de los datos, lo que podría dar como resultado un informe incorrecto de eventos.

Gestión del ciclo de vida de seguridad: la función de gestión del ciclo de vida permite a los proveedores de servicios y a los fabricantes controlar los aspectos de seguridad de los dispositivos IoT cuando están en funcionamiento. El reemplazo rápido de las claves del dispositivo en tiempo real durante la recuperación ante desastres garantiza una interrupción mínima del servicio. Además, el desmantelamiento seguro del dispositivo garantiza que los dispositivos desechados no se reutilizarán y explotarán para conectarse a un servicio sin autorización.

6. IoT. Ejemplo de planta conectada

En este capítulo vamos a ver a alto nivel el despliegue de una solución de planta conectada que nos permite la gestión remota y una gestión analítica avanzada de las líneas de producción industrial. El motivo de negocio que se persigue mediante esta tecnificación de la planta es incremento de la eficacia del equipamiento, la reducción de los costes de mantenimiento, el incremento de la calidad de los productos y la mejora de otros aspectos en la eficacia operativa.

Dentro de la planta donde se ha implementado esta solución, se ha sensorizado todos los elementos de la cadena de producción de la pieza, desde la maquina cortadora del metal, la moldeadora, la prensa hasta pulidora ubicada al final de la cadena. De esta manera es posible no solo tener una trazabilidad de una pieza desde el mismo momento que empieza su fabricación, sino que con su análisis en las herramientas cloud que se utilizan, poder medir métricas como la calidad de la soldadura o presión la aplicada, de forma que podemos tener una información en tiempo real de la calidad de nuestros productos, pudiendo corregirlos antes de que lleguen al mercado.

6.1. Planta Industrial conectada

Para la configuración de este entorno se han utilizado dos tecnologías principalmente. En la parte que se ubicaría en la planta se utiliza los elementos proporcionados por Ignition OPC. Para la parte del tratamiento y explotación de la información usaremos los elementos que Microsoft Azure nos proporciona dentro de su catálogo de productos en el ámbito del IoT.

Ignition OPC es un software de servidor desarrollado por Ignition Automation que actúa como hub para todos los elementos que se encuentran desplegados en una planta de producción proporcionando una total integración de los sistemas, independientemente de la marca, modelo o plataforma de la que dispongamos.

Integra todo lo necesario para crear todo tipo de aplicación industrial, tanto a nivel de equipos de escritorio como displays industriales y pantallas móviles, proporcionándonos datos en tiempo real a cualquier potencial usuario, en cualquier lugar y en cualquier dispositivo que disponga de un navegador web.

La conexión entre la parte on-premises y Azure se ha securizado mediante la creación de una vpn entre las redes de cada una de las plantas y el cloud, utilizando el servicio de Azure Firewall que la solución nos ofrece.

Adicionalmente y dada la existencia de un tenant de O365 en la organización, hemos aprovechado los usuarios y grupos de este (sincronizados mediante el servicio AD Connect) para aplicar permisos RBAC a todos los recursos ubicados en la suscripción.

En la siguiente imagen podemos ver los diferentes elementos que componen la solución y las conexiones que se establecen entre ellos.

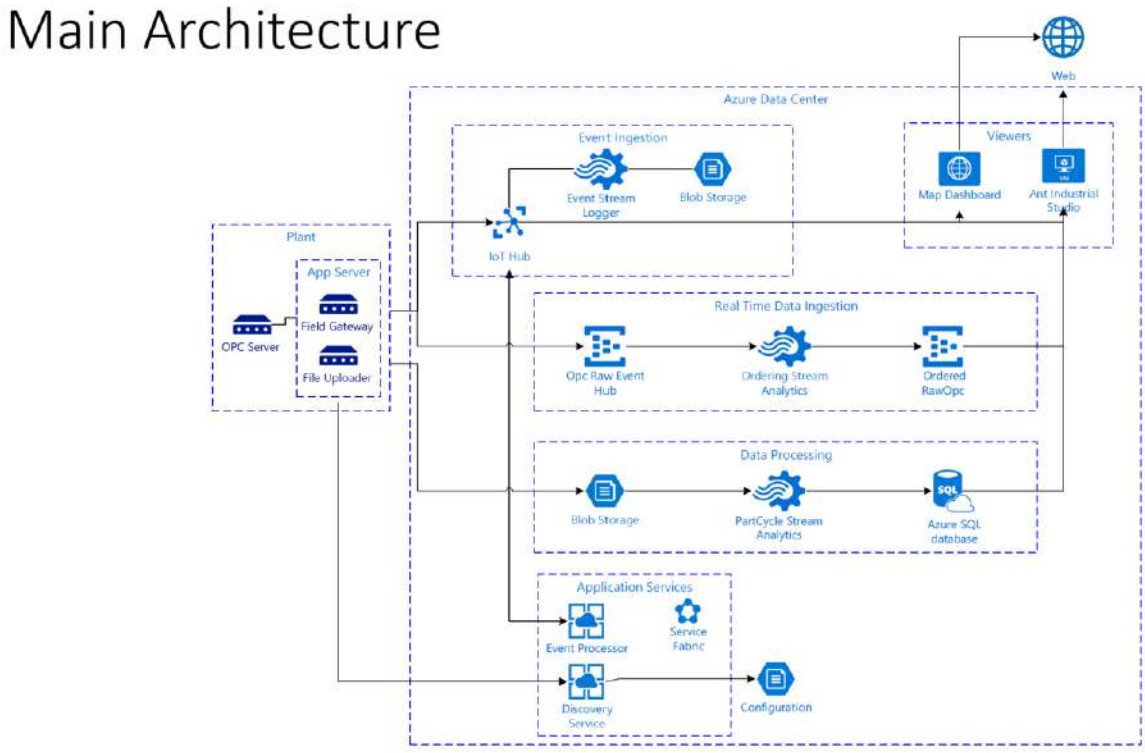


Figura 22 – Esquema de planta conectada

Planta de fabricación

Dentro de la planta de fabricación industrial, se ubican los distintos PLC (*programmable logic controller)* que recogen la información de los diferentes elementos monitorizados, los cuales están conectados al servidor OPC (en el capítulo dedicado a IIoT explicaremos el en que consiste el protocolo OPC UA).

El servidor OPC se encuentra a su vez conectado a un cliente OPC, software cuyas principales finalidades son la habilitación de las comunicaciones, el control de los dispositivos y el procesamiento de los datos del dispositivo de cara a reducir la cantidad de datos que son transferidos al backend, en este caso Azure.

Como funciones adicionales, el field gateway también se encarga del buffering de los datos, la tradición entre los diferentes protocolos y el procesamiento de las reglas de evento.

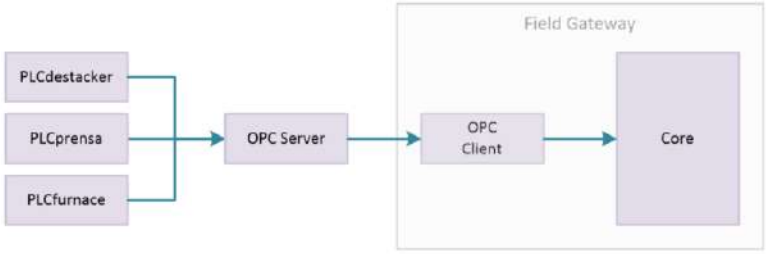


Figura 23 – Elementos de la planta conectada

Inserción de datos en tiempo real

La gestión en tiempo real de la información recibida por la planta a través de su field Gateway es recibida por el un recurso de Azure llamado Azure Event Hub. Debido a la independencia que tiene este elemento de los cuales se conectan a él, solo será necesario el despliegue de uno de ellos en nuestra plataforma cloud.

Figura 24 – Iot entrada de datos en tiempo real

Algunas de las tareas de procesamiento sobre los datos recibidos son realizadas con la ayuda de los Jobs de Stream Analytics. Estos Jobs incluyen como elementos principales un input, una query y un output. El origen de los inputs viene determinado por el origen de data stream. La query es usada para la transformación de los datos recibidos del input, siendo el output el lugar a donde se redirige el resultado de esta tarea.

Inserción de eventos

Utilizando como elemento principal de entrada y salida de las comunicaciones en el cloud, el Azure IoT Hub permite, dada su gran escalabilidad y seguridad, que una gran variedad de dispositivos se conecte a él.

El procesador de eventos está encargado de la recogida de eventos recibidos del field gateway, envío y recepción de comandos a través del IoT Hub. Para el almacenamiento de los eventos utilizamos una cuenta de almacenamiento de tipo blob.

Figura 25 – IoT Gestión de eventos

Procesamiento de datos

Dentro de este grupo de componentes cumple la función del almacenado en Azure de todos los datos provenientes del servidor OPC a través del field gateway file uploader, procesando los mismos y dando como resultado un conjunto de eventos en formato tabla. Estos conjuntos de datos son almacenados en una base de datos para su explotación con otro componente de la solución Ignition, el Ignition Industrial Studio.

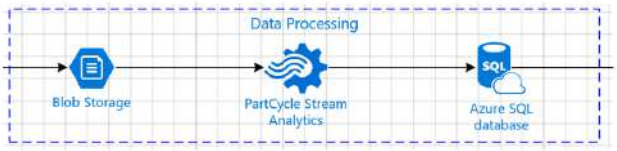


Figura 26 – IoT Proceso de datos

Este almacenamiento también recibe datos provenientes de la insercción de eventos para tareas de troubleshooting.

Servicios de Aplicación

La capa de aplicación proporciona soporte y gestión a los dispositivos conectados a la solución. Dentro de ella encontramos microservicios alojados en containers desplegados dentro de un Service Fabric. Este elemento está construido inicialmente bajo un conjunto de cinco máquinas virtuales balanceadas configurados con un scale set (crecimiento dinámico).

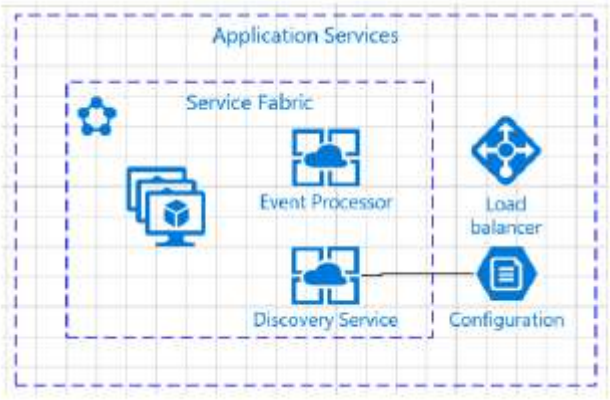


Figura 27 – IoT Servicios de aplicación

Capa de visualización

Esta capa constituye el lugar donde el usuario final interactúa con el interfaz que permite la obtención de los informes requeridos, así como la comprobación del estado general de todos los elementos que componen el sistema. Como elementos principales de la misma podemos señalar un mapa que nos permite ver el ultimo estado de los elementos de la planta así como otro que incluye la información en tiempo real o histórica que recibimos de ella.

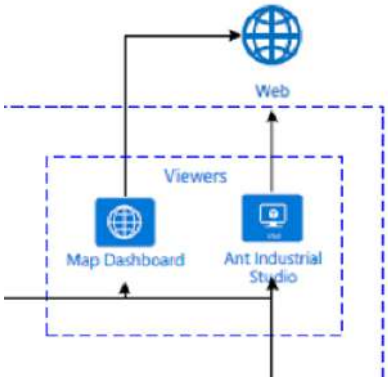


Figura 28 – IoT Capa de visualización

6.2. Arquitectura de referencia en Azure

Si consultamos la documentación relativa a las arquitecturas PaaS que nos ofrece Azure, vemos que en la que se nos presenta como referencia una estructura muy similar a la que se ha desplegado en nuestra planta de producción.

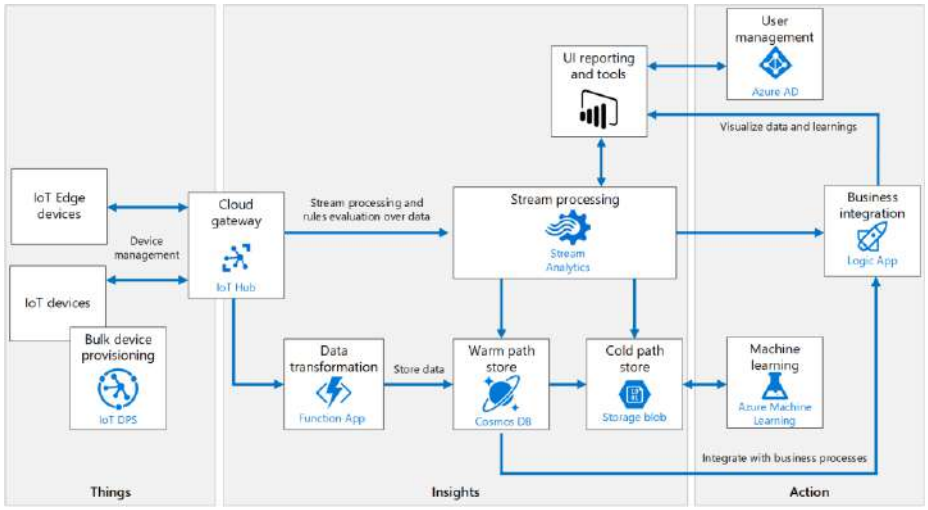


Figura 29 - IoT Arquitectura de referencia en Azure

En ella podemos distinguir tres áreas principalmente el área de las “cosas”, la cual envía datos para la generación de “conocimiento”, el cual genera “acciones” cuya finalidad es la mejora de un proceso o negocio.

Por ejemplo, un plc de unos de los dispositivos monitorizados en la planta que monitoriza la presión de una plancha envía esta información y en función de la misma podemos ver si esta es correcta o no, y en caso de ser incorrecta poder tomar las medidas oportunas para su solución.

También vemos que hay dos formas de procesar la información, las llamadas línea fría y línea caliente.

- La línea caliente analiza los datos casi en tiempo real según son recibidos. Esta ruta de acceso se implementa típicamente usando un motor de procesamiento de flujo. La salida puede desencadenar una alerta o puede escribirse en un formato estructurado que se pueda consultar mediante herramientas analíticas.

- La línea fría realiza el procesamiento por lotes a intervalos más largos (por hora o por día). La línea fría generalmente opera sobre grandes volúmenes de datos, pero los resultados no necesitan ser tan inmediatos como la ruta caliente. En la línea frío, la telemetría sin procesar se captura y luego se introduce en un proceso por lotes.

La seguridad en el entorno de Azure que nos proporciona Microsoft para IoT puede está dividida en tres áreas principales:

- **Seguridad de dispositivos**: Securizacion del dispositivo IoT durante su despliegue.
- **Seguridad en la conexión**: Asegurar que la transmisión de información entre el dispositivo IoT y el IoT Hub es confidencial y resistente a intrusos.
- **Seguridad en la nube**: Proporcionar mecanismos para asegurar la información mientras se desplaza por los recursos del cloud y en su lugar de almacenamiento.

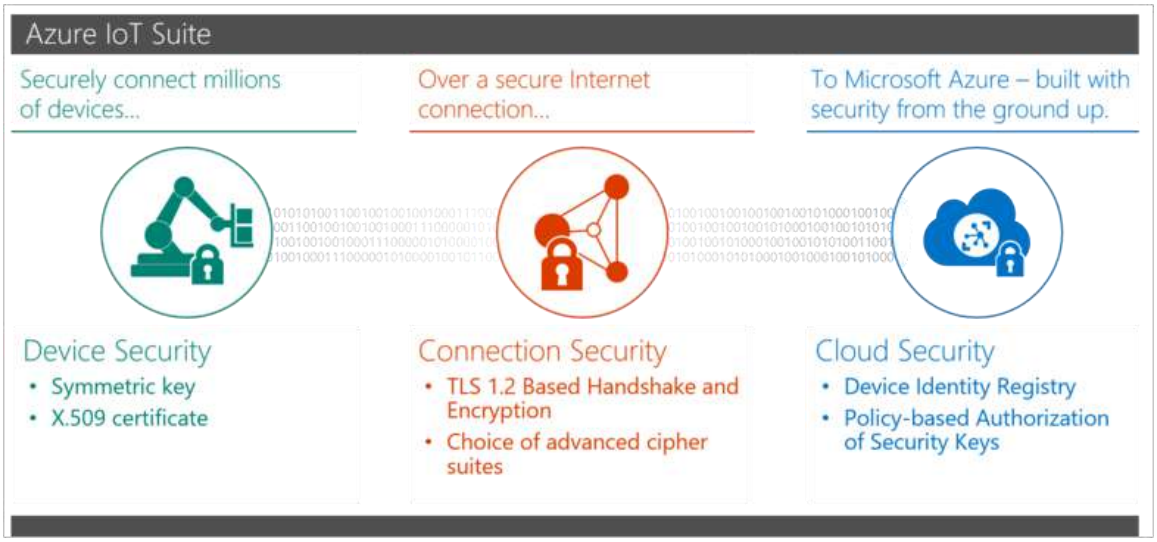


Figura 30 – Áreas de seguridad de Azure

6.3. Ignition OPC UA

Para la creación de una pequeño PoC con la cual ilustrar como implementar el funcionamiento de unos dispositivos IIoT de ejemplo hemos utilizado la versión de evaluación del producto Ignition OPC UA.

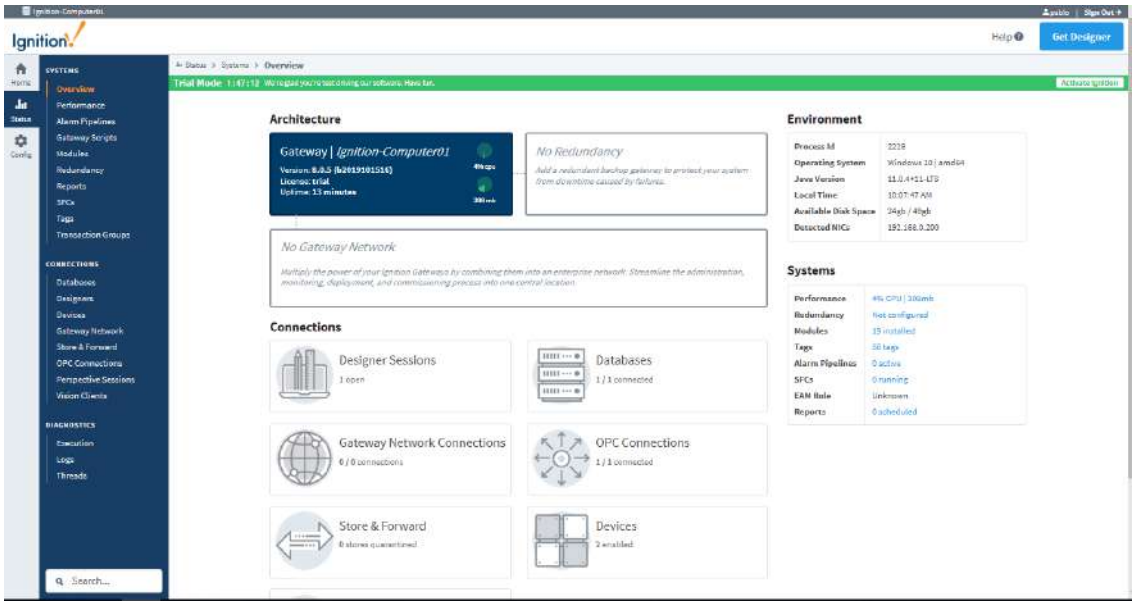


Figura 31 – IIoT Menú Principal Ignition OPC UA

Una vez que hemos accedido a la aplicación, damos de alta un par de dispositivos para que nos reporten datos a la plataforma. Hemos elegido un par de elementos de demo que vienen con la solución.

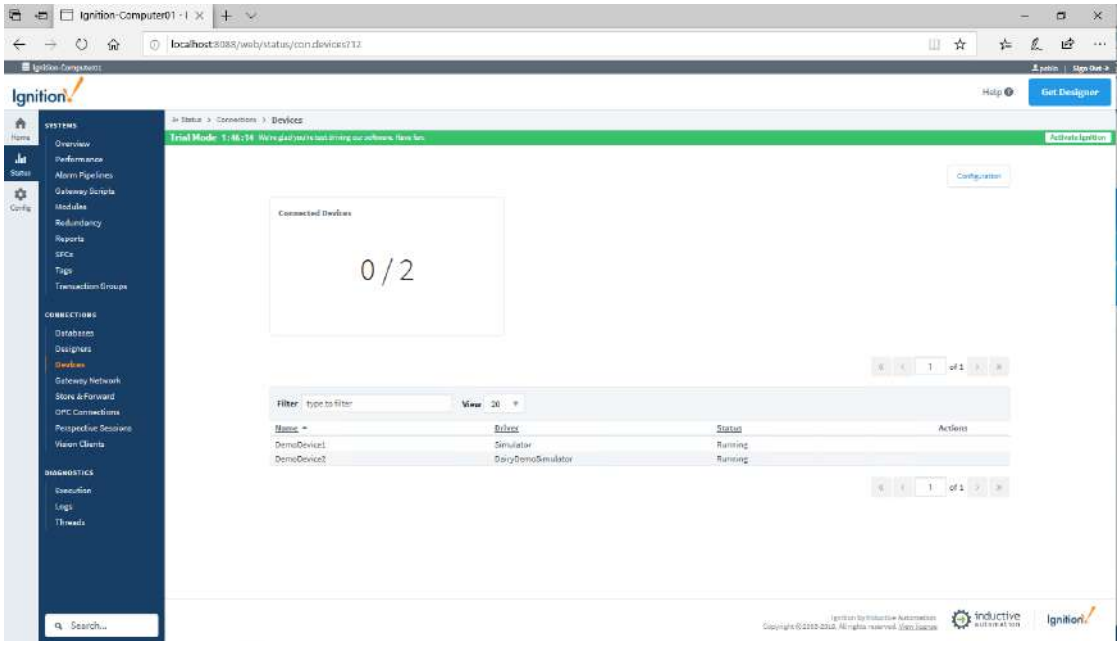


Figura 32 – IioT Dispositivos creados en la plataforma

Dentro de la herramienta de diseño que proporciona hemos diseñado un formulario que nos muestra los valores en tiempo real de dos valores que mide el dispositivo creado. En la gráfica hemos añadido una gráfica que nos muestra los valores históricos que han tenido los sensores a lo largo del tiempo.

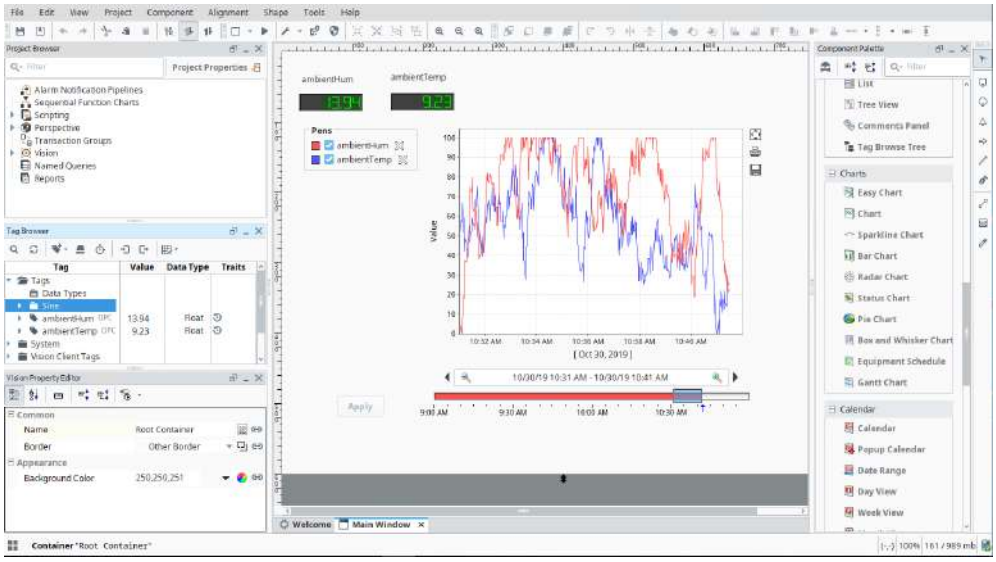


Figura 33 – IIoT Datos en tiempo real e históricos

En la última imagen que adjunto se muestra una línea de fabricación completa con todos los sensores desplegados en ella junto con la información que están proporcionando.

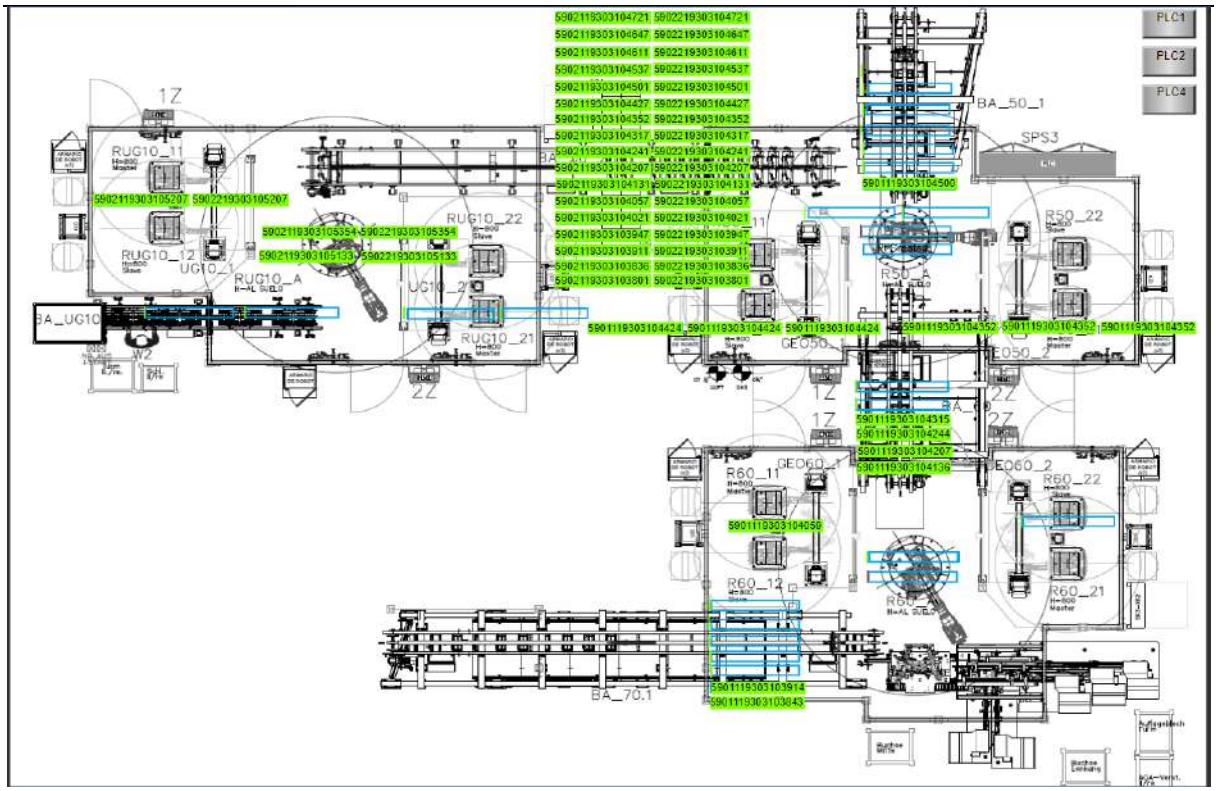


Figura 34 IIoT Esquema de planta sensorizada

6.4. Protocolo OPC Classic / OPC UA

Ningún otro estándar de comunicaciones industrial ha alcanzado tal nivel de aceptación a través de las diferentes industrias y fabricantes de equipamiento del que ha tenido OPC Classic, Es utilizado para la interconexión de una larga variedad de sistemas industriales y de negocio, como por ejemplo SCADA, SIS´s, PLC.

La razón de este éxito se sustenta en un principio, y es que es el único interfaz real que puede ser usado para comunicar con diferentes dispositivos y aplicaciones industriales, sin tener en cuenta el fabricante, el software o los protocolos usados en el sistema.

OPC Classic

Antes de la aparición de OPC, los desarrolladores de aplicaciones tenían que desarrollar drivers de comunicaciones específicos para cada sistema de control con el cual se quisiera conectar.

OPC no elimina la necesidad de tener drivers si no que cada vendedor solo necesita implementar los interfaces necesarios para trabajar con OPC, los cuales suelen ser un OPC server para su producto en concreto y un OPC cliente que interactúa con los OPC servers de otros vendedores.

Inicialmente, el estándar OPC estaba basado en el sistema operativo de MSFT y en OLE (Object Linking and Embedding) para el control de procesos. En el año 2006, la fundación OPC lanzo las especificaciones para OPC UA, las cuales utilizan una arquitectura orientada al servicio. En ellas se implementan las siguientes acciones:

- Superar las limitaciones relativas a la arquitectura que tenía OPC Classic.
- Nuevas necesidades que han surgido en aspectos relativos a la seguridad y el modelado de datos.
- Proporcionar una plataforma más escalable y flexible.

- Construcción en una plataforma independiente que no está enlazada con una tecnología especifica.

En la actualidad, las siglas OPC están identificadas con *Open Platform Communcations.* Una de las cosas que más podemos destacar de OPC es que es un API más que un protocolo. Proporciona un mayor nivel de abstracción que los protocolos de comunicación, como pueden ser Ethernet o TCP/IP.

El siguiente esquema muestra las diferentes capas del OPC Classic junto con los protocolos subyacentes protocolos de comunicaciones, COM, DCOM y RPC.

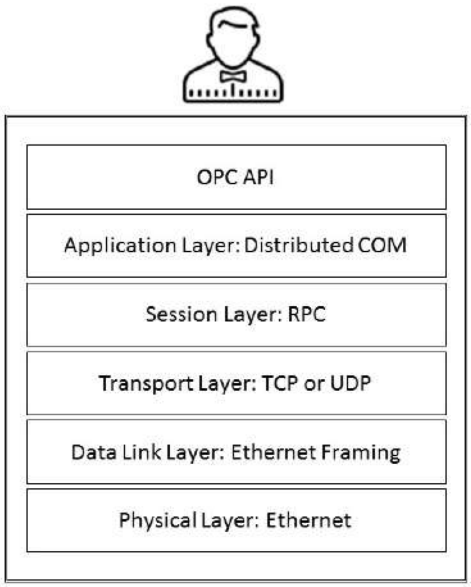


Figura 35 – Capas de OPC Classic

- El modelo OPC Classic tenía varias limitaciones, entre las que podemos destacar:
- Estaba construido basado en tecnologías MSFT.
- El tráfico del protocolo COM necesita un número indeterminado de puertos de red abiertos lo cuales, a menudo, están bloqueados por los firewalls.
- DCOM y RPC son unos mecanismos pesados y complicados. Los objetos DCOM a menudo tienen problemas de rendimiento y son difíciles de mantener.

OPC UA

La primera respuesta de la fundación OPC para eliminar las restricciones relacionadas con el uso de las tecnologías COM y DCOM fue el desarrollado de OPC XML-DA. Básicamente mantenía las características principales de OPC, pero adoptando una infraestructura de comunicación que no está enlazada con un proveedor o una determinada plataforma de software.

El protocolo OPC-UA fue desarrollado con el objetivo de reemplazar todas las versiones existentes basadas en COM y resolver los problemas de rendimiento y seguridad, satisfaciendo a su ver la necesidad de la creación de modelos de datos extensibles. Está basado en un objetivo orientado al servicio, el cual está definido por el estándar IEC 62451. Entre los principales retos están:

- El uso de componentes OPC en entornos no Windows
- Hacer posible colocar sus principales componentes en dispositivos más pequeños
- Implementar comunicaciones estándar a través del firewall.

Desde un punto de vista técnico, OPC UA funciona de la siguiente forma:

- La API aísla el código del cliente y el servidor desde la pila OPC UA

- La pila OPC UA convierte las llamadas de la API en mensajes
- La pila OPC UA recibe mensajes enviándolos al cliente o al servidor a través de la API.

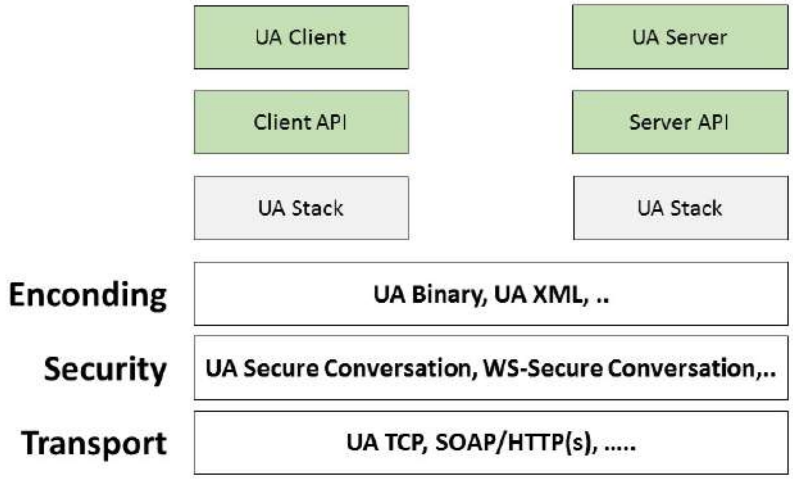


Figura 36 – Pila OPC UA

Modelo de seguridad en OPC UA

Este modelo esta implementado a través de la definición de un canal seguro en la cual se basan las sesiones. Un canal seguro hace que el intercambio de información sea seguro de diferentes maneras:

- Asegura la integridad de los datos mediante el uso de firmas digitales.
- Asegura la confidencialidad a través de la encriptación.
- Lleva a cabo la autenticación y la autorización mediante el uso de certificados X.509.

Los elementos que están involucrados en este modelo son: la capa de aplicación, la capa de sesión y la capa de transporte:

- La capada de aplicación es utilizada para transmitir la información entre los clientes y los servidores que han establecido una sesión OPC UA
- Una sesión OPC UA es establecida en un canal seguro (localizado en la capa de comunicación), el cual lo hace seguro para la transmisión de la información.
- La capa de transporte es la responsable de transmitir y recibir los datos a través de un socket.

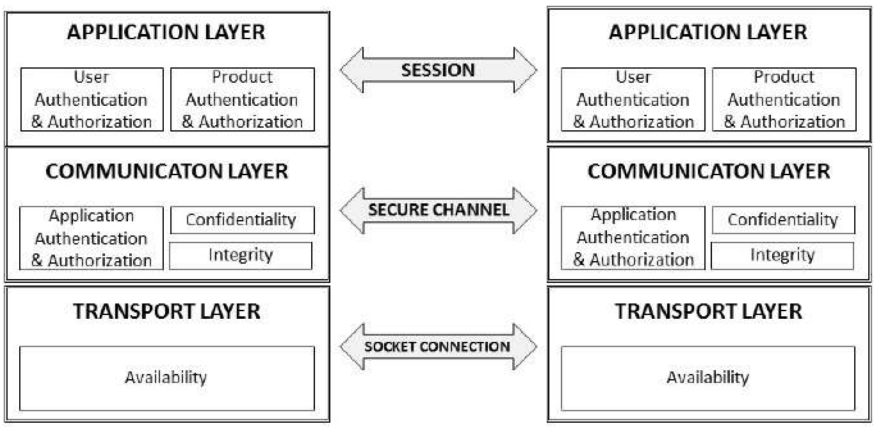


Figura 37 – Capa de seguridad en OPC UA

La creación de un canal seguro está basada en los endpoints, y cada servidor ofrece uno o más endpoints, los cuales tienen las siguientes características:

- Endpoint URL: esta dirección de red es usada por el cliente para establecer un canal seguro
- Certificado de aplicación de instancia de servidor: es la clave pública del servidor usada por el cliente para hacer posible el intercambio seguro de información.
- Política de seguridad: es un conjunto de algoritmos usados en los mecanismos de seguridad, como puede ser AES.
- Modo de seguridad: asegura la autenticación a nivel de aplicación. Hay diferentes modelos, como, por ejemplo, SignAnEncript, Sign o None.
- Autenticación: son los mecanismos usados para autenticar un usuario durante la creación de una sesión mediante el uso de una pareja de usuario y password, un certificado o utilizando autenticación anónima.
- Protocolo transporte: especifica el protocolo de transporte usado.

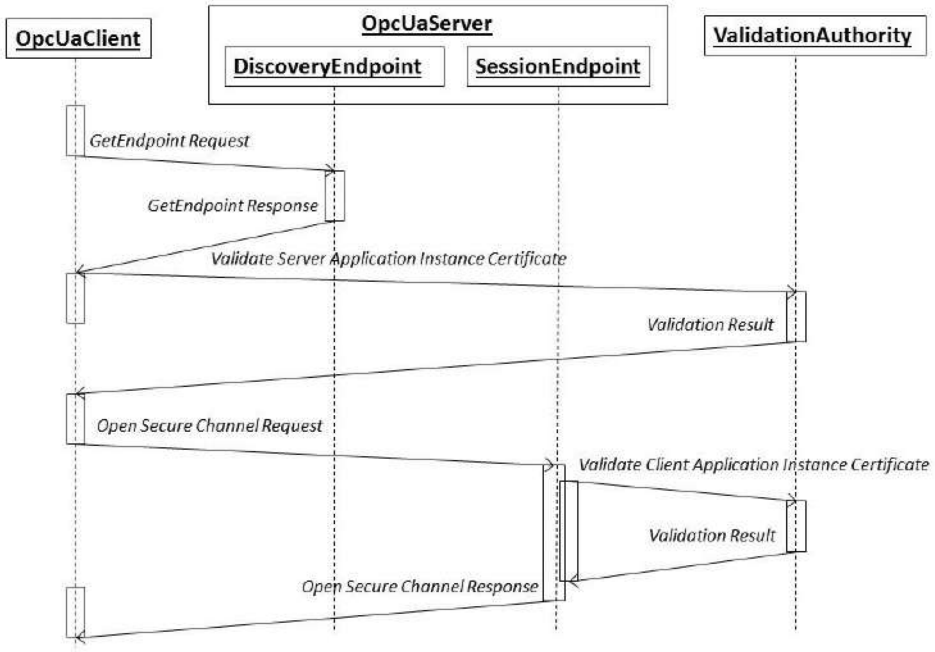


Figura 38 – Pasos 1 y 2 de la secuencia de seguridad

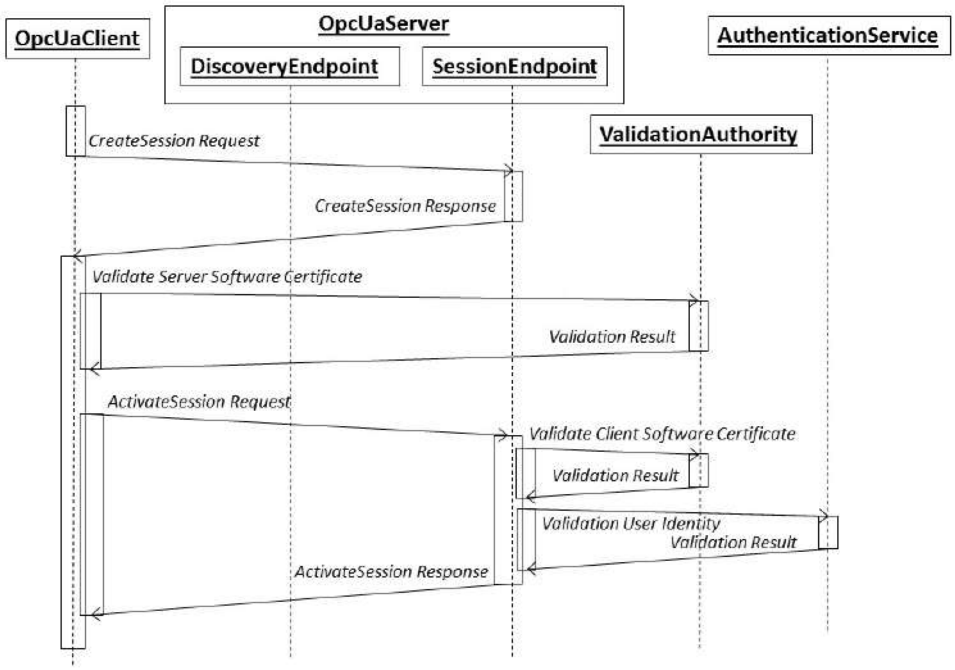


Figura 39 – Pasos 3 y 4 de la secuencia de seguridad

7. IoT. Modelos conceptuales de IIoT en Cloud.

En el siguiente capítulo vamos a ver tres ejemplos operativos desplegados en el servicio cloud de MSFT (Azure) que nos permitirán obtener una visión de la interacción de los elementos del mundo IoT/OT con los del mundo cloud, y como a través de esa relación, las empresas pueden obtener ventajas de su utilización.

Para el despliegue de estas soluciones hemos utilizado una suscripción de Azure de tipo PAYG (Pay As You Go) que he creado para poder alojar los recursos que he necesitado desplegar. Este tipo de suscripción nos factura en función de los elementos creados y el tiempo que estos están activos en la misma.

7.1. Planta conectada

Esta implantación está basada la arquitectura de referencia de Azure para entornos de IoT industrial. En este despliegue se han utilizado los siguientes elementos:

- *Industrial device interoperability*
  - *Connect to industrial assets with an OPC UA interface.*
  - *Use the simulated production lines (running OPC UA servers in Docker containers) to see live telemetry.*
  - *Monitor OPC UA servers from a cloud dashboard.*
- *Remote management*
  - *Configure your OPC UA assets from the cloud dashboard (call methods, read, and write data).*
  - *Publish and unpublish telemetry data from your OPC UA assets from a cloud dashboard.*
- *Cloud dashboard*
  - *View telemetry previews.*
  - *View trends in telemetry data and create correlations using the Time Series Insights Explorer dashboard.*

  - *See calculated Overall Equipment Efficiency (OEE) and Key Performance Indicators (KPIs).*
  - *View industrial asset hierarchies in a tree topology and on an interactive map.*
  - *View, acknowledge, and close alerts.*
- *Azure Time Series Insights*
  - *Store, visualize, and query large amounts of time-series data.*
  - *Perform deep, real-time analysis of your device data.*
- *Configurable threshold-based rules for alerts*
- *End-to-end security*
  - *Configure security permissions for users using Role-Based Access Control (RBAC).*
  - *End-to-end encryption with OPC UA authentication (using X.509 certificates) as well as security tokens.*

Para comenzar su despliegue hemos de indicar los detalles de la suscripción a utilizar como se muestra en la siguiente imagen

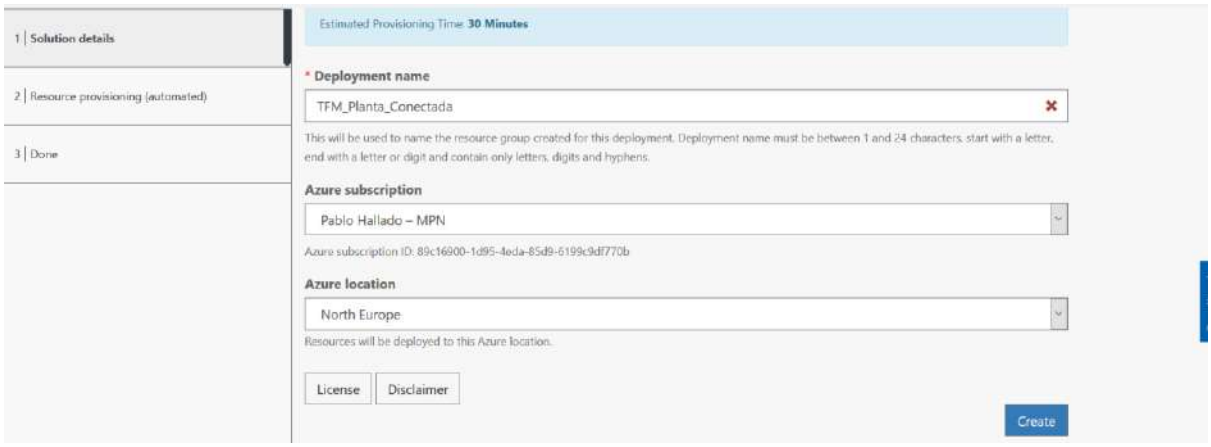


Figura 40 – Datos Suscripción Planta Conectada

Una vez proporcionados comienza la creación de esta (unos 30 minutos aproximadamente) tras los cuales nos aparecerá como disponible para poder acceder a ella.

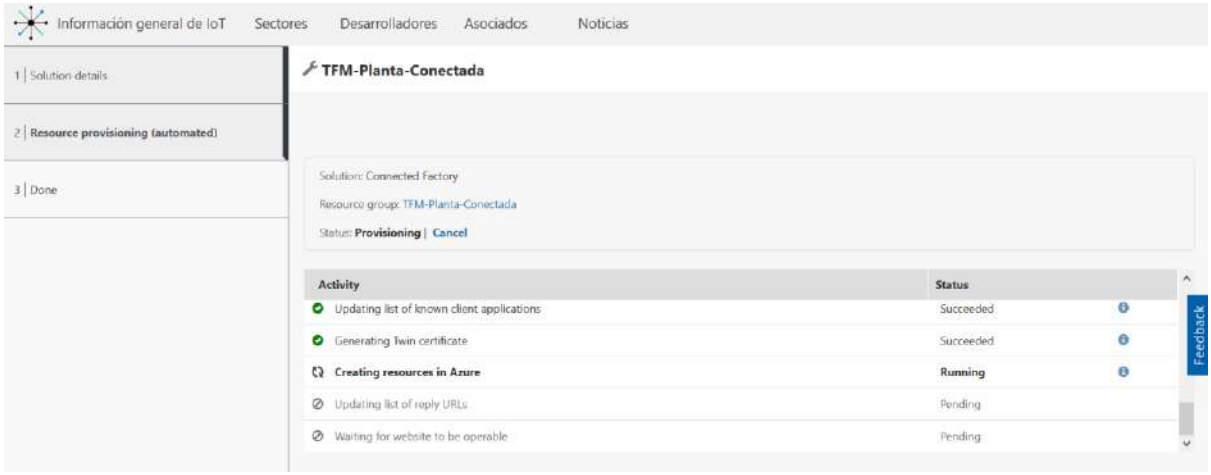


Figura 41 – Despliegue Planta Conectada

Una vez terminado el proceso ya podemos acceder a ella pulsando en la imagen correspondiente.

Figura 42 – Acceso a la Planta Conectada

Si accedemos a la suscripción de Azure veremos que se nos ha creado un grupo de recursos (Resource Group) dentro del cual se nos habrán colocado todos los elementos anteriormente indicados.

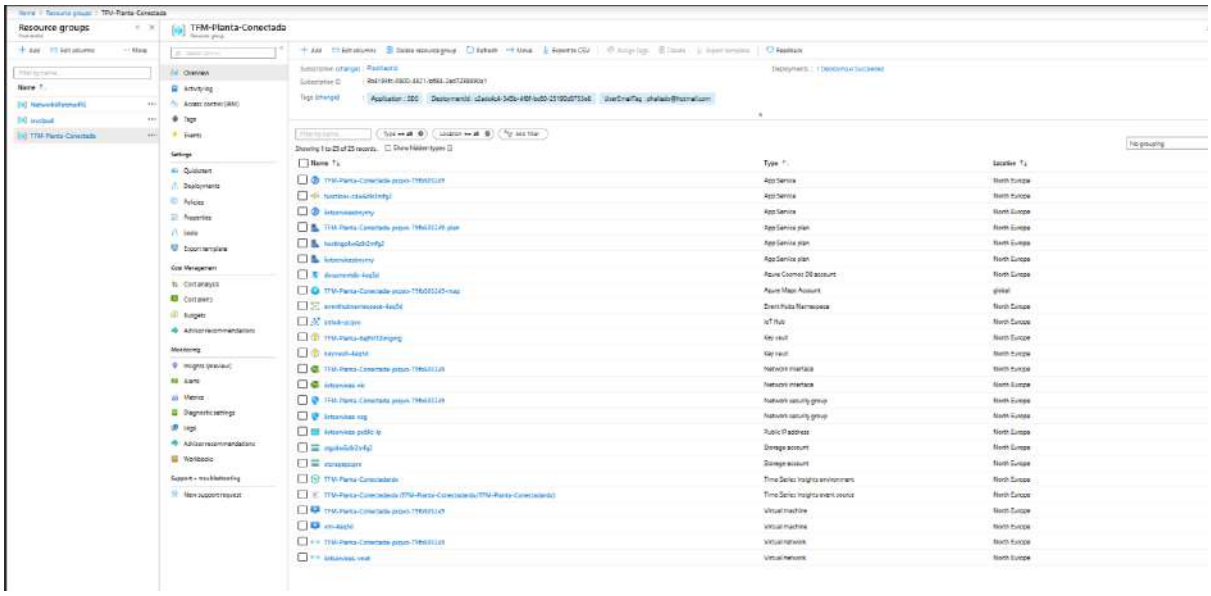


Figura 43 – Planta Conectada. Elementos creados en Azure

La página de acceso a la solución nos muestra en su parte izquierda las distintas ubicaciones de las plantas, así como el elemento que dentro de ellas se fabrica. Podemos ver el estado de cada una de las líneas de fabricación y un resumen de las ultimas alertas aparecidas en el sistema.

Figura 44 – Página principal de la planta conectada

Apreciamos en el pie de la ventana unos indicadores que nos muestran el estado general de la solución en función de varios valores como la eficiencia general o el rendimiento.
Navegando por los deferentes elementos de la pantalla podemos llegar al nivel de monitorización más bajo, como se puede ver en las siguientes imágenes. A cada nivel de detalle que nos desplazamos veremos información de los componentes que se encuentran a ese nivel.

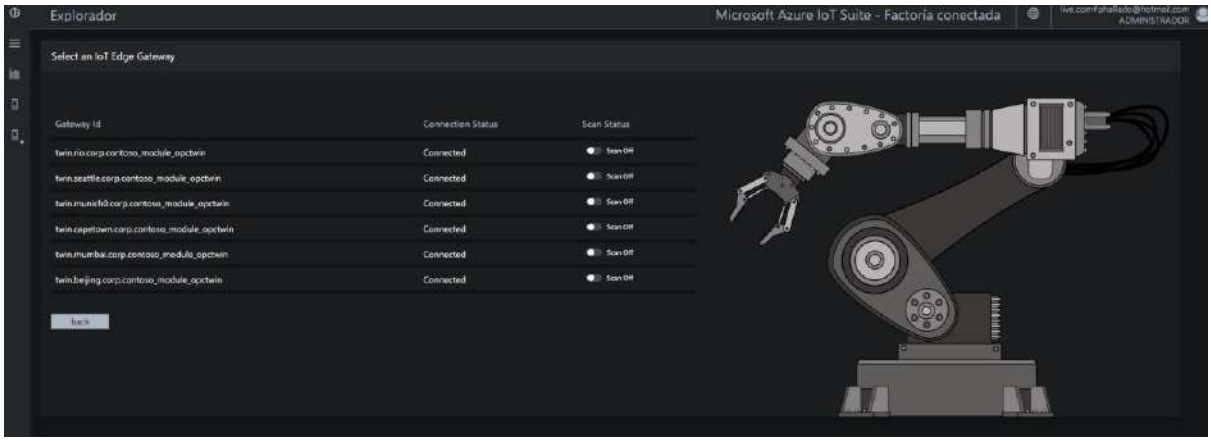


Figura 45 Planta Conectada – IoT Edge Gateway

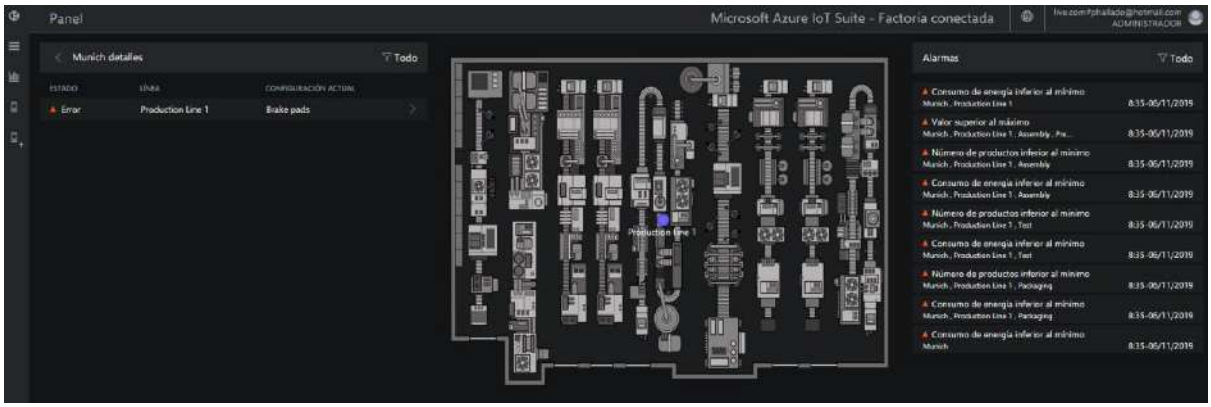


Figura 46 – Planta Conectada – Detalle de la línea de producción

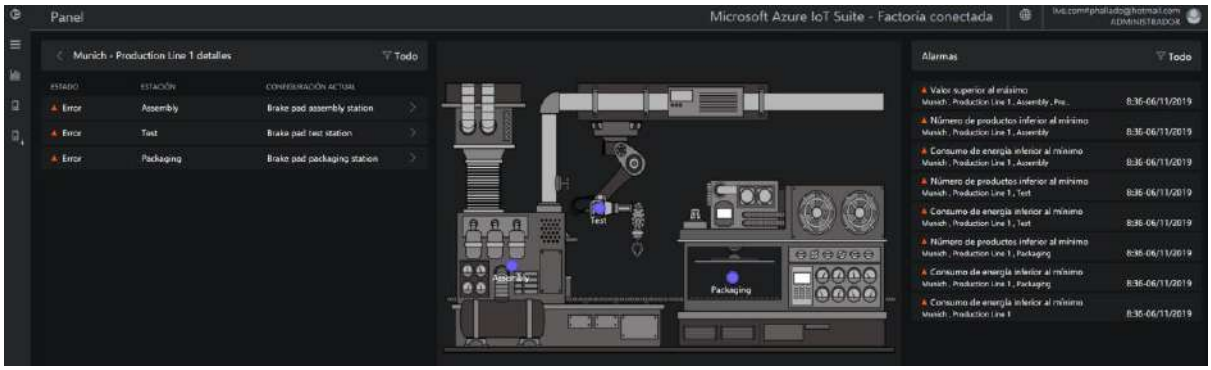


Figura 47 – Planta Conectada – Elementos de la línea de producción

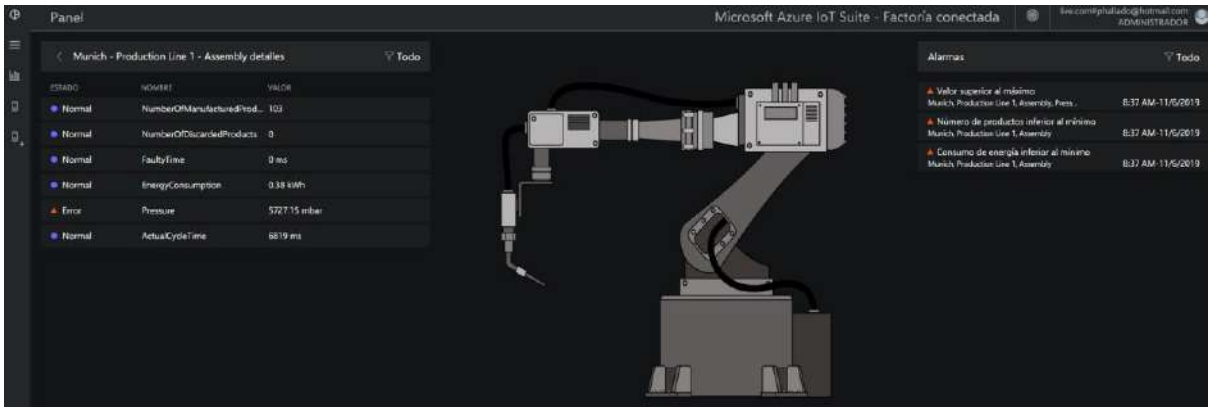


Figura 48 – Planta Conectada – Detalles del elemento de ensamblado (alarmas)

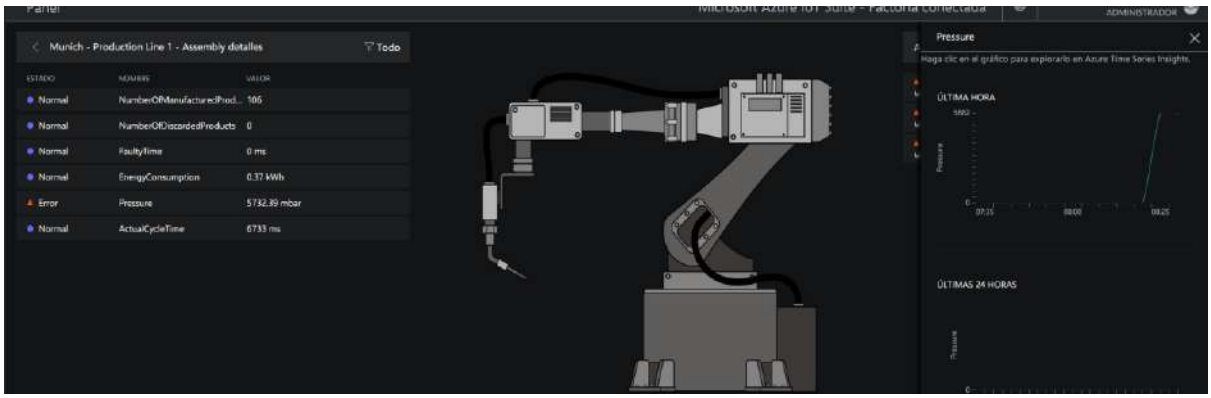


Figura 49 – Planta Conectada – Detalles del elemento de ensamblado (grafica)

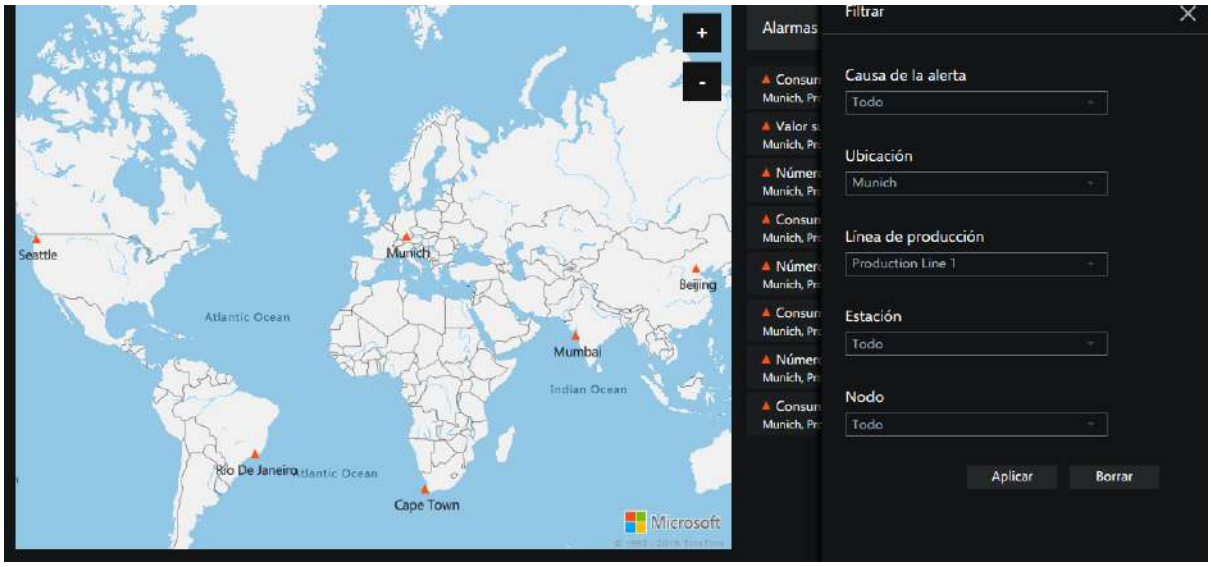


Figura 50 – Planta Conectada – Filtrado desde la página principal

Como vemos en la imagen anterior, desde la página principal de la solución podemos filtrar el estado de los elementos para ver su estado sin tener que desplazarnos dentro de ellos.

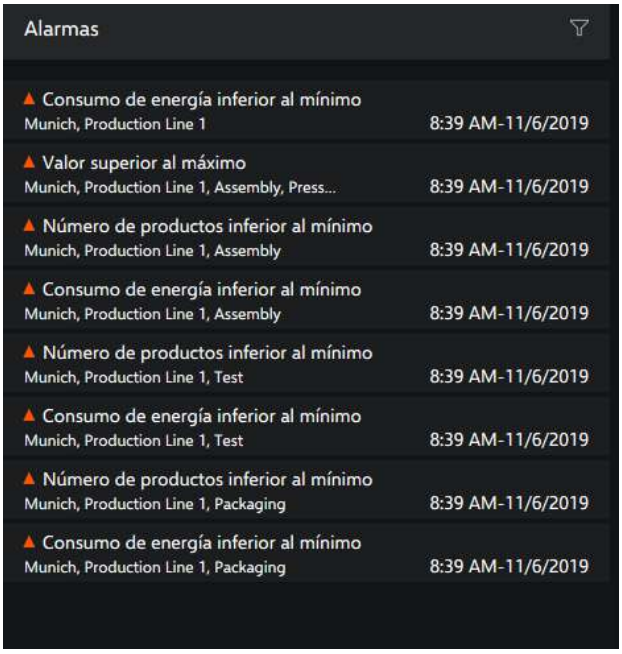


Figura 51 – Planta Conectada – Resultados filtrados desde la página principal

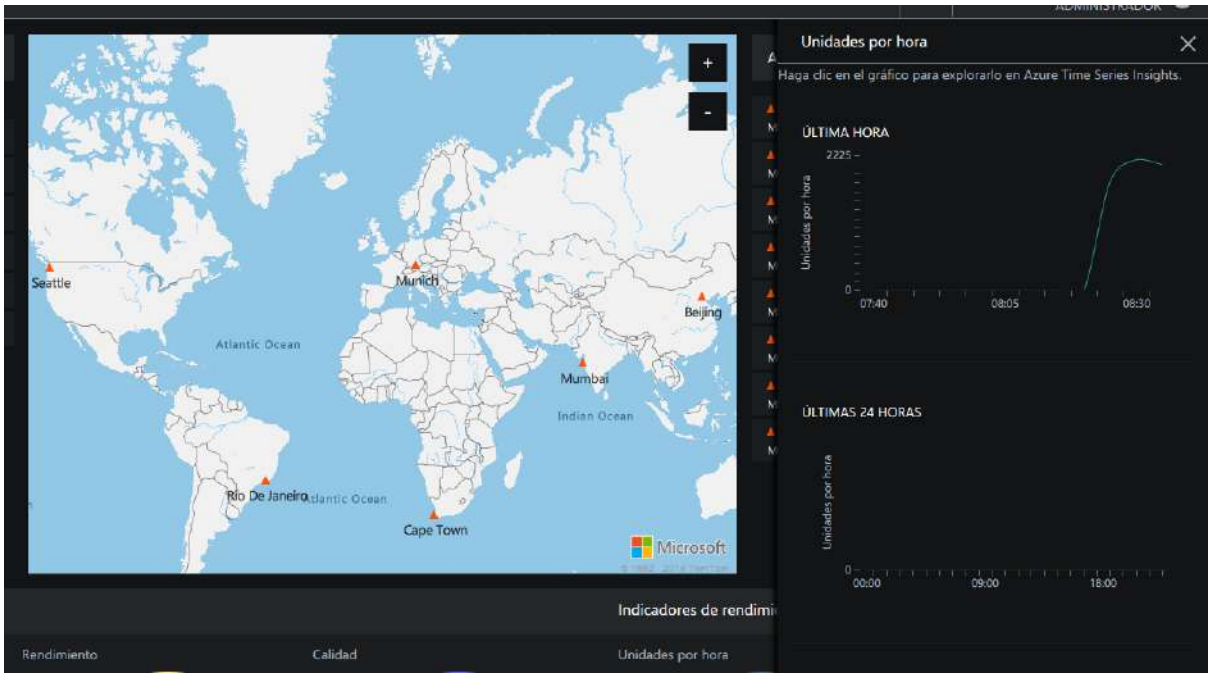


Figura 52 – Planta Conectada – Estado desde la página principal (grafica)

7.2. Remote Monitoring

En siguiente ejemplo vamos a mostrar otra solución que mediante la combinación del mundo cloud con el IIoT nos ofrecen una solución de monitorización remota, que permite el control de diversos elementos, como, por ejemplo, distintos valores de su flota de camiones.

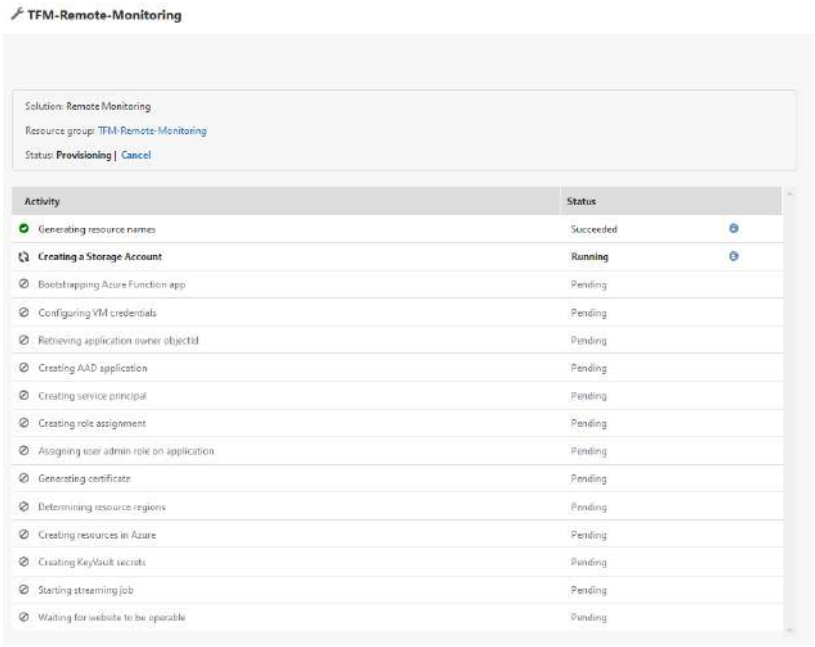


Figura 53 – Despliegue de la solución de monitorización remota

La ventana de acceso a la solución nos muestra la siguiente información:

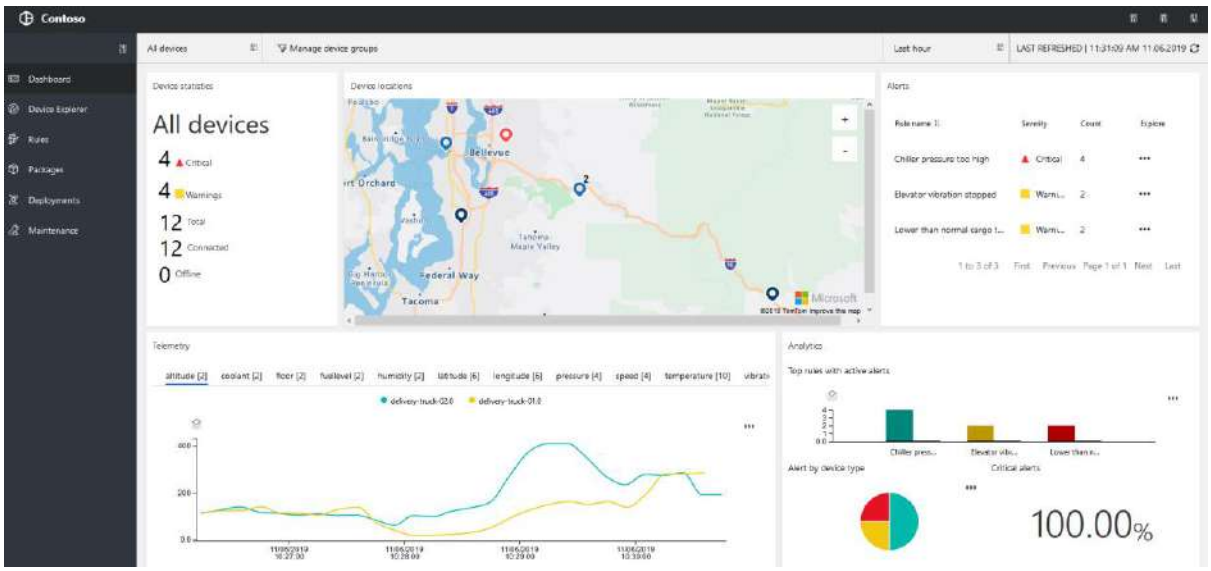


Figura 54 – Pantalla principal de la gestión remota

Como se aprecia, la información que podemos recopilar de uno de los sensores instalado en uno de los camiones incluye: Situación GPS (en el mapa), velocidad, latitud, longitud, temperatura, nivel de combustible, etc.

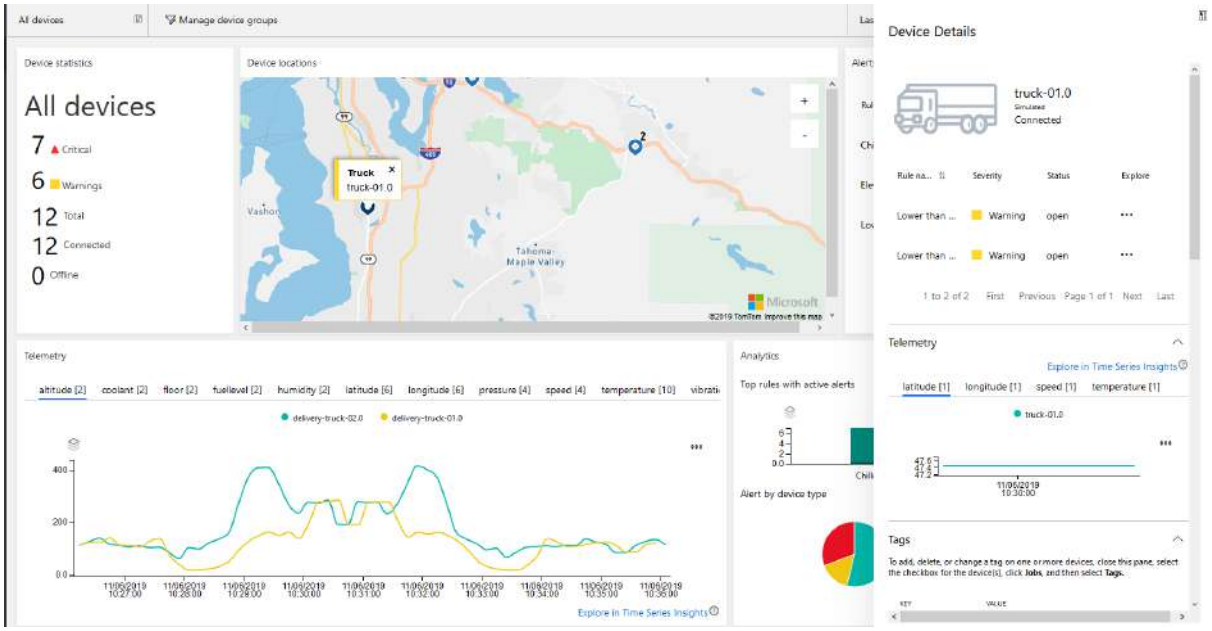


Figura 55 – Detalles de la información de uno de los camiones

Podemos definir reglas en función del umbral que definamos a partir del cual se nos generara la alerta correspondiente, mostrándonos también su historial de eventos.

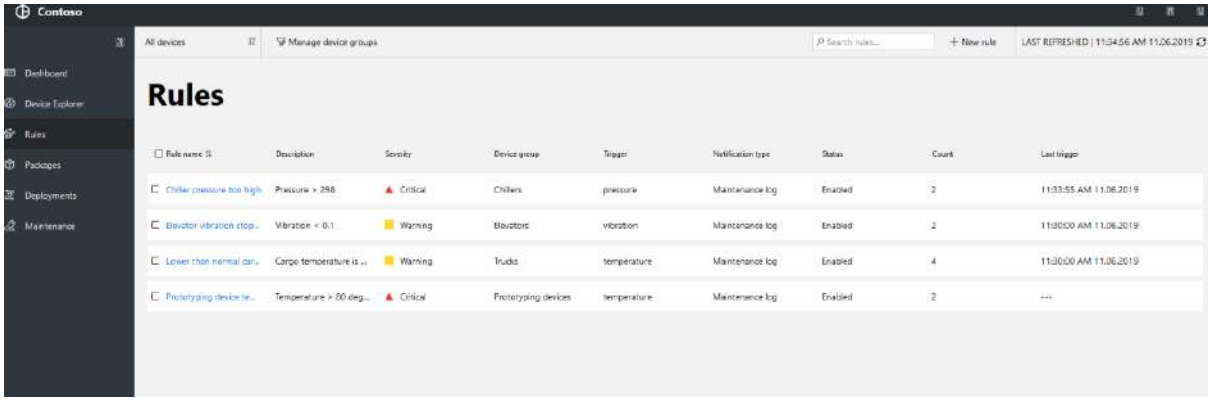


Figura 56 – Definición de reglas de aviso

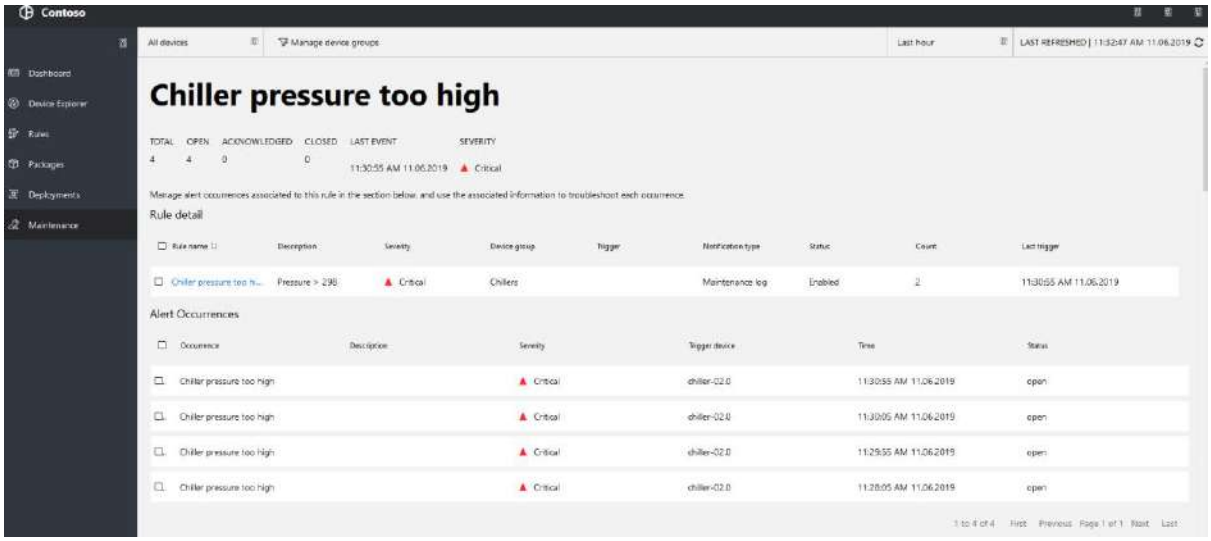


Figura 57 – Reglas e historial de alertas

7.3. Mantenimiento Predictivo

La última propuesta está basada en una solución de mantenimiento predictivo en el mundo de la aviación de cara a predecir los periodos de revisión de los motores de un avión.

Cuando la ejecución de la solución avanza vemos como la vida útil de los motores va disminuyendo en función del avance del tiempo.

Figura 58 – Página principal de la solución de mantenimiento predictivo

Cuando se alcanza el umbral definido vemos como el motor cambia de color en la infografía avisándonos de que se acerca a su límite de uso.

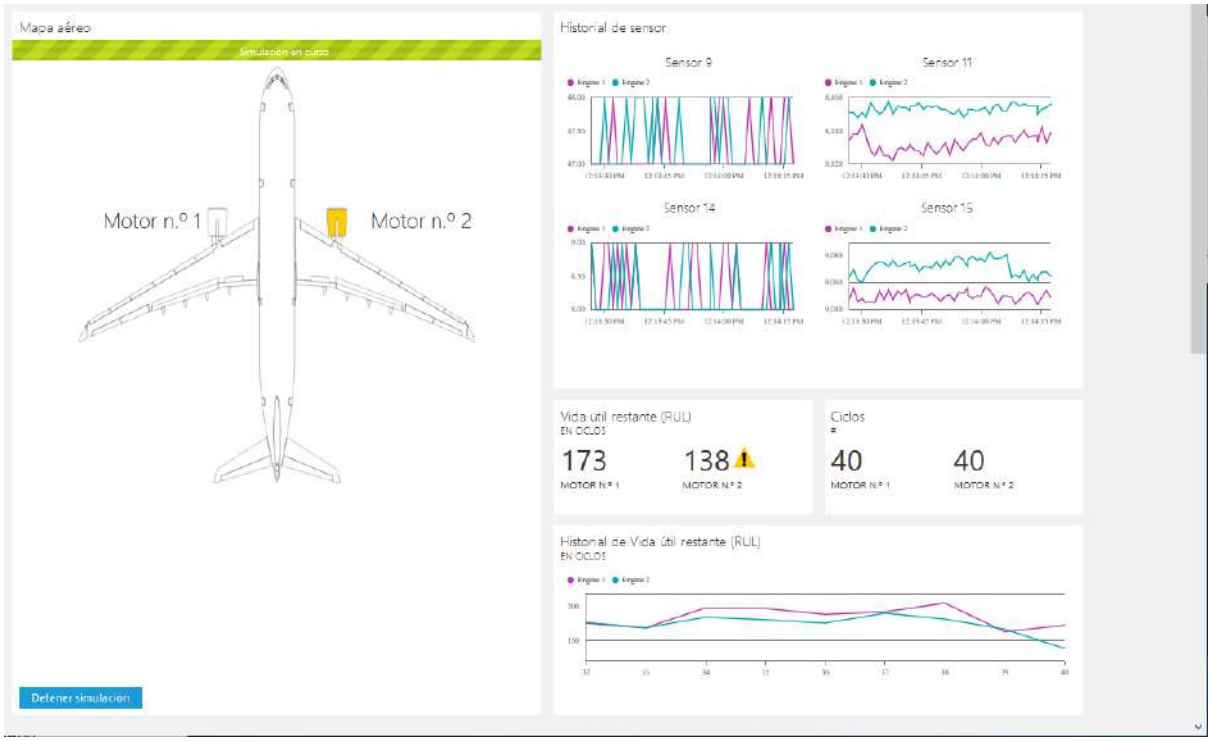


Figura 59 – Aviso de umbral de mantenimiento 1

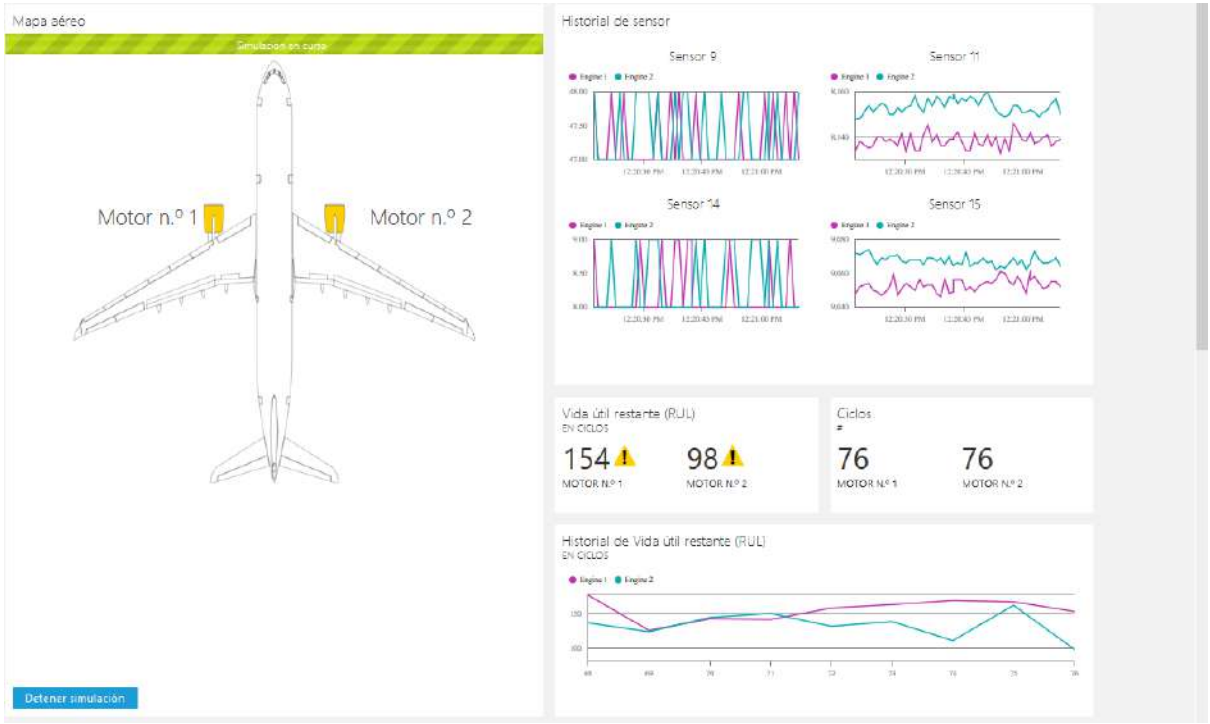


Figura 60 – Aviso de umbral de mantenimiento 2

A través de estas tres soluciones hemos querido mostrar varios entornos donde la aplicación de las soluciones IT / OT junto con los servicios de cloud, nos permite tener un control elevado de nuestros dispositivos industriales, lo cual repercute en un mayor grado de control de plataforma, obteniendo beneficios en aspectos económicos, logísticos, de gestión, etc., lo que es una garantía de que la empresa se adapta a los nuevos tiempos que ya están entre nosotros.

8. Nuevos enfoques de la seguridad. SDP. ZeroTrust. Azure Sphere

El modelo tradicional de seguridad se basaba en que las empresas invertían grandes cantidades de dinero y recursos en securizar su perímetro de seguridad, el cual estaba claramente delimitado por la ubicación de sus recursos (servidores, aplicaciones) alrededor de sus datacenters.

En la actualidad, este perímetro es mucho más difuso debido a que las aplicaciones y servicios de las empresas se encuentran ubicados en distintos sitios, no solo en los sitios físicos tradicionales, sino en ubicaciones cloud, por ejemplo.

También el punto desde el cual estos recursos son consumidos ha cambiado. Cada vez es más habitual el que los empleados no se encuentren únicamente en las oficinas centrales, sino que hay un número creciente de personas que trabajan en movilidad o desde sus casas y, además, utilizando dispositivos diversos, como móviles y tabletas.

El mundo de IoT no es un elemento extraño a esta nueva filosofía, sino que es un actor principal dada la importancia que este mundo está adquiriendo en el entorno del cliente final y, sobre todo, en el mundo empresarial. La diversidad de elementos de este entorno hace que la seguridad sea una premisa clave a solventar, y estos nuevos enfoques ayudan afrontar estos retos de una manera más flexible y efectiva.

Como resultado de este entorno cambiante, las empresas están comenzando a abandonar el tradicional, y nuevos conceptos como SDP (Software Defined Perimeter) y ZeroTrust Networks están empezando a ser claves en la nueva organización de la seguridad en las empresas.

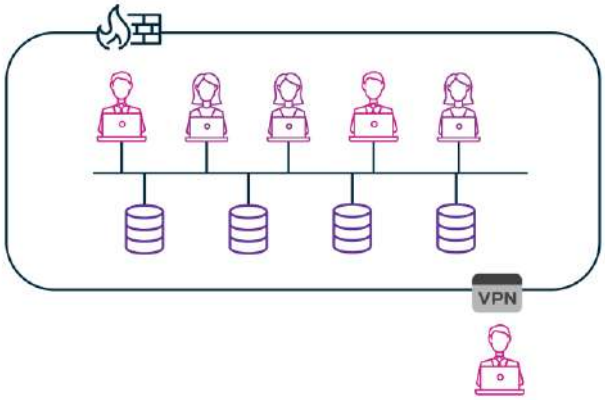


Figura 61 – Esquema Tradicional Seguridad

8.1. SDP

Como he indicado anteriormente, el enfoque tradicional de seguridad no encaja con el paradigma actual de un perfil de conexión cambiante y dinámico.

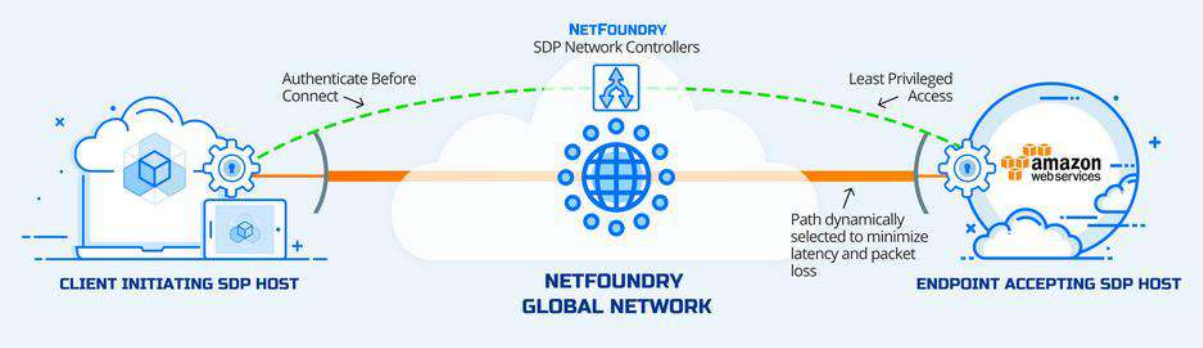


Figura 62 – Esquema de SDP

El concepto de SDP está basado en la creación de un marco de seguridad para el establecimiento de redes de acceso micro-segmentadas. SDP crea de manera dinámica una red entre el usuario y los recursos a los cuales ésta ha de acceder.

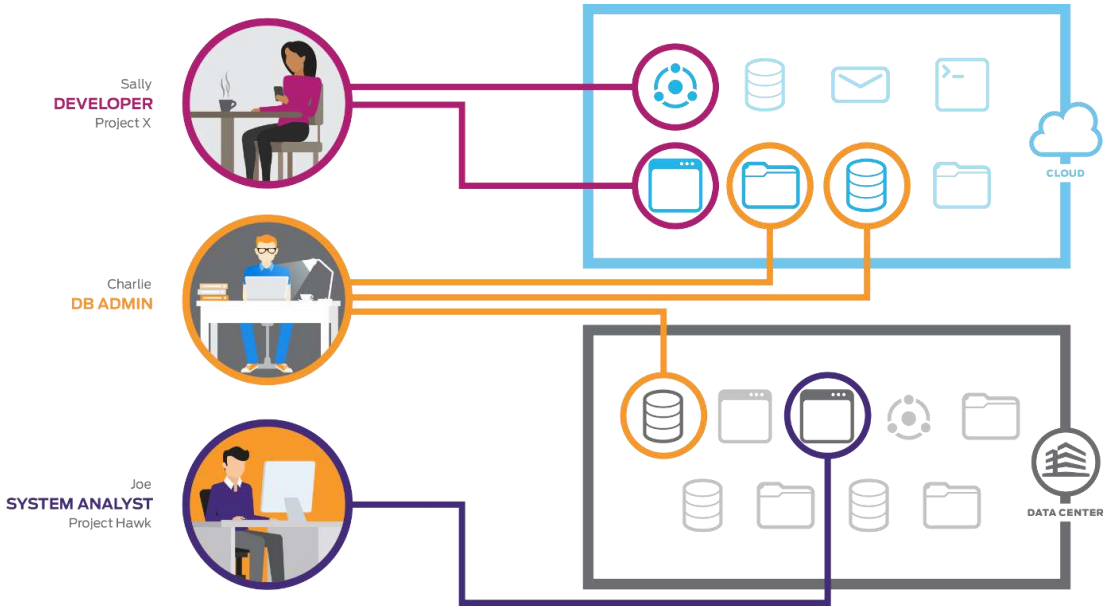


Figura 63 – SDP – Accesos de usuarios en la empresa actual

Este nuevo entorno se basa en tres pilares fundamentales:

- Centrado en la identidad el usuario: está diseñado en alrededor de la identidad del usuario en lugar de la dirección IP de este.
- Zero Trust: basado en la regla de “nunca confiar, siempre verificar”
- Creado para la nube: diseñado para funcionar en redes de nube proporcionando una seguridad escalable.

Estos tres pilares garantizan que cualquier dispositivo que intenta acceder a cualquier recurso de nuestra infraestructura es autenticado y autorizado antes de que pueda acceder a los mismos. Todos los recursos de red no autorizados son inaccesibles, aplicando el principio del *menor privilegio de acceso a la red*, lo cual también reduce la superficie de ataque al ocultar estos recursos de usuarios no autorizados o autenticados.

En una arquitectura SDP típica, existen varios puntos en donde todas y cada una de las conexiones se validan e inspeccionan de cara a ayudar a demostrar la autenticidad. Normalmente, en el modelo SDP hay un controlador que define las políticas mediante las cuales los clientes pueden conectarse y obtener acceso a diferentes recursos. El gateway SDP ayuda a dirigir el tráfico al centro de datos

correcto o a los recursos de la nube. Finalmente, los dispositivos y servicios hacen uso de un cliente SDP que se conecta y solicita acceso desde el controlador a los recursos.

8.2. ZeroTrust

Una de las tendencias que más auge está tomando en la actualidad en lo relativo a la seguridad es el relativo a las arquitecturas de Zeo Trust. La popularidad de este término ha ido creciendo a lo largo de los años. Básicamente asume el concepto de “culpable antes que inocente” en todo. Cada elemento que necesita acceder a cualquier servicio o aplicación es interrogado para determinar su validez.

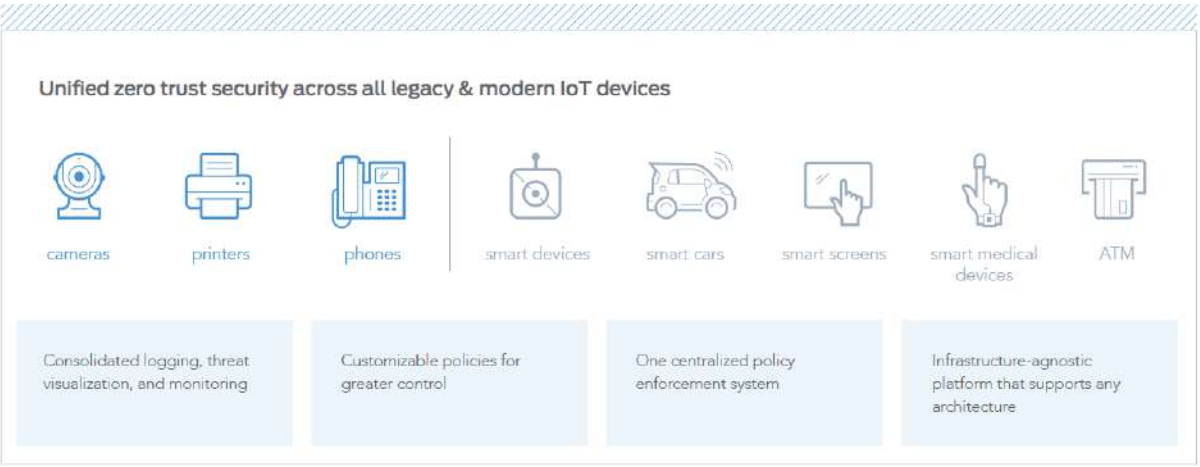


Figura 64 – Zero Trust

Como sabemos el mundo de IoT ya entre nosotros, depositando en él importantes responsabilidades. Este nuevo ecosistema puede desarrollarse en un entorno de Zero Trust y somos capaces de cumplir con las siguientes premisas:

- Un conocimiento exhaustivo de cada dispositivo, de todas sus capacidades y de todos sus medios de comunicación.
- Disponer de una vía segura de actualización de los dispositivos.
- Una continua monitorización de la configuración y de las relaciones de las que dispone el dispositivo.
- Disponer de una monitorización automática entre zonas de confianza.

Vamos a ver en el siguiente punto una visión a alto nivel de cómo podemos implementar mecanismos de esta arquitectura utilizando tecnologías MSFT, como una de las empresas tecnológicas punteras que encontramos en el mercado.

8.3. Microsoft y Zero Trust

MSFT lleva tiempo trabajando en estas tecnologías. En la siguiente figura podemos ver el roadmap con las fases que esta arquitectura tiene para ellos:

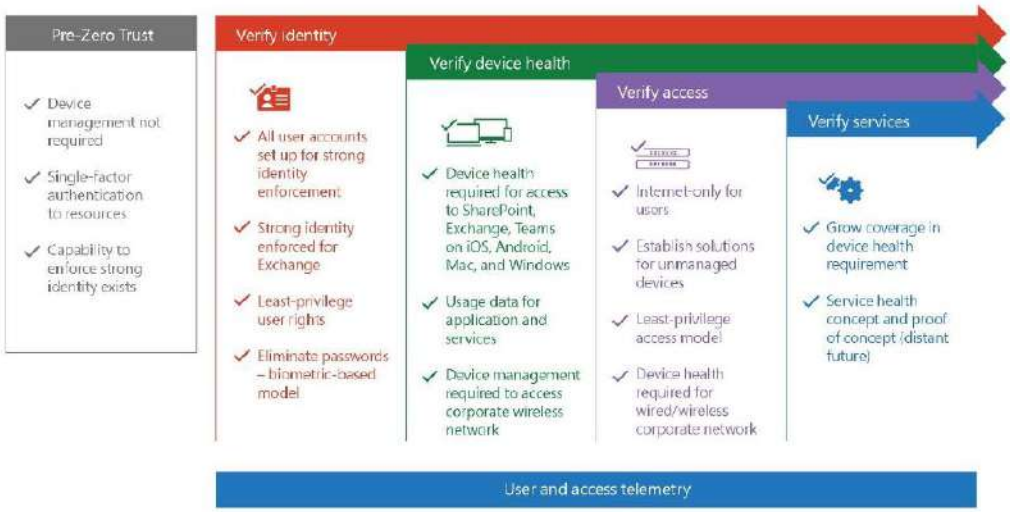


Figura 65 – Principales componentes de cada fase de Zero Trust

A nivel de estructura de arquitectura, MSFT nos proporciona el siguiente esquema como referencia de como implementar Zero Trust.

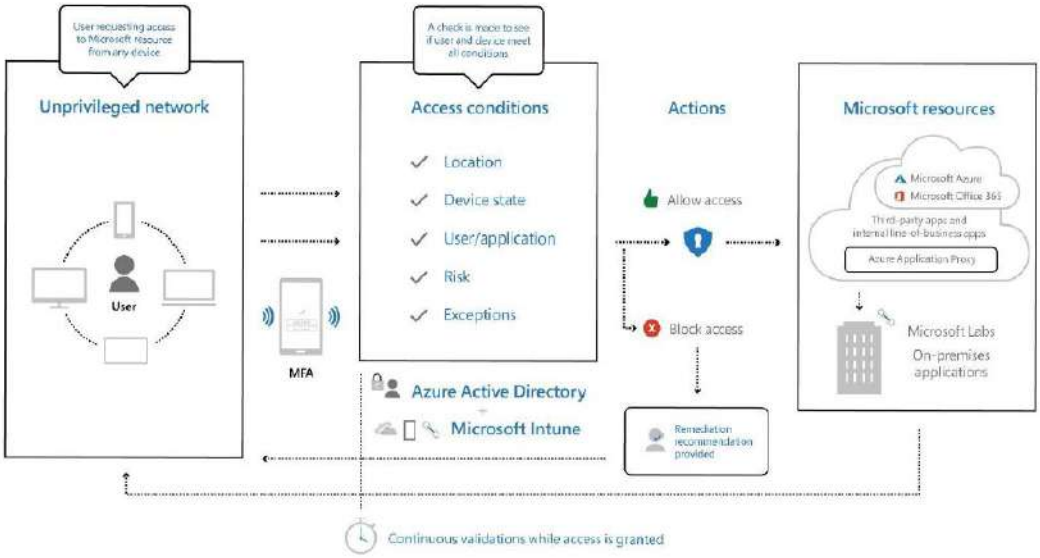


Figura 66 – Arquitectura de Zero Trust

Como vemos en la imagen anterior, el acceso condicional en Azure Active Directory se encuentra en el centro de esta estrategia. La gestión y la verificación de las entidades que se conectan a nuestro entorno de producción es el primer paso que debemos afrontar.

El uso del acceso condicional que nos proporciona Azure AD nos permite la definición de unas políticas de acceso que nos permiten crear condiciones y controles que han de cumplirse antes de concederse el acceso.

Este acceso condicional permite la aplicación de manera obligatoria de políticas de seguridad que son automáticamente disparadas cuando se dan ciertas condiciones, pudiendo bloquear el acceso si se detecta que el entorno pueda ser comprometido.

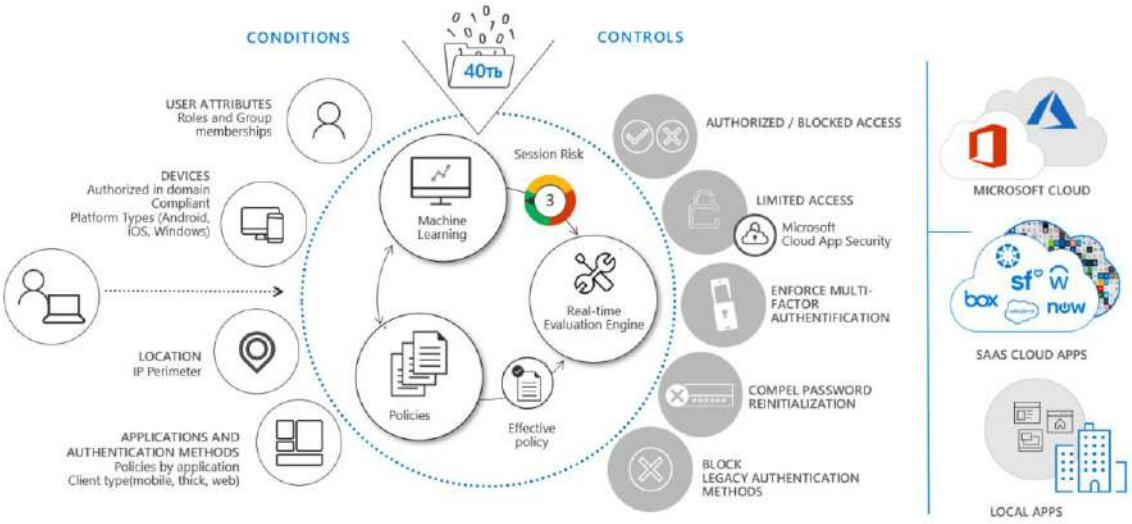


Figura 67 – Acceso condicional En Azure Active Directory

8.4. Microsoft Azure Sphere

Microsoft ha desarrollado una plataforma segura y de alto nivel que incluye las características de conectividad y seguridad requeridas para los dispositivos IoT conectados a Internet. Comprende una MCU que contiene un sistema operativo Linux y una plataforma cloud que nos proporciona una seguridad continua.

La MCU Azure Sphere integra las capacidades de procesamiento en tiempo real con la capacidad de ejecutar un sistema operativo de alto nivel. Una MCU de Azure Sphere, junto con su sistema operativo y plataforma de aplicaciones, permite la creación de dispositivos seguros conectados a Internet que se pueden actualizar, controlar, monitorear y mantener de forma remota.

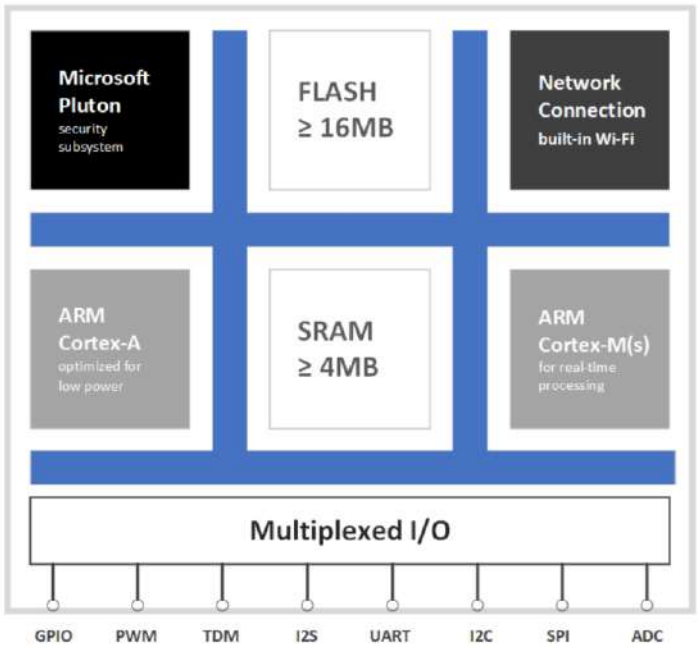


Figura 68 – Componentes de una MCU

Un dispositivo conectado que incluye una MCU Azure Sphere, ya sea junto o en sustitución de una MCU existente, proporciona mayor seguridad, productividad y oportunidad. Por ejemplo:

- Un entorno de aplicación seguro con conexiones autenticadas minimiza los riesgos de seguridad debido a la suplantación de identidad, software fraudulento o ataques de denegación de servicio, entre otros.
- Las actualizaciones de software se pueden implementar automáticamente vía OTA en cualquier dispositivo conectado para solucionar problemas, proporcionar nuevas funciones o contrarrestar los métodos de ataque emergentes, mejorando así la productividad del personal de soporte.
- Los datos de uso del producto se pueden informar a la nube a través de una conexión segura para ayudar a diagnosticar problemas y diseñar nuevos productos, lo que aumenta la oportunidad de servicio del producto, interacciones positivas con el cliente y desarrollo futuro.

El servicio de seguridad de Azure Sphere es un aspecto integral de Azure Sphere. Con este servicio, las MCU de Azure Sphere se conectan de manera segura a la nube y a la web. El servicio garantiza que el dispositivo arranque solo con una versión autorizada de software.

Además, proporciona un canal seguro a través del cual Microsoft puede descargar e instalar automáticamente actualizaciones del sistema operativo en los dispositivos implementados en el campo para mitigar los problemas de seguridad. No se requiere intervención del fabricante ni del usuario final, lo que cierra un agujero de seguridad bastante común.

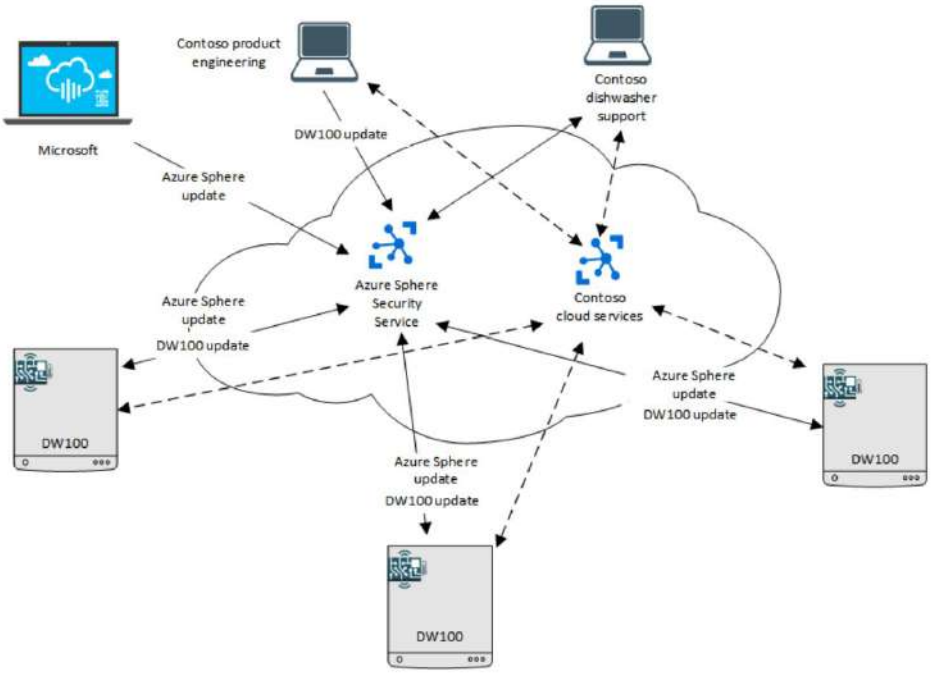


Figura 69 – Ejemplo de entorno de Azure Sphere

El Servicio de seguridad de Azure Sphere consta de tres componentes principales: autenticación basada en certificados, actualización e informes de errores.

- Autenticación basada en certificados: El componente de autenticación proporciona certificación remota y autenticación basada en certificados. El servicio de certificación remota se conecta a través de un protocolo de desafío-respuesta que garantiza, no solo que el dispositivo arranca con el software correcto, sino con la versión correcta de ese software.

  Una vez que la certificación tiene éxito, el servicio de autenticación se comunica a través de una conexión TLS segura y emite un certificado que el dispositivo puede presentar a un servicio web, como Microsoft Azure o la nube privada de una empresa. El servicio web valida la cadena de certificados, verificando así que el dispositivo es genuino, que su software está actualizado y que Microsoft es su fuente. El dispositivo puede conectarse de manera segura con el servicio en línea.

- Actualización: El servicio de actualización distribuye actualizaciones automáticas para el sistema operativo Azure Sphere y para las aplicaciones. El servicio de actualización asegura la operación continua y permite el servicio remoto y la actualización del software de la aplicación.

- Informe de errores: El servicio de informe de errores proporciona informes simples de errores para el software implementado. Para obtener datos más completos, use las funciones de informes y análisis que se incluyen con una suscripción de Microsoft Azure.

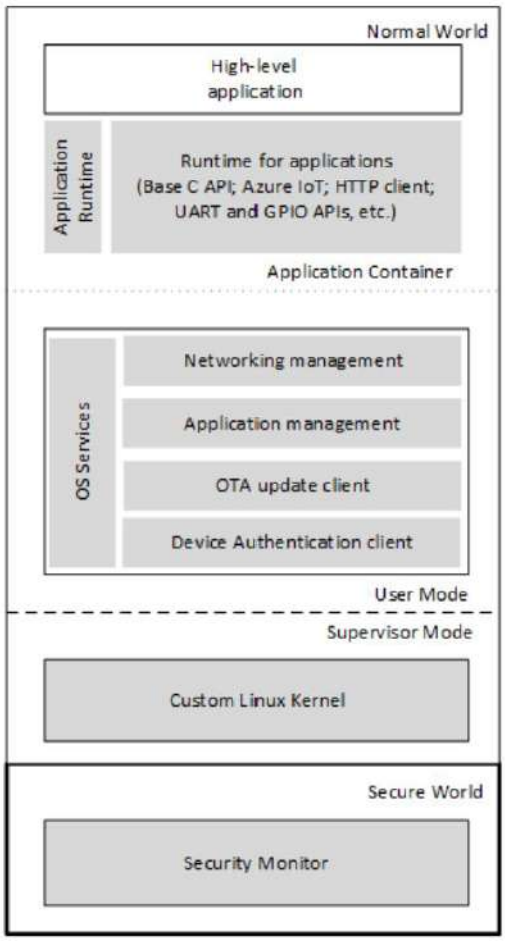


Figura 70 – Arquitectura Software de Azure Sphere

La plataforma Azure Sphere está diseñada en torno a estas siete propiedades:

- Raíz de confianza basada en hardware: Una raíz de confianza basada en hardware garantiza que el dispositivo y su identidad no se puedan separar, evitando así la falsificación de dispositivos. Cada MCU de Azure Sphere se identifica mediante una clave criptográfica inolvidable que se genera y se protege mediante el hardware del subsistema de seguridad diseñado por Microsoft. Esto garantiza una raíz de confianza de hardware segura y resistente a la manipulación desde la fábrica hasta el usuario final.

- Zona de Seguridad: La mayor parte del software del dispositivo permanece fuera de la zona confiable de la MCU, reduciendo así la superficie de los ataques.

- Defensa en profundidad: La defensa en profundidad proporciona múltiples capas de seguridad y, por lo tanto, múltiples mitigaciones contra cada amenaza. Cada capa de software en la plataforma Azure Sphere verifica que la capa de arriba esté asegurada.

- Compartimentación: La compartimentación limita el alcance de cualquier error individual. Las MCU de Azure Sphere contienen contramedidas de silicio, incluidos firewalls de hardware, para evitar que una violación de seguridad en un componente se propague a otros componentes. Un entorno de tiempo de ejecución limitado y de "espacio aislado" evita que las aplicaciones corrompan el código o los datos seguros.

- Autenticación basada en certificados: El uso de certificados firmados, validados por una clave criptográfica inolvidable, proporciona una autenticación mucho más fuerte que las contraseñas. La plataforma Azure Sphere requiere que cada elemento de software esté firmado. Las comunicaciones de dispositivo a nube y de nube a dispositivo requieren autenticación basada en certificados.

- Seguridad renovable: El software del dispositivo se actualiza automáticamente para corregir vulnerabilidades conocidas o violaciones de seguridad, que no requieren intervención del fabricante del producto o del usuario final. El servicio de seguridad de Azure Sphere actualiza el sistema operativo Azure Sphere y sus aplicaciones automáticamente.

- Informe de errores: Los errores en el software o hardware del dispositivo son típicas en los ataques de seguridad actuales; el error del dispositivo en sí mismo constituye un ataque de denegación de servicio. La comunicación de dispositivo a la nube proporciona una alerta temprana de posibles errores. Los dispositivos Azure Sphere pueden informar automáticamente los datos operativos y los errores a un sistema de análisis basado en la nube, pudiendo realizar las tareas de actualización y mantenimiento de forma remota.

Estos enfoques, entre otros, no han llegado para hacer borrón y cuenta nueva sobre los sistemas ya existentes, sino que vienen a complementarlos, aportando una visión más actual de la seguridad no solo en IoT, sino en todos los entornos que ha día de hoy se encuentran en el mundo empresarial.

Las empresas, a medida que evolucionan sus sistemas han de evolucionar también la forma en que éstos han de protegerse y dada la velocidad a la que el mundo de las tecnologías evoluciona, modelos de seguridad altamente flexibles, fiables y fáciles de adoptar, aparecen como elementos clave para obtener el objetivo perseguido, que no es otro que darlos del mayor nivel de seguridad posible.

9. Conclusiones

Desde sus orígenes como red destinada a comunicar centros de defensa hasta nuestros días, el auge de Internet ha sido imparable. Es casi impensable imaginar un mundo sin este servicio, tanto a nivel de un usuario doméstico como en el ámbito empresarial.

Durante este proceso de crecimiento las funcionalidades que nos ha ido proporcionado han ido en aumento casi a la misma velocidad que su uso. Sitios web, correo electrónico, mensajería instantánea, video llamadas, redes sociales, compras on-line y un largo etc. forman parte de este gran abanico de servicios.

No obstante, no todos los aspectos que estos servicios necesitan para su funcionamiento han sido tenidos en cuenta con el mismo peso, siendo la seguridad uno de ellos. No ha sido hasta una época reciente en la que nos hemos empezado a preocupar de una manera más amplia de la seguridad en Internet.

Estas medidas de seguridad han puesto el foco en proteger el perímetro tradicional en el que las empresas alojaban los servicios que nos proporcionaban, dedicando grandes inversiones en firewall, IDS, antivirus, etc. Pero con la llegada de servicios como el cloud y también los dispositivos IoT, esta frontera se ha convertido en algo más difuso y difícil de securizar.

Es cierto que el grado de protección que las empresas habían alcanzado en sus datacenter había alcanzado niveles muy elevados, pero ante los desafíos de las nuevas formas de consumir servicios, las empresas tienen aún un gran camino que recorrer.

Hemos visto que, en lo relativo al mundo de IoT y dadas las peculiaridades de los elementos que lo componen, es necesario el despliegue de otras medidas para proteger y gestionar a estos nuevos elementos que forman parte activa y muy importante de nuestros entornos empresariales. La diversidad de estos en diferentes aspectos como el fabricante, recursos, uso, etc. hacen que sus brechas de seguridad sean numerosas y que sean susceptibles de ser atacados por hackers, que pueden acceder a informaciones importantes y peligrosas si cayeran en manos equivocadas (imaginar que un hacker pudiera hacerse con el control de los sensores de AA de un datacenter y causar el apagado de miles de servidores o el control de los semáforos de una cuidad).

Estas nuevas medidas de protección han de ser muy flexibles y fáciles de aplicar para un usuario final y tienen que aportar un alto grado de éxito. Soluciones como SDP, ZeroTrust van encaminadas a ofrecernos soluciones que protejan a esta nueva varia de elementos de una manera eficaz y fácil de gestionar, pero hoy en día, tenemos un largo camino por recorrer.

Los últimos ataques sufridos por las empresas, como el WannaCry, ha puesto de manifiesto la importancia de la seguridad en los entornos de IT y ha empezado a concienciar a las empresas para que dediquen más recursos técnicos y económicos en aras de su mejora. Hay un largo camino por recorrer en este tema y aunque un sistema seguro al 100% es un reto utópico, es necesaria la concienciación de todos, consumidores finales, usuarios, personal de IT, empresarios, para poder seguir disfrutando de los beneficios de un mundo conectado en un entorno seguro.

A nivel personal, la elaboración de este TFM me ha permitido conocer más en detalle este entorno y sus aplicaciones, sobre todo en el ámbito industrial lo que me ha ayudado a comprender los entornos de IIoT que en mi actual trabajo se encuentran desplegados, lo que me ayudara a poder crecer profesionalmente en esta área, de gran peso en mi entorno profesional.

10. Bibliografía y fuentes consultadas

10.1. Libros consultados

- Michael Washam , Jonathan Tuliani, et ál. «Exam Ref AZ-103 Microsoft Azure Administrator». Microsoft Press. ISBN: 978-0-13-546658-2. June 2019.

- Mike Pfeiffer, Derek Schauland, Nicole Stevens, Timothy L. Warner. «Exam Ref AZ-300 Microsoft Azure Architect Technologies». Microsoft Press. ISBN: 978-0-13-580254-0. November 2019.

- Giacomo Veneri & Antonio Capasso. «Hands-On Industrial Internet of Things». Packt. ISBN: 978-1-78953-722-2.

10.2. Páginas web consultadas

- [1] Microsoft Docs; IoT Security Architecture; <https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture?context=azure/iot-hub/rc/rc>
- [2] Azure Microsoft; IoT Suite; <https://azure.microsoft.com/es-es/blog/microsoft-azure-iot-suite-connecting-your-things-to-the-cloud/>
- [3] Postscapes; IoT Protocols; <https://www.postscapes.com/internet-of-things-protocols/>
- [4] RealTimeLogic; IoT Protocols; <https://realtimelogic.com/articles/Secure-IoT-Protocols/>
- [5] Ionos; Fog Computing; <https://www.ionos.es/digitalguide/servidores/know-how/fog-computing/>
- [6] Techtarget; Fog Computing; <https://internetofthingsagenda.techtarget.com/definition/fog-computing-fogging/>
- [7] Deloitte; IoT Things; <https://www2.deloitte.com/es/es/pages/technology/articles/IoT-internet-of-things.html>
- [8] Bcendon; Redes IoT; <http://www.bcendon.com/las-redes-mas-usadas-en-el-iot/>
- [9] Tomasmarte; Tecnologias IoT; <https://www.tomasmarte.com/2018/08/22/10-tecnologias-de-comunicacion-en-iot-que-debes-conocer/>
- [10] Incibe; IoT Ataques y Recomendaciones; <https://www.incibe-cert.es/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones>
  [11] Azure Microsoft; IoT; <https://azure.microsoft.com/en-us/overview/iot/>
- [12] Online Books Review; Best IoT Books; <https://www.onlinebooksreview.com/articles/best-iot-books>
- [13] Microsoft Docs; IoT Architecture; <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/iot/>
- [14] Cmswire; Edge and Fog Computing; <https://www.cmswire.com/information-management/edge-computing-vs-fog-computing-whats-the-difference/>
- [15] Gradiant; Edge and Fog Computing; <https://www.gradiant.org/blog/edge-fog-computing-cloud/>

[16] WinSystems; Fog and Edge Computing - Differences; <https://www.winsystems.com/cloud-fog-and-edge-computing-whats-the-difference/>
- [17] Xakata; Edge Computing; <https://www.xataka.com/internet-of-things/edge-computing-que-es-y-por-que-hay-gente-que-piensa-que-es-el-futuro/>
- [18] Microsoft Docs; Azure Sphere; <https://docs.microsoft.com/en-us/azure-sphere/>
- [19] Microsoft Docs; Azure Sphere MT3620; <https://docs.microsoft.com/en-us/azure-sphere/hardware/mt3620-user-guide>
- [20] GitHub; IoT Solutions; <https://github.com/microsoftarchive/iot-journey/blob/master/docs/02-architecting-IoT-solutions.md>
- [21] Mendix; Anatomy IoT Solution <https://www.mendix.com/blog/anatomy-iot-solution/>
- [22] Techbeacon; IoT Architecture Stages <https://techbeacon.com/enterprise-it/4-stages-iot-architecture>
- [23] Microsoft Docs; IoT Industrial <https://docs.microsoft.com/es-es/azure/iot-accelerators/overview-iot-industrial>
- [24] Microsoft Docs; IoT Accelerators <https://docs.microsoft.com/es-es/azure/iot-accelerators/iot-accelerators-faq-cf>
- [25] Azureiotsolutions; Accelerators <https://www.azureiotsolutions.com/Accelerators>
- [26] Inductiveautomation; Ignition https://inductiveautomation.com/ignition/