UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Departamento de Comunicaciones

Universitat Politècnica de València

Especificación y desarrollo de una pasarela física y virtual para interoperabilidad de dispositivos heterogéneos en el ámbito de Internet de las Cosas

Tesis Doctoral

Programa de Doctorado en Telecomunicación

Autor:
Eneko Olivares Gorriti

Director:
Carlos Enrique Palau Salvador

Octubre de 2021

A mis padres, a mis hermanas y a todas las personas que han estado conmigo durante esta etapa.

Agradecimientos

Al director de esta tesis doctoral, Carlos Palau, por la confianza que ha tenido siempre conmigo y por la oportunidad que me ha dado durante varios años de trabajar con él.

A mis compañeros del laboratorio, que me han regalado momentos inolvidables y me han ayudado siempre que lo he necesitado.

A mi familia, por su apoyo y haber cuidado de mí todo este tiempo.

Y a Jara, por toda la ayuda y paciencia que ha tenido siempre conmigo.

Muchas gracias a todos.

Resumen

En los últimos años, Internet de las Cosas ("Internet of Things" o "IoT") ha evolucionado de ser simplemente un concepto académico, construido alrededor de protocolos de comunicación y dispositivos, a ser un ecosistema con aplicaciones industriales y de negocio con implicaciones tecnológicas y sociales sin precedentes.

Gracias a las nuevas redes de acceso inalámbricas emergentes, sensores mejorados y sistemas embebidos con procesadores cada vez más eficientes y baratos, una gran cantidad de objetos (tanto de nuestra vida cotidiana como de sistemas y procesos industriales) están interconectados entre sí, trasladando la información del mundo físico a las aplicaciones y servicios de Internet.

A través de las pasarelas IoT los dispositivos que interactúan con el mundo físico son capaces de conectarse a las redes de comunicación e intercambiar información. Son varios los retos que deben afrontar las pasarelas en su papel dentro del Internet de las Cosas, entre ellas, la escalabilidad, seguridad, la gestión de dispositivos y, recientemente, la interoperabilidad.

La falta de interoperabilidad entre los dispositivos provoca importantes problemas tecnológicos y empresariales, tales como la imposibilidad de conectar dispositivos IoT no interoperables a plataformas IoT heterogéneas, la imposibilidad de desarrollar aplicaciones IoT que exploten múltiples plataformas en dominios homogéneos y/o cruzados, la lentitud en la introducción de la tecnología IoT a gran escala, el desánimo en la adopción de la tecnología IoT, el aumento de los costes, la escasa reutilización de las soluciones técnicas y la insatisfacción de los usuarios.

El propósito de esta tesis doctoral es la búsqueda de una solución óptima para la interoperabilidad entre dispositivos de Internet de las Cosas

mediante la definición de una pasarela IoT genérica, modular y extensible; sin dejar de lado aspectos esenciales como la seguridad, escalabilidad y la calidad de servicio.

Se completa esta tesis doctoral con una implementación software de la pasarela IoT siguiendo la definición propuesta, así como el despliegue y la evaluación de los resultados obtenidos en numerosos casos de uso pertenecientes a pilotos del proyecto de investigación Europeo “INTER-IoT” financiado a través del programa marco Horizonte 2020.

Resum

En els últims anys, Internet de les Coses ("Internet of Things" o "IoT") ha evolucionat de ser simplement un concepte acadèmic, construït al voltant de protocols de comunicació i dispositius, a ser un ecosistema amb aplicacions industrials i de negoci amb implicacions tecnològiques i socials sense precedents.

Gràcies a les noves xarxes d'accés "wireless" emergents, sensors millorats i sistemes embeguts amb processadors cada vegada més eficients i barats, una gran quantitat d'objectes (tant de la nostra vida quotidiana com de sistemes i processos industrials) estan interconnectats entre si, traslladant la informació del món físic a les aplicacions i serveis d'Internet.

A través de les passarel·les IoT els dispositius que interactuen amb el món físic són capaços de connectar-se a les xarxes de comunicació i intercanviar informació. Són diversos els reptes que han d'afrontar les passarel·les en el seu paper dins de la Internet de les Coses, entre elles, l'escalabilitat, seguretat, la gestió de dispositius i, recentment, la interoperabilitat.

La falta d'interoperabilitat entre els dispositius provoca importants problemes tecnològics i empresarials, com ara la impossibilitat de connectar dispositius IoT no interoperables a plataformes IoT heterogènies, la impossibilitat de desenvolupar aplicacions IoT que exploten múltiples plataformes en dominis homogenis i/o croats, la lentitud en la introducció de la tecnologia IoT a gran escala, el descoratjament en l'adopció de la tecnologia IoT, l'augment dels costos, l'escassa reutilització de les solucions tècniques i la insatisfacció dels usuaris.

El propòsit d'aquesta tesi doctoral és la cerca d'una solució òptima per a la interoperabilitat entre dispositius d'Internet de les Coses mitjançant la definició d'una passarel·la IoT genèrica, modular i extensible; sense

deixar de costat aspectes essencials com la seguretat, escalabilitat i la qualitat de servei.

Es completa aquesta tesi doctoral amb una implementació programari de la passarel·la IoT seguint la definició proposada, així com el desplegament i l'avaluació dels resultats obtinguts en nombrosos casos d'ús pertanyents a pilots del projecte d'investigació Europeu "INTER-IoT" finançat a través del programa marc Horitzó 2020.

Abstract

In recent years, the Internet of Things ("IoT") has evolved from being simply an academic concept, built around communication protocols and devices, to an ecosystem with industrial and business applications with unprecedented technological and social implications.

Thanks to new emerging wireless access networks, improved sensors and embedded systems with increasingly efficient and inexpensive processors, a large number of objects (both in our daily lives and in industrial systems and processes) are interconnected with each other, moving information from the physical world to Internet applications and services.

Through IoT gateways, devices that interact with the physical world are able to connect to communication networks and exchange information. There are several challenges that gateways must face in their role within the Internet of Things, including scalability, security, device management and, recently, interoperability.

The lack of interoperability between devices causes major technological and business problems, such as the impossibility of connecting non-interoperable IoT devices to heterogeneous IoT platforms, the impossibility of developing IoT applications that exploit multiple platforms in homogeneous and/or cross-domains, the slow introduction of IoT technology on a large scale, discouragement in the adoption of IoT technology, increased costs, low utilization of technical solutions and user dissatisfaction.

The purpose of this doctoral thesis is the search for an optimal solution for interoperability between Internet of Things devices by defining a generic, modular and extensible IoT gateway; without neglecting essential aspects such as security, scalability and quality of service. This doctoral Thesis is completed with a software implementation of the IoT

gateway following the proposed definition, as well as the deployment and evaluation of the results obtained in numerous use cases belonging to the pilots of the European research project “INTER-IoT” funded through the Horizon 2020 framework program.

Tabla de contenidos

Lista de figuras

Lista de tablas

Glosario

3rd Generation Partnership Project

Es una asociación de diferentes organismos de estandarización de telecomunicaciones (ARIB, ATIAS, CCSA, ETSI, TSDSI, TTA, TTC) proporcionando un entorno estable para producir las especificiaciones que definen las tecnologías del 3GPP.

5G New Radio

Es una nueva tecnología de acceso radioeléctrico (RAT) desarrollada por el 3GPP para la red móvil 5G, diseñada para ser el estándar global de la interfaz de las redes 5G.

5G Non Standalone

Uno de los modos de red de 5G. A diferencia de 5G SA, esta utiliza la infrastructura de red existente de 4G para ofrecer mayor velocidad y ancho de banda.

5GENESIS

Proyecto perteneciente al programa europeo de investigación Horizonte 2020. El objetivo principal es la validación los KPI de 5G para varios casos de uso, tanto en montajes controlados como en eventos a gran escala [1].

5th Generation Technology Standard for Broadmand Cellular Networks

Es el estándar de quinta generación para redes celulares de banda ancha. Las redes 5G son redes celulares digitales en las que el área de servicio se divide en pequeñas células geográficas.

[1] https://5genesis.eu/

Advanced Message Queuing Protocol

Es una estándar abierto para aplicaciones *middleware* orientadas a mensajes. Describe un protocolo de comunicación binario a nivel de aplicación que soporta múltiples patrones de comunicación y caracterísitcas como enrutamiento, colas, orientación de los mensajes, fiabilidad y seguridad.

Alliance for Internet of Things Innovation

Contribuye a la creación de un ecosistema europeo de IoT dinámico y acelerar su adopción. Entre sus miembros se encuentran los principales actores europeos en IoT empresas, centros de investigación, universidades, asociaciones y representantes de los usuarios finales.

Application Programming Interface

Es un tipo de interfaz de software que ofrece un servicio a otras piezas de software. Una especificación API describe cómo construir o utilizar dicha conexión o interfaz.

Backhaul

En una red jerárquica de telecomunicaciones, es la parte de la red que comprende los enlaces intermedios entre la red troncal (*backbone*) y las pequeñas subredes del borde de la red.

Complex Event Processor

Sistema que permite procesar flujos de eventos en tiempo real, permitiendo la extracción y el análisis de los mismos.

Computer Aided Software Engineering

La ingeniería de software asistida por ordenador es el ámbito de las herramientas de software utilizadas para diseñar e implementar aplicaciones. Las herramientas CASE son similares a las herramientas de diseño asistido por ordenador (CAD).

Constrained Application Protocol

Es un protocolo especializado para dispositivos de capacidades limitadas. Está diseñado para su uso entre dispositivos conectados a través de una redes de baja potencia y con pérdidas.

Cyber-Physical Systems

Un sistema ciberfísico es un sistema informático en el que un mecanismo es controlado o supervisado por algoritmos computacionales. En los siste-

mas ciberfísicos, los componentes físicos y de software están profundamente entrelazados.

European Committee for Electrotechnical Standardisation

Es responsable de la estandarización a nivel europeo en el ámbito de la ingeniería eléctrica. Junto con ETSI y CEN forma el sistema europeo de normalización técnica.

European Committee for Standardisation

Es un organismo público de estandarización cuya misión es fomentar la economía del mercado único europeo y del continente europeo en general.

European Research Cluster on the Internet of Things

El objetivo del Clúster Europeo de Investigación sobre el Internet de las Cosas es abordar el gran potencial de las capacidades basadas en IoT en Europa y coordinar las actividades llevadas a cabo.

European Telecommunications Standards Institute

Es una organización de estandarización independiente y sin ánimo de lucro en el ámbito de la información y las comunicaciones. Apoya el desarrollo y la comprobación de normas técnicas mundiales para sistemas, aplicaciones y servicios basados en las TIC.

Extranet

Es una red privada y controlada que permite el acceso a terceros a un subconjunto de la información accesible desde la intranet de una organización.

gNodeB

Next Generation Node B es una implementación conforme al 3GPP de la estación base 5G NR. Se compone de funciones de red independientes que implementan las normas del 3GPP.

Hypertext Transfer Protocol

Protocolo de la capa de aplicación dentro del conjunto de protocolos de Internet. Es la base de comunicación Web para la distribución de contenidos (originalmente sólo *hipertexto*, actualmente cualquier tipo de *hipermedia*).

Institute of Electrical and Electronics Engineers

Es una asociación profesional de ingeniería electrónica e ingeniería eléctrica (y disciplinas asociadas). Actualmente, produce más del 30 % de las publicaciones en los campos de ingeniería eléctrica, electrónica e informática.

INTER-Framework

Conjunto de herramientas desarolladas dentro del proyecto INTER-IoT que permiten y facilitan la utilización de las diferentes soluciones desarrolladas en cada capa de INTER-Layer, entre las que se encuentra una SDK de desarrollo y una API común de acceso y gestión de las diferentes capas.

INTER-HARE

Protocolo creado bajo el proyecto con el mismo nombre. El protocolo resuelve el problema de la escalabilidad en LPWAN y mediante el uso de tecnologías IoT multibanda concurrentes, donde una LPWAN de 868 MHz actúa como Backhaul transparente para un conjunto de subredes que trabajan a 2,4 GHz.

INTER-IoT Cross-Domain Pilot

Piloto ejecutado en el contexto del proyecto INTER-IoT que combina casos de uso de los pilotos de INTER-Health, INTER-LogP y casos de uso de diferentes dominios presentados durante la convocatoria abierta del proyecto.

INTER-IoT Health Pilot

Piloto ejecutado en el contexto del proyecto INTER-IoT cuyo objetivo es la validación de la plataforma de interoperabilidad en un entorno sanitario diseñado y construido para adaptarse específicamente a las necesidades de comunicación y pacientes y profesionales de la salud.

INTER-IoT Port and Logistics Pilot

Piloto ejecutado en el contexto del proyecto INTER-IoT cuyo objetivo es la validación de la plataforma de interoperabilidad en un entorno logístico portuario, permitiendo la transmisión de información entre las diferentes plataformas de gestión tradicionales con plataformas IoT que están desplegados de manera aislada por los diferentes actores portuarios.

INTER-Layer

INTER-IoT presenta una solución de interoperabilidad orientada a capas entre diferentes sistemas y plataformas de IoT. INTER-Layer incluye varias soluciones de interoperabilidad dedicadas a capas específicas o niveles: dispositivos (D2D), redes (N2N), middleware (MW2MW), aplicaciones y servicios (AS2AS), y datos y semántica (DS2DS).

INTER-Meth

Es una metodología desarrollada dentro del proyecto INTER-IoT que tiene como objetivo apoyar el proceso de integración de plataformas heterogéneas

de IoT paraobtener interoperabilidad entre ellas y permitir la implementación y despliegue de aplicaciones IoT sobre ellas.

International Electrotechnical Commission

La Comisión Electrotécnica Internacional es una organización internacional de normalización que prepara y publica normas internacionales para todas las tecnologías eléctricas, electrónicas y afines.

International Organization for Standardization

Es el mayor organismo independiente no gubernamental de estandarización internacional y está compuesto por representantes de otros organismos de estandarización.

International Telecommunications Union

La Unión Internacional de Telecomunicaciones es un organismo especializado de las Naciones Unidas responsable de todos los asuntos relacionados con las tecnologías de la información y la comunicación Promueve el uso global compartido del espectro radioeléctrico, facilita la cooperación internacional en la asignación de órbitas de satélites, ayuda a desarrollar y coordinar las normas técnicas mundiales y trabaja para mejorar la infraestructura de telecomunicaciones en el mundo en desarrollo.

Internet Engineering Task Force

Es una organización de normalización que desarrolla y promueve estándares de Internet, en particular las normas técnicas que componen el conjunto de protocolos de Internet (TCP/IP).

Internet of Things

En castellano *Internet de las cosas*, es un término utilizado para referirse a la interconexión de diferentes elementos, tanto físicos como virtuales, que llevan incorporados sensores, software de procesamiento y otras tecnologías que permiten el intercambio de datos con otros dispositivos o sistemas através de Internet u otras redes de comunicación.

Interoperability of Heterogeneous IoT Platforms

Proyecto perteneciente al programa europeo de investigación Horizonte 2020 [2] en el que se ha encuadrado mayoritariamente el trabajo realizado en esta tesis. Consta de una solución de interoperabilidad orientada a capas

[2] https://inter-iot.eu/

(INTER-Layer), un conjunto de herramientas de desarrollo y configuración (INTER-FW), una herramienta CASE en base a una metodología para facilitar los despliegues de interoperabilidad (INTER-Meth) y tres pilotos de validación (INTER-LogP, INTER-Health e INTER-Domain).

Intranet

Una intranet es una red informática para compartir información y otros servicios informáticos dentro de una organización, normalmente excluyendo el acceso de personas ajenas a ella.

IPv6 over Low power Wireless Personal Area Networks

Grupo de trabajo perteneciente a la IETF cuyo objetivo era la creación de mecanismos que permiten la encapsulación y compresión de cabeceras para la transmisión de paquetes IPv6 sobre redes inalámbricas para dispositivos con capacidades limitadas.

Java Virtual Machine

Es una máquina virtual que permite al dispositivo donde esté instalado ejecutar programas Java, así como programas escritos en otros lenguajes que también se compilan en *bytecode* de Java.

Key Performance Indicators

Es un indicador de rendimiento para la medición del rendimiento de un proyecto. Es el principal factor que evalúa el éxito de una organización o actividad concreta.

Local Area Network

Red de telecomunicaciones de ámbito local que interconecta dispositivos en una zona limitada tal y como pueden ser los hogares, escuelas u oficinas.

Long Range Wide Area Network

Es una especificación que define los parámetros de la capa física inalámbrica de largo alcance (*LoRa*) desde el dispositivo a la infrastructura al igual que el protocolo que provee interoperabilidad entre fabricantes.

Long Term Evolution

La evolución a largo plazo es un estándar de comunicación inalámbrica de banda ancha para dispositivos móviles, basado en las tecnologías GSM/EDGE y UMTS/HSPA.

Low Power Local Area Network

Red local de telecomunicaciones inalámbricas diseñada para permitir comunicaciones a una baja tasa de bits y un consumo muy bajo de potencia.

Low Power Wide Area Network

Red de área amplia de telecomunicaciones inalámbricas diseñada para permitir comunicaciones de largo alcance a una baja tasa de bits y un consumo muy bajo de potencia.

Machine to Machine

La comunicación de máquina a máquina es una comunicación directa entre dispositivos que utilizan cualquier canal de transmisión (cableado o inalámbrico). Éste intercambio de información se produce entre dos máquinas remotas y suele utilizar mensajes no inteligibles para los humanos y mecanismos de compresión para optimizar la transmisión.

Massive Machine Type Communications

Paradigma de comunicaciones que implica el establecimiento de un gran número de conexiones a dispositivos que transmiten de forma intermitente pequeñas cantidades de tráfico.

Measuring Mobile Broadband Networks in Europe

Proyecto perteneciente al programa europeo de investigación Horizonte 2020. El objetivo del proyecto era el diseño, construcción y operación de una plataforma abierta, flexible y a escala europea para realizar experimentos en redes de banda ancha móvil 3G/4G.

Message Queuing Telemetry Transport

Es un protocolo de red ligero que sigue el modelo de publicación-suscripción para el transporte de mensajes entre dispositivos. El protocolo suele ejecutarse sobre TCP/IP, aunque cualquier protocolo de red que proporcione conexiones ordenadas, sin pérdidas y bidireccionales puede soportar este protocolo.

Metropolitan Area Network

Red telecomunicaciones que cubre un área geográfica mayor que la LAN. Suele componerse de varias LAN interconectadas a una misma Red Troncal o *backbone*, por ejemplo, la red de instituciones o corporaciones grandes o infraestructuras de red públicas municipales o regionales.

mobile Health

La salud móvil es un término utilizado para la práctica de medicina y salud pública con el apoyo de dispositivos móviles.

MODBUS

Protocolo de comunicación de datos originalmente diseñado para los controladores lógicos programables de la empresa Modicon. Hoy en día se ha convertido en el protocolo estándar *de facto* para la interconexión de dispositivos electrónicos industriales.

Narrow-Band IoT

El Internet de las Cosas de banda estrecha es un estándar de tecnología radioeléctrica de red de área amplia de baja potencia (LPWAN) desarrollado por el 3GPP para dispositivos y servicios celulares.

Network Function Virtualization

La virtualización de funciones de red es un concepto de arquitectura de red que aprovecha las tecnologías de virtualización para virtualizar funciones de nodos de red en bloques de construcción que pueden conectarse, para crear y prestar servicios de comunicación.

Network Management System

Es un conjunto de aplicaciones que permite a los administradores de red gestionar los componentes independientes de una red dentro de un marco de gestión de red mayor.

Network Slice

La fragmentación de la red 5G es una arquitectura de red que permite la multiplexación de redes lógicas virtualizadas e independientes en la misma infraestructura de red física

NFV Management and Orchestration

Marco para la gestión y orquestación de funciones de red virtualizadas y otros componentes de software. Además, permite la orquestación de los recursos de computación, almacenamiento, red y las funciones de red virtual como el enrutamiento, cortafuegos y equilibrio de carga.

OneM2M

Es una asociación mundial constituida por 8 de las principales organizaciones de desarrollo de normas TIC del mundo. El objetivo de la organización

es crear una norma técnica global para la arquitectura, interoperabilidad, especificaciones API y seguridad para tecnologías M2M e IoT.

Open Service Gateway Initiative

OSGi puede hacer referencia tanto a la alianza, al estándar o a la especificación que comparten las mismas siglas. La especificación describe un sistema modular y una plataforma de servicios para el lenguaje de programación Java mediante un modelo de componentes dinámicos.

Open Source MANO

Es una comunidad perteneciente a la ETSI y dirigida por los operadores que ofrece una pila de gestión y orquestación de código abierto (MANO) alineada con los modelos de información ETSI NFV y que cumple los requisitos de las redes NFV de producción.

Operational Support System

Son sistemas informáticos de apoyo a las operaciones utilizados por los proveedores de servicios de telecomunicaciones para gestionar sus redes. Apoyan funciones de gestión como el inventario de la red, el suministro de servicios, la configuración de la red y la gestión de fallos.

Personally Identifiable Information

Según el reglamento general de protección de datos (*GPDR* por sus siglas en inglés) una PII se define como "cualquier información que esté relacionada con una persona física identificada o identificable".

Radio Access Technology

Son las tecnologías de acceso radioeléctrico como método de conexión física a una red de comunicación basada en radio. Por ejemplo, un teléfono móvil admite múltiples RAT en el mismo dispositivo: Bluetooth, Wi-Fi, GSM, LTE o 5G.

Radio Frequency IDentification

La identificación por radiofrecuenciautiliza campos electromagnéticos para identificar y rastrear automáticamente las etiquetas adheridas a los objetos. Un sistema RFID consta de un pequeño transpondedor de radio, un receptor de radio y un transmisor. Cuando se activa por un impulso electromagnético de un dispositivo lector de RFID cercano, la etiqueta transmite datos digitales, normalmente un número identificativo, al lector.

Radio Resource Management

Es la gestión a nivel de sistema de las características de transmisión radioeléctrica en los sistemas de comunicación inalámbricos, por ejemplo las redes celulares, las redes de área local inalámbricas, los sistemas de sensores inalámbricos y las redes de radiodifusión.

REpresentational State Transfer

Arquitectura de transferencia de información entre máquinas especialmente diseñado para servicios Web. Define un conjunto de restricciones para el acceso y gestión de los recursos a través de una interfaz uniforme y métodos HTTP concretos.

Software Defined Network

Las redes definidas por software es un enfoque de la gestión de redes que permite una configuración de red dinámica y eficiente desde el punto de vista de la programación con el fin de mejorar el rendimiento y la supervisión de la red, lo que la asemeja más a la computación en nube que a la gestión de redes tradicional.

Software Development Kit

Generalmente, una colección de herramientas software para facilitar la creación o la extensión de aplicaciones software.

Standard Essential Patents

Una patente esencial es una patente que reivindica una invención que debe utilizarse para cumplir una norma técnica. Por lo tanto, las organizaciones de normalización suelen exigir a sus miembros que divulguen y concedan licencias sobre sus patentes y solicitudes de patentes pendientes que cubren una norma que la organización está desarrollando.

Standards Developing Organizations

Son organismos cuya función principal es el desarrollo, coordinación, revisión y producción de diferentes normas técnicas.

Tecnologías de la Información y la Comunicación

Es un término utilizado para hacer referencia a las tecnologías de la información integrado con las telecomunicaciones, incluyendo los sistemas de computación y software que permiten a los usuarios el acceso, almacenamiento, transmisión y manipulación de la información audiovisual.

Virtual Network Function

Servicios de red virtualizados que se ejecutan en plataformas de computación abiertas y que antes se llevaban a cabo mediante tecnología de hardware propietaria y dedicada.

Virtualized Infrastructure Manager

Es una parte específica de la arquitectura MANO. Es el responsable de controlar y gestionar los recursos de computación, almacenamiento y red de la infraestructura NFV.

Web Services Description Language

Es una interfaz en XML para la descripción de servicios web, normalmente a través de interfaces web SOAP.

Wide Area Network

Red de teleconmunicaciones que se extiende sobre una área geográfica muy amplia; Internet es considerada una red WAN.

Wireless Body Area Network

Es una red inalámbrica de dispositivos electrónicos "vestibles". Estos dispositivos pueden estar incrustados en el interior del cuerpo (como pueden ser los implantes médicos), sobre la superficie en una posición fija (pulseras) o portables (dispositivos de "bolsillo").

Wireless Sensor Networks

Son redes de sensores espacialmente dispersos y dedicados que controlan y registran las condiciones físicas del entorno y envían los datos recogidos a una ubicación central.

Acrónimos

3GPP	3rd Generation Partnership Project
5G	5th Generation Technology Standard for Broadmand Cellular Networks
5G NR	5G New Radio
5G-NSA	5G Non Standalone
5GENESIS	5GENESIS
6LowPAN	IPv6 over Low power Wireless Personal Area Networks
AIOTI	Alliance for Internet of Things Innovation
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
CASE	Computer Aided Software Engineering
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
CEP	Complex Event Processor
COAP	Constrained Application Protocol
CPS	Cyber-Physical Systems
ETSI	European Telecommunications Standards Institute
gNB	gNodeB
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IERC	European Research Cluster on the Internet of Things
IETF	Internet Engineering Task Force
INTER-HARE	INTER-HARE
IoT	Internet of Things

ISO	International Organization for Standardization
ITU	International Telecommunications Union
JVM	Java Virtual Machine
KPI	Key Performance Indicators
LAN	Local Area Network
LoRaWaN	Long Range Wide Area Network
LPLAN	Low Power Local Area Network
LPWAN	Low Power Wide Area Network
LTE	Long Term Evolution
m-Health	mobile Health
M2M	Machine to Machine
MAN	Metropolitan Area Network
MANO	NFV Management and Orchestration
mMTC	Massive Machine Type Communications
MONROE	Measuring Mobile Broadband Networks in Europe
MQTT	Message Queuing Telemetry Transport
NB-IoT	Narrow-Band IoT
NFV	Network Function Virtualization
NMS	Network Management System
NS	Network Slice
OSGI	Open Service Gateway Initiative
OSM	Open Source MANO
OSS	Operational Support System
PII	Personally Identifiable Information
RAT	Radio Access Technology
REST	REpresentational State Transfer
RFID	Radio Frequency IDentification
RRM	Radio Resource Management
SDK	Software Development Kit
SDN	Software Defined Network
SDO	Standards Developing Organizations
SEP	Standard Essential Patents
TIC	Tecnologías de la Información y la Comunicación
UIT	International Telecommunications Union
VIM	Virtualized Infrastructure Manager
VNF	Virtual Network Function
WAN	Wide Area Network

WBAN	Wireless Body Area Network
WSDL	Web Services Description Language
WSN	Wireless Sensor Networks

Capítulo 1

Introducción

1.1. Introducción

Internet de las Cosas ("Internet of Things" o IoT) es un paradigma de comunicación emergente que está siendo considerado como uno de los principales motores de la nueva era de la información. Internet de las Cosas considera la presencia ubicua en el entorno de un conjunto de "cosas", que mediante conexiones cableadas y/o inalámbricas y esquemas de direccionamiento únicos son capaces de compartir su estado, interactuar y cooperar entre ellos para crear nuevas aplicaciones y servicios. En los últimos años, Internet de las Cosas ha evolucionado de ser simplemente un concepto académico, construido alrededor de protocolos de comunicación y dispositivos, a un ecosistema con aplicaciones industriales y de negocio, gracias a las nuevas redes de acceso inalámbricas emergentes, sensores mejorados y sistemas embebidos con procesadores cada vez más eficientes y baratos.

Hoy en día ya no se cuestiona qué es Internet de las Cosas sino más bien, qué soluciones podemos aportar a las dificultades que surgen a la hora de implementar este nuevo paradigma.

Una de las dificultades que plantea el Internet de las Cosas es el procesamiento de la gran cantidad de datos sensoriales que se generan (y que están aumentando exponencialmente), lo que exige técnicas sofisticadas para procesar los datos. Los datos se utilizan de forma diferente para diferentes aplicaciones en función de los requisitos lo que suele ser una tarea compleja. La extracción del contexto ambiental, los datos del entorno y el comportamiento del usuario a partir de los sensores es un elemento clave para las aplicaciones en Internet de las Cosas. Dado que los sensores y dispositivos son muy diversos y generan

datos heterogéneos, la adquisición de conocimiento preciso a partir de los datos en bruto es una tarea difícil en entornos complejos y dinámicos.

Otra dificultad importante que surge en el Internet de las Cosas es la interoperabilidad entre los diferentes estándares y protocolos que dirigen y gestionan el conjunto de dispositivos y sus datos en la red.

El propósito de esta investigación será la búsqueda de una solución óptima para la interoperabilidad entre dispositivos de Internet de las Cosas mediante el desarrollo de una pasarela genérica y modular que permita la comunicación mediante múltiples redes de acceso y protocolos, así como la conexión con diferentes plataformas de Internet de las Cosas. Además, se propondrá como requisito indispensable que esta pasarela pueda ejecutar un procesamiento inteligente de los datos (que sea capaz de recopilar los datos, aplicar varias políticas de tratamiento de datos en función de los requisitos de una aplicación, y luego decidir si los datos tienen que ser procesados localmente o en la nube) cerca de los dispositivos IoT de manera que se pueda proporcionar una respuesta rápida a cualquier procesamiento local necesario.

También se incluirá, aunque no sea objeto explícito de esta investigación, un estudio exhaustivo de otras funciones y aspectos que pueden ser implementados en una pasarela de Internet de las Cosas, como puede ser la seguridad o la calidad de servicio.

1.2. Motivación

La importancia de desarrollar una arquitectura y una implementación que ha motivado el trabajo de investigación de esta tesis, se derivan de los problemas expuestos en la Sección 1.1. Es decir, la falta de interoperabilidad entre dispositivos y la falta de soluciones para ofrecer respuestas rápidas a grandes cantidades de datos de sensores. A continuación se enumeran los factores que han motivado la necesidad de realizar este trabajo de investigación:

- Los dispositivos están estrechamente acoplados con las plataformas IoT, lo que les impide interactuar con otros dispositivos y plataformas, por lo que crean silos cerrados.
- Algunas pasarelas no ofrecen soluciones modulares, por lo que son entornos cerrados sin posibilidad de extensión.
- La mayoría de pasarelas en entornos industriales ofrecen soluciones demasiado complejas, y no pueden adaptarse a entornos más sencillos.

- Algunas pasarelas no implementan algunos servicios importantes (por ejemplo, el descubrimiento), o lo hacen de forma manera incompatible.
- Los dispositivos itinerantes pueden perderse o ser inaccesibles, por lo que muchas veces se generan pérdidas de datos.
- Existen muy pocas pasarelas enfocadas a entornos industriales que sean de código abierto y con capacidad de ser desplegadas en el "Edge/Fog".

1.3. Objetivos

El objetivo general de esta investigación es el estudio de las soluciones de interoperabilidad entre dispositivos IoT alcanzables mediante la creación y desarrollo de una pasarela modular y extensible. Para ello, se cumplirán los siguientes objetivos específicos:

- Análisis y estudio de las diferentes patrones y mecanismos de interoperabilidad entre dispositivos IoT existentes, sus limitaciones y sus posibles soluciones.
- Estudio de la viabilidad en la creación de una pasarela modular y extensible que rompe con la concepción monolítica y separa las funciones en una parte física y otra virtual.
- Identificar los dispositivos, protocolos de red y plataformas más utilizadas en los entornos de Internet de las Cosas y estudiar su posible implementación en la pasarela IoT propuesta.
- Diseñar y desarrollar la pasarela IoT propuesta mediante tecnologías y herramientas de código abierto.
- Validar la solución propuesta y el prototipo de pasarela IoT mediante casos de uso definidos, así como el análisis de los resultados y conclusiones obtenidas.

1.4. Principales aportaciones

La siguiente lista de publicaciones, clasificadas por su tipología, han sido realizadas y publicadas en el marco de investigación de esta tesis doctoral.

1.4.1. Artículos en congresos internacionales

- E. Olivares and B. Molina and C. E. Palau and M. Esteve and M. A. Portugues and A. Garcia *Access Control in a Port - A GeoRBAC Approach* In *10th International Conference on Critical Information Infrastructures Security (CRITIS 2015)*, pages 37-40, October 2015. https://doi.org/10.1007/978-3-319-33331-1_19.

- M. Uriarte and O. Lopez and J. Blasi and O. Lazaro and A. Gonzalez and I. Prada and E. Olivares and C. E. Palau and B. Molina and M. A. Portugues and A. Garcia *Sensing Enabled Capabilities for Access Control Management: IoT as an Enabler for the Advanced Management of Access Control* In *2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI 2016)*, pages 253-258, April 2016. https://doi.org/10.1109/IoTDI.2015.20.

- E. Olivares and C. E. Palau and O. Lazaro and A. Gonzalez and O. Lopez and M. Uriarte and J. Blasi and I. Prada *Usable Access Control enabled by Sensing Enterprise Architectures* In *6th International IFIP Working Conference on Enterprise Interoperability (IWEI 2015)*, pages 1-10, May 2015. http://ceur-ws.org/Vol-1414.

- B. Molina and C. E. Palau and E. Olivares and M. Esteve and M. Montesinos and A. Romeu *Live Fallas: A Future Internet smart city APP for large-scale events* In *IEEE International Conference on Multimedia and Expo (ICME 2015)*, pages 1-4, June 2015. https://doi.org/10.1109/ICMEW.2015.7169828.

- M. Cankar and E. Olivares and M. Markovic and F. Fuart *Fog and Cloud in the Transportation, Marine and eHealth Domains* In *Euro-Par 2017: Parallel Processing Workshops*, pages 292-303, August 2018. https://doi.org/10.1007/978-3-319-75178-8_24.

1.4.2. Capítulos de libro

- M. Uriarte and O. Lopez and J. Blasi and O. Lazaro and A. Gonzalez and I. Prada and E. Olivares and C. E. Palau and M. A. Portugues and A. Garcia. *Sensing Enabled Capabilities for Access Control Management*, chapter 8, pages 149-167. Springer International Publishing, 2018. https://doi.org/10.1007/978-3-319-61300-0_8.

- E. Olivares and C. E. Palau et al. *IoT Platforms Initiative*, chapter 9, pages 265-289. River Publishers. July, 2016. https://doi.org/10.13052/rp-9788793379824.

1.4.3. Artículos en revistas

- B. Molina and E. Olivares and C. E. Palau and M. Esteve A Multimodal Fingerprint-Based Indoor Positioning System for Airports. *IEEE Access*, 6:10092-10106, 2018. https://doi.org/10.1109/ACCESS.2018.2798918.

1.4.4. Participación en proyectos de investigación

La concepción de la idea inicial para esta tesis doctoral, surge desde la realización de varios proyectos de investigación en los que he participado:

- *ACIO: Access control in organizations* [1]
- *DORA: Door to door information for airports and airlines* [2]
- *FiContent2: Future media internet for large scale Content experimentation 2* [3]
- *INTER-IoT: Interoperability of Heterogeneous IoT Platforms* [4]
- *PIXEL: Port IoT Environmental Leverage* [5]

1.4.5. Software

Una de las principales aportaciones de la presente tesis doctoral, es la implementación software de una pasarela IoT que cumple con la definición y los objetivos propuestos. Esta pasarela ha sido desarrollada en el marco del proyecto INTER-IoT y es de código abierto bajo una licencia "Apache 2.0".

[1] https://www.celticnext.eu/project-acio/
[2] https://ec.europa.eu/inea/en/horizon-2020/projects/h2020-transport/aviation/dora
[3] https://web.archive.org/web/20120125045627/http://www.fi-content.eu/
[4] https://inter-iot.eu/
[5] https://pixel-ports.eu/

1.5. Organización de la memoria

La memoria de la presente tesis doctoral está estructurada en 8 capítulos de la siguiente manera:

- En el Capítulo 2, se hace una revisión completa del estado del arte del Internet de las Cosas, de la interoperabilidad de los dispositivos, los modelos y arquitecturas actuales y se enumeran las carencias existentes. En la Sección 2.2 se examina la evolución del Internet de las Cosas: desde los sistemas ciberfísicos hasta lo que hoy en día conocemos como IoT. Basándose en esta evolución, en la Sección 2.3 se enumeran las características principales del Internet de las Cosas y se busca una definición correcta de este concepto. En la Sección 2.4 se citan los ámbitos de aplicación más comunes del Internet de las Cosas y qué ventajas ofrece su aplicación en cada sector. A continuación, en la Sección 2.5 se hace un estudio exhaustivo de los estándares más relevantes en el Internet de las Cosas, enfocado a los dispositivos y las pasarelas, puesto que son los pilares fundamentales para el correcto desarrollo de la arquitectura e implementación. El estudio de las pasarelas existentes, las tecnologías y los sensores/actuadores más utilizados y para los que se ha de dar soporte se exponen en la Sección 2.6. Finalmente, se listan los elementos diferenciadores de la pasarela propuesta en esta tesis doctoral en la Sección 2.7.

- En el Capítulo 3, se propone una arquitectura teórica de una pasarela de Internet de las Cosas que de respuesta a los problemas identificados entornos a la interoperabilidad entre dispositivos IoT. Para ello, en la Sección 3.2 se ofrece una visión general del Internet de las Cosas, los elementos que la componen, y los despliegues más comunes. En la Sección 3.3 se hace un estudio exhaustivo de los requisitos funcionales y no-funcionales necesarios que ha de cumplir la pasarela IoT propuesta, al igual que su nivel de importancia según la metodología "Volere". En la Sección 3.4 se propone la arquitectura de la pasarela dual (física y virtual), sus bloques funcionales (comunes, de la parte física y de la parte virtual). A continuación, se listan los posibles modelos de interacción según el despliegue realizado en la Sección 3.5. Finalmente, en la Sección 3.6 se especifica un modelo de datos completo de los elementos que componen la pasarela física y la pasarela virtual.

- En el Capítulo 4, se expone la implementación de la pasarela basándonos en lo establecido en la arquitectura y utilizando el lenguaje de programación "Java" y el "framework" modular con OSGI. En la Sección 4.2

se expone el "framework" de ejecución común y el hilo principal de la pasarela. A continuación, en la Sección 4.3 y la Sección 4.4 se muestran, respectivamente, las implementaciones específicas de la pasarela física y la virtual. En la siguiente Sección 4.5 se expone de manera concreta el módulo central de interconexión entre ambas partes de la pasarela, y el mecanismo de seguridad implementado. En la Sección 4.6 se muestra las opciones de extensibilidad e interacción que se han desarrollado en la pasarela. Finalmente, en la Sección 4.7 se detallan los diferentes KPI medidos durante las fases de implementación y validación.

- En el Capítulo 5, se presenta el proyecto de investigación europeo en el que el trabajo de esta tesis se encuadra, INTER-IoT. A continuación, en la Sección 5.1 y la Sección 5.2 se exponen los pilotos en los cuales ha sido evaluada la pasarela en casos de uso reales.

- En el Capítulo 6, se expone otro proyecto de investigación europeo en el que se ha validado la pasarela, 5GENESIS. En concreto, en la Sección 6.1 se presenta el piloto en el que se utilizó la pasarela.

- En el Capítulo 7, se presentan otros casos de uso (Sección 7.1, Sección 7.2, Sección 7.3) en los cuales se ha utilizado con éxito la pasarela.

- En el Capítulo 8, se concluye la exposición de esta tesis doctoral. En la Sección 8.1 se exponen las conclusiones obtenidas y lecciones aprendidas durante el transcurso de esta investigación. En la Sección 8.2 se resumen los logros y el alcance obtenido y finalmente, en la Sección 8.3, se enumeran las posibles líneas de trabajo futuras de este trabajo de investigación.

Capítulo 2

Estado del arte

2.1. Introducción

La conexión de máquinas inteligentes, dotadas de un número creciente de sensores electrónicos, a través de Internet, se conoce como "Internet de las Cosas" (IoT) [1]. En los casos de uso más habituales, gracias a IoT, cualquier objeto físico y virtual puede conectarse a otros objetos y a Internet, creando un tejido de conectividad entre las cosas y entre los usuarios y las cosas [2, 3].

El diseño de Internet y, en concreto, la extensión de Internet a IoT se basa en la convergencia de la infraestructura con el software y los servicios. Se requiere una práctica común para diseñar soluciones cruzadas entre el software y la infraestructura con el fin de proporcionar soluciones integradas para abordar los sistemas complejos actuales y futuros. [4]

En el entorno de IoT, esta convergencia es evidente, y la continua evolución genera cada vez más objetos y plataformas inteligentes conectadas que llevan incorporados sensores y sus respectivos servicios asociados.

Inicialmente, el concepto de IoT adquirido por la comunidad es la de una red de objetos inteligentes interconectados que son capaces de intercambiar información. Sin embargo, esta idea es aplicable a otro tipo de sistemas (como veremos a continuación los CPS y los WSN) por lo que es importante matizar las particularidades de un sistema IoT [5].

Los despliegues de IoT están aumentando, al igual que los estándares, las alianzas y el interés por la homogeneización. Todo ello está dando un fuerte impulso a que el IoT sea considerado hoy como una de las tecnologías emergentes más prometedoras. Cada vez más aparatos, coches, artefactos y accesorios

estarán conectados y se comunicarán entre sí y con otros objetos, aportando así una conectividad amplificada y una mejor visibilidad de la cadena de suministro. Las aplicaciones de IoT son numerosas y cada objeto puede transformarse en un objeto inteligente que envía varias informaciones valiosas a otros dispositivos [6].

En este capítulo abordaremos cómo surge el Internet de las Cosas y su evolución, analizaremos los ámbitos de aplicación más comunes en la actualidad y las arquitecturas y modelos de interconexión más comunes. A continuación se expondrán las diferentes soluciones existentes para la interoperabilidad entre dispositivos IoT, en qué ámbitos son aplicables, este análisis reforzarán los objetivos expuestos en 1.3.

2.2. Evolución del Internet de las Cosas

La evolución del Internet de las Cosas ha sido, y es, intrínseca a la evolución natural de las redes e Internet por lo que es muy difícil establecer un momento temporal en el que aparece el concepto de IoT. Cuando el grupo dedicado a IoT se propuso definir de forma concreta el concepto de Internet de las Cosas y sus atributos, se establecieron como precursores (y en cierto modo, coetáneos también) los CPS y los WSN.

Además, también reconocieron que la mayor dificultad en la definición de Internet de las Cosas radica principalmente en la visión particular y sesgada de las entidades proponentes.

2.2.1. Sistemas Ciberfísicos

En la mayoría de las actividades académicas y de proyectos, la diferencia entre Internet de las Cosas y los sistemas ciberfísicos no queda clara y es difícil encontrar una fuente que establezca una distinción clara entre ambos términos. La mayoría de las personas consideran que las dos definiciones son explicaciones diferentes de la misma idea y utilizan las palabras indistintamente. Sin embargo, existen diferencias reales e intentaremos abordar los puntos comunes y las diferencias entre estos dos conceptos.

Un sistema ciberfísico es un sistema de elementos computacionales que colaboran y controlan entidades físicas. Ocurre cuando los sistemas mecánicos y eléctricos (por ejemplo, los sensores y las herramientas de comunicación)

integrados en los productos y materiales se conectan en red utilizando componentes de software. Utilizan los conocimientos e información compartidos de los procesos para controlar de forma independiente los sistemas de logística y producción. En consecuencia, los sistemas ciberfísicos tienden a ir más allá de la mera identificación y control de cosas individuales para llegar al nivel de conexión en red entre objetos identificados y compartir información sobre una condición específica con el fin de lograr un determinado objetivo con mayor eficiencia. A diferencia de los sistemas embebidos tradicionales, el CPS es una red de aparatos que interactúan con entradas y salidas físicas en lugar de dispositivos independientes [7].

Las aplicaciones más comunes de los CPS suelen ser sistemas autónomos basados en sensores y habilitados para la comunicación. Por ejemplo, muchas redes de sensores inalámbricos monitorizan algún aspecto del entorno y transmiten la información procesada a un nodo central para que este pueda tomar decisiones con datos más fiables recogidos de numerosas fuentes distribuidas.

En este contexto, la llamada "red inteligente" puede considerarse un buen ejemplo de CPS. Una red inteligente es una red eléctrica modernizada que utiliza tecnologías de información y comunicación analógicas o digitales para recopilar y actuar sobre la información —como los comportamientos de proveedores y consumidores— de forma automatizada para mejorar la eficiencia, la fiabilidad, la economía y la sostenibilidad de la producción y distribución de electricidad [8, 9].

Por el contrario, un sistema de IoT parte del nivel en el que una "cosa" única se identifica mediante un identificador global único y se puede acceder a ella desde cualquier lugar y en cualquier momento. El nivel de información que se obtiene al acceder a la "cosa" puede ser tan bajo como un dato estático que se almacena en las etiquetas RFID. Principalmente, el Internet de las Cosas se ocupa de la identificación única, la conexión con Internet y la accesibilidad de las "cosas". Sin embargo, los objetos identificados en un sistema IoT pueden estar conectados en red para controlar un determinado escenario de forma coordinada, en cuyo caso se puede considerar que un sistema IoT crece hasta el nivel de un CPS.

En general podemos decir que los CPS se ocupan principalmente de la actividad colaborativa de los sensores o actuadores para lograr un determinado objetivo y para ello los CPS utilizan un sistema IoT para lograr el trabajo colaborativo de los sistemas distribuidos.

Una de las diferencias fundamentas entre los Sistemas Ciberfísicos e Internet de las Cosas, las "cosas" (los elementos físicos) deben estar conectadas a

Internet que es una red por encima de una Intranet o Extranet. Pero un CPS no tiene este requisito siempre que los objetos que colaboran estén identificados de forma única dentro del contexto de la aplicación y colaboren para lograr el objetivo de detección o actuación requerido.

De lo anterior podemos concluir que, desde el punto de vista de la red o la comunicación, un CPS parte de la interconexión y la colaboración de objetos en un escenario de intranet y puede crecer hasta el nivel de interconexión de objetos a través de Internet para lograr una tarea de detección o actuación colaborativa. Mientras que, desde el punto de vista de las aplicaciones, es la IoT la que parte del nivel más bajo de la identificación de un objeto para leer los datos almacenados estáticamente en las etiquetas RFID y puede crecer hasta el nivel de la interconexión entre los objetos identificados para realizar un trabajo de colaboración en el que, en este caso, crece hasta el nivel de CPS.

En general, desde el punto de vista de la red o de la comunicación, el Internet de las Cosas se dirige a una visión más amplia de la conexión de objetos en un aspecto global, mientras que desde el punto de vista de la aplicación, los CPS se dirigen a la coordinación de los objetos en red para lograr un objetivo específico.

2.2.2. Redes de Sensores Inalámbricos

Aunque es fácil confundir las Redes de Sensores Inalámbricos (o WSN por sus siglas en inglés) con un sistema de Internet de las Cosas, existe una clara diferencia entre ambos.

Una WSN es una red distribuida espacialmente de sensores autónomos que monitorizan las condiciones físicas o ambientales, como la temperatura, el sonido, la presión, etc., y pasan sus datos de forma cooperativa a través de la red hasta una ubicación central. La WSN está formada por "nodos", desde unos pocos hasta varios cientos o incluso miles, en los que cada nodo está conectado a uno (o a veces varios) sensores. El ámbito de la WSN se limita a la recolección coordinada de datos [10, 11].

En cambio, el alcance de un sistema IoT va más allá, el objetivo es llegar donde se pueda añadir inteligencia a los objetos para que puedan hacer el trabajo de actuación de forma que se pueda lograr un determinado objetivo sin intervención humana. Además, la identificación única de las "Cosas" y su conexión a Internet es otra característica necesaria de IoT que no pertenece a las WSN.

En general, las WSN pueden ser una parte de la IoT, ya que los sensores utilizados en un sistema de IoT pueden conectarse en red para lograr un resultado coordinado.

2.3. Definición y características principales del Internet de las Cosas

En esta sección numeraremos las características principales y necesarias para que una red de objetos interconectados pueda ser considerada una red IoT. Posteriormente concluiremos la sección desarrollando una definición de Internet de las Cosas que condense todo lo expuesto en las secciones anteriores.

2.3.1. Características principales del Internet de las Cosas

- **Interconexión de las "Cosas":** La primera característica de IoT se deriva del nombre que la describe. Es un sistema que se ocupa de la interconexión de "Cosas". La palabra "Cosa" se refiere a cualquier objeto físico que sea relevante desde la perspectiva del usuario o de la aplicación [12].

- **Conexión de las "Cosas" a Internet:** Del nombre IoT, también podemos aprender que las "Cosas" están conectadas a Internet. En consecuencia, del nombre podemos deducir que el sistema no es una Intranet o Extranet de las "Cosas" [13].

- **"Cosas" identificables de forma unívoca:** Un sistema IoT está compuesto por cosas que son identificables de forma unívoca [14, 10].

- **Ubicuidad:** Según la definición de la ITU [15] la ubicuidad es una característica importante de un sistema IoT que indica que la red está disponible en cualquier momento y lugar. Pero en el contexto de IoT el concepto "en cualquier lugar" y "en cualquier momento" no tiene por qué referirse, respectivamente, a "globalmente" y "siempre". El "en cualquier lugar" se refiere principalmente al concepto de dónde se necesita y el "en cualquier momento" se refiere igualmente a cuándo se necesita [11].

- **Capacidad de detección/actuación:** En el sistema IoT intervienen sensores/actuadores. Los sensores/actuadores están conectados a las "Cosas" y realizan la detección/actuación que aportan la inteligencia de las "Cosas".

- **Inteligencia incorporada:** Los objetos inteligentes y dinámicos, incorporan funciones de inteligencia y conocimiento como herramientas y se convierten en una extensión del cuerpo y la mente humanos.

- **Capacidad de comunicación interoperable:** El sistema IoT tiene una capacidad de comunicación basada en protocolos de comunicación estándar e interoperables [16].

- **Autoconfigurabilidad:** El otro comportamiento importante que tiene un sistema IoT es la "autoconfigurabilidad". Debido a la heterogeneidad de los dispositivos (incluyendo sensores, actuadores, dispositivos de almacenamiento, dispositivos de control de servicios, teléfonos móviles, elementos de red y ordenadores) y el número de dispositivos que se conectan a Internet bajo el paraguas del IoT, el control remoto o basado en la nube parece ser una tarea desalentadora destinada a sufrir una limitada escalabilidad. Por tanto, la dirección natural de los dispositivos IoT es gestionarse a sí mismos, tanto en términos de su configuración de software/hardware y su utilización de recursos (energía, ancho de banda de ancho de banda, acceso al medio, etc.). La autoconfiguración consiste principalmente en las acciones de descubrimiento de vecinos y descubrimiento de servicios, organización de la red y provisión de recursos [17].

- **Programabilidad:** Las "cosas" de un sistema IoT tienen una característica de programabilidad. En el nivel más sencillo, un dispositivo programable es aquel que puede adoptar una serie de comportamientos a las órdenes de un usuario sin necesidad de realizar cambios físicos.

2.3.2. Definición básica del Internet de las Cosas

Tras revisar la literatura existente y teniendo en cuenta lo expuesto en las secciones anteriores, podemos definir Internet de las Cosas de la siguiente manera:

> Internet de las cosas es la red entre objetos físicos o virtuales inteligentes conectados a Internet. Los objetos son unívocamente identificables y son capaces de intercambiar y/o modificar información sobre su estado mediante un protocolo y un esquema de datos acordado.

2.4. Ámbitos de aplicación del Internet de las Cosas

Actualmente, sería imposible enumerar todos los diferentes ámbitos y escenarios en los que son aplicados los conceptos y herramientas que ofrece Internet de las Cosas. Los escenarios de Internet de las Cosas varían sustancialmente dependiendo de su escala y complejidad.

En las siguientes subsecciones, definiremos los ámbitos de aplicación de IoT más comunes [18].

2.4.1. Transporte y logística

En la logística del transporte, IoT mejora no solo los sistemas de flujo de materiales, sino también el posicionamiento global y la autoidentificación de cargas. Además, aumenta la eficiencia energética y, por tanto, disminuye el consumo de energía. En conclusión, se espera que IoT aporte cambios profundos a la cadena de suministro global de suministro global a través del movimiento inteligente de la carga. Esto se logrará mediante la sincronización continua de la información de la cadena de suministro y el seguimiento en tiempo real de los objetos. También se espera que proporcione una naturaleza más transparente, visible y controlable a la cadena de suministro, permitiendo una comunicación más inteligente entre las personas y la carga [19].

2.4.2. Hogar inteligente

Los hogares inteligentes hoy en día ya son conscientes, gracias a IoT de lo que ocurre dentro de un edificio, incidiendo principalmente en tres aspectos: uso de recursos (conservación de agua y consumo de energía), la seguridad y el confort. El objetivo con todo esto es conseguir mejores niveles de confort

a la vez que se reduce el gasto global. Además, las casas inteligentes también abordan los problemas de seguridad mediante de mecanismos de detección de robos, incendios o entradas no autorizadas. Los actores involucrados en este escenario constituyen un grupo muy heterogéneo. Hay diferentes actores que van a cooperar en el hogar del usuario, como las empresas de Internet, los fabricantes de dispositivos de operadores de telecomunicaciones, proveedores de servicios multimedia de medios de comunicación, empresas de seguridad, compañías eléctricas, etc.

2.4.3. Ciudad inteligente

Aunque el término ciudad inteligente es todavía un concepto difuso, existe un acuerdo general en que se trata de una zona urbana que crea un desarrollo sostenible y una alta calidad de vida. Este modelo [20] aclara las características de una ciudad inteligente, que abarca la economía, las personas, la gobernanza, la movilidad el medio ambiente y la vida. Superar estas áreas clave puede hacerse a través de un fuerte capital humano o social y/o una infraestructura de TIC. En el caso de esta última, un primer análisis empresarial concluye que varios sectores/industrias se beneficiarán de ciudades más digitalizadas e inteligentes [21, 22].

2.4.4. Entornos industriales

Las empresas podrán hacer un seguimiento de todos sus productos mediante etiquetas RFID por de la cadena de suministro global; como consecuencia, las empresas reducirán sus gastos de funcionamiento (OPEX) y mejorarán su productividad gracias a una mayor integración con otros sistemas. En general, IoT proporcionará procedimientos automáticos que implican una drástica transformación de los empleados hacia actividades de mayor nivel, ya que los trabajadores serán sustituidos por escáneres de códigos de barras, lectores, sensores y actuadores. Sin duda, estas tecnologías traerán oportunidades para los trabajadores y se necesitará un gran número de técnicos para programar y reparar estas máquinas. Esto es sinónimo de una transferencia a trabajos de mantenimiento, pero también constituye un nuevo reto que ofrece una oportunidad para pasar a este tipo de empleos y evitar el desempleo [23].

2.4.5. Entornos comerciales

IoT satisface tanto las necesidades de los clientes como las de las empresas. La comparación de precios de un producto; o la búsqueda de otros productos de la misma calidad a precios más bajos o con las promociones de las tiendas no solo da información a los clientes, sino también a tiendas y negocios. Disponer de esta información en tiempo real ayuda a las empresas a mejorar su negocio y a satisfacer las necesidades de los clientes. Obviamente, las grandes cadenas minoristas aprovecharán su posición dominante para imponer el futuro mercado minorista de IoT. En particular empresas con posiciones de control, son capaces de impulsar la adopción de la tecnología IoT debido a sus considerables cuotas de mercado.

2.4.6. Entornos sanitarios

Hoy en día, las personas tienen ya la posibilidad de ser seguidas a distancia y controladas por especialistas. El seguimiento del historial de salud de las personas es otro aspecto que hace que la sanidad electrónica asistida por IoT sea muy versátil. Las aplicaciones comerciales podrían ofrecer la posibilidad de un servicio médico no solo a los pacientes sino también a especialistas, que necesitan información para proceder a su evaluación médica. En este ámbito, IoT hace que la interacción humana sea mucho más eficiente porque no solo permite la localización, sino también el seguimiento y la monitorización de los pacientes. Los actores más importantes en este escenario serán los hospitales públicos y privados. Cabe mencionar que los operadores de telecomunicaciones son bastante activos en el ámbito de la sanidad electrónica [24, 13, 25, 26].

2.4.7. Entornos energéticos

Este entorno tiene muchos solapamientos con otros escenarios, como el hogar y la ciudad inteligentes. Un reto en estos escenarios es detectar los medios que ayuden a ahorrar energía (“Smart Grid”). En relación con esta área de aplicación hay que destacar las iniciativas que implican una producción de energía limpia distribuida, ya que hoy en día muchas casas tienen paneles solares.

Como parte fundamental, la medición inteligente se considera una condición previa para permitir la supervisión, el control y la comunicación inteligentes en las aplicaciones de la red. El uso de plataformas IoT en la medición inteligente proporcionará los siguientes beneficios:

- Una red eficiente de contadores inteligentes que permite detectar y restablecer el servicio. Estas capacidades redundan en beneficio de los clientes.
- Proporciona a los clientes un mayor control sobre su consumo de energía o consumo de agua, proporcionándoles más opciones para gestionar sus facturas.
- Se espera que el despliegue de IoT de los contadores inteligentes reduzca la necesidad de construir centrales eléctricas. Construir centrales eléctricas que solo son necesarias para los picos de demanda ocasionales es muy caro. Un enfoque más económico es permitir que los clientes reduzcan su demanda mediante tarifas basadas en el tiempo u otros programas de incentivos, o de los consumos para apagar temporalmente los aparatos que no se utilizan.

Por último, combinando el análisis de la oferta y la demanda, las empresas energéticas podrán realizar una conformación más eficiente de la demanda. No se limitarán a incentivar a los consumidores, sino apagar los aparatos que no se necesiten (como el congelador durante 20 minutos). Además, estos procesos deben ocurrir automáticamente. De nuevo nos encontramos ante un escenario heterogéneo, en el que intervienen diversas partes interesadas. Los principales actores son, por supuesto, las empresas; pero también las entidades públicas serán actores importantes [8, 9].

2.5. Estándares relevantes de IoT

El Internet de las Cosas es un ecosistema muy cambiante, por tanto, los nuevos conceptos, arquitecturas y tecnologías sufren desde el principio de una alta volatilidad. Si en un breve período de tiempo no son adquiridos por la comunidad, desaparecen inevitablemente.

Para asegurar la correcta adopción de las tecnologías clave dentro del ecosistema de Internet de las Cosas y evitar el posible fracaso de las herramientas emergentes que son realmente útiles, diferentes entidades de estandarización y alianzas se esfuerzan en impulsar e intentar regular este ecosistema.

Como veremos más adelante, uno de los problemas y desafíos más grandes a los que se enfrentan las entidades de estandarización es la apropiación del mercado. Mediante estándares abiertos de comunicación e intercambio de información de las diferentes plataformas de Internet de las Cosas se intenta frenar la tendencia de crear “silos” aislados y que el ecosistema de Internet

de las Cosas converja hacia herramientas incapaces de interoperar entre ellos. Como podemos observar en la figura 2.1 Existen numerosas entidades y grupos de trabajo destinados con el fin de impulsar las diferentes iniciativas de estandarización.

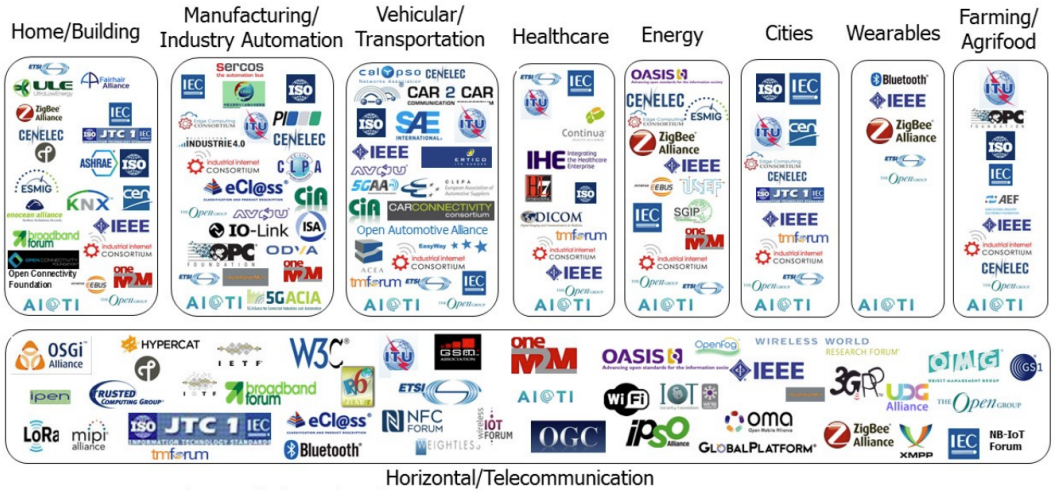

Figura 2.1: Alianzas y entidades de estandarización de IoT según sus ámbitos de aplicación[2]

A continuación describiremos los cuerpos y entidades de estandarización más relevantes para el trabajo de investigación realizado y que actualmente que tienen grupos de trabajo dedicados a la estandarización del ecosistema de Internet de las Cosas.

2.5.1. Alliance for Internet of Things Innovation (AIOTI)

La Comisión Europea puso en marcha la AIOTI en marzo de 2015 para crear un vibrante ecosistema de IoT en Europa, y tiene como objetivo principal romper los silos entre las principales áreas de aplicación vertical de IoT. Es una herramienta importante para apoyar la política y el diálogo dentro del ecosistema del Internet de las cosas y con la Comisión Europea.

[2]Fuente: AIOTI WG3 - Release 2.9 (2019)

AIOTI se basa en el trabajo del Grupo de Investigación Europeo en IoT (IERC) y amplía las actividades hacia la innovación dentro y entre las industrias. También ofrece la oportunidad de debatir sobre los obstáculos legales que impiden una mayor adopción de la IoT y de forjar un consenso. La Alianza también ayuda a la Comisión a preparar la futura investigación e innovación, normalización y política de IoT.

La alianza AIOTI se estructura en 11 grupos de trabajo (WG) de los cuales son de vital importancia el "WG3" cuyos objetivos se centran en la estandarización de IoT y los 7 grupos de trabajo dedicados a los diferentes dominios de aplicación de IoT.

2.5.2. British Standards Institute (BSI)

El Instituto Británico de Estandarización es relevante para IoT porque desarrolló las tres primeras normas de Ciudades Inteligentes y sentaron un gran precedente en el futuro desarrollo de otras normativas de estandarización.

Las normativas más importantes son:

- *PAS 180* [3]: Ciudades inteligentes. Vocabulario.
- *PAS 181* [4]: Marco para las ciudades inteligentes.
- *PAS 182* [5]: Modelo de concepto de ciudad inteligente.
- *PAS 212* [6]: Alianza HyperCat, propuesta de interoperabilidad y descubrimiento automático de dispositivos IoT.
- *EPL 278* [7]: Sistemas de transporte inteligentes.

[3] https://www.bsigroup.com/en-GB/smart-cities/Smart-Cities-Standards-and-Publication/PAS-180-smart-cities-terminology/
[4] https://www.bsigroup.com/en-GB/smart-cities/Smart-Cities-Standards-and-Publication/PAS-181-smart-cities-framework/
[5] https://www.bsigroup.com/en-GB/smart-cities/Smart-Cities-Standards-and-Publication/PAS-182-smart-cities-data-concept-model/
[6] https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2016/july/Internet-of-Things-interoperability-specification-is-published/
[7] https://standardsdevelopment.bsigroup.com/committees/50001517

2.5.3. Smart and Sustainable Cities and Communities Coordination Group

El Grupo de Coordinación de Ciudades y Comunidades Inteligentes y Sostenibles (SSCC-CG) es un grupo de coordinación entre los tres Organismos Europeos de Estandarización: CEN, CENELEC y ETSI. En él participan también los Organismos Nacionales de Estandarización (NSO) europeos y los organismos de representación de los consumidores, como la Asociación Europea para la de los Consumidores en la Estandarización y la Organización Europea de Ciudadanos del Medio Ambiente para la Estandarización.

- **Comité Europeo de Estandarización (CEN):** Varios comités técnicos tienen entre sus objetivos impulsar normativas de Internet de las Cosas en diferentes dominios de aplicación. Entre ellos: *TC-204* [8]: Dispositivos médicos, *TC-247: Automatización, control y gestión de edificios* [9], *TC-251: Informática sanitaria* [10]y *TC-278: Sistemas inteligentes de transporte* [11].

- **Comité Europeo de Estandarización Electrotécnica (CENELEC):** Numerosos grupos de trabajo tienen en cuenta las nuevas tecnologías y la incorporación de Internet de las Cosas en los diferentes dominios. Cabe destacar el grupo de trabajo

  Industry Best Practices and an Industry Code of Conduct for Licensing of Standard Essential Patents in the field of 5G and Internet of Things [12]

  cuyo objetivo es definir un conjunto de mejores prácticas recomendadas para la concesión de licencias SEP, en particular para beneficiar a los nuevos sectores y verticales preparados para reconocer los nuevos beneficios asociados a la adopción de 5G e IoT.

[8] https://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:6185&cs=10A20482E9369B3FEC68A9E396AE72531

[9] https://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:6228&cs=1B5974C9B3FD83E512BE27B1A4221DC20

[10] https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT,FSP_ORG_ID:37414,6232&cs=16013DFED8CF9EF7DBCC3BA21EB3D5E7A

[11] https://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:6259&cs=1EA16FFFE1883E02CD366E9E7EADFA6F7

[12] https://www.cenelec.eu/dyn/www/f?p=104:7:1426627901594201::::FSP_ORG_ID,FSP_LANG_ID:2409601,25

- **Instituto Europeo de Estándares de Telecomunicaciones (ETSI):** Desarrolla normas predominantemente en el área de las comunicaciones, pero recientemente desarrolla normas y arquitecturas para las capas superiores en la pila de protocolos de comunicación. Sus miembros se encargan colectivamente de redactar y acordar las normas organizadas en comités. Los comités más relevantes para la estandarización de IoT son: *CYBER* [13] (ciberseguridad), *SMARTM2M* [14] (IoT y comunicaciones máquina a máquina), *ITS* [15] (sistemas de transporte inteligentes) y *SMARTBAN* [16] (redes de área personal inteligentes).

2.5.4. OneM2M

Este organismo de estandarización se puso en marcha en 2012. Se trata de una iniciativa mundial que desarrolla especificaciones para garantizar el despliegue más eficiente de los sistemas de comunicación Máquina a Máquina (M2M) y el Internet de las Cosas (IoT). Las especificaciones de OneM2M proporcionan un marco para apoyar aplicaciones y servicios como la red inteligente, el coche conectado, la automatización del hogar, la seguridad pública y la salud.

OneM2M es la especificación con mayor tracción, ya que fue fundado por organismos de estandarización mundiales de reconocido prestigio (en Europa).

2.5.5. Institute of Electrical and Electronics Engineers (IEEE)

La Asociación de Normas del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE-SA) está estableciendo un marco de referencia y una arquitectura para IoT. El marco arquitectónico definido en la norma *IEEE 2413* [17]tiene como objetivo promover la interacción entre dominios, ayudar al sistema interoperabilidad y la compatibilidad funcional de los sistemas de IoT. IEEE-SA también desarrolla normas de IoT en diferentes sectores, los más relevantes son:

[13] https://www.etsi.org/committee/1393-cyber
[14] https://www.etsi.org/committee/1414-smartm2m
[15] https://www.etsi.org/committee/1402-its
[16] https://www.etsi.org/committee/1413-smartban
[17] https://standards.ieee.org/standard/2413-2019.html

- **Comunicaciones:** *IEEE 802* – comunicaciones cableadas e inalámbricas [18]; *IEEE 802.15.4* - comunicaciones en redes inalámbricas de baja capacidad [27]; *IEEE 1901* - comunicaciones sobre líneas eléctricas [28].

- **Transporte:** *IEEE 802.11p* - capas inferiores del sistema WAVE (acceso inalámbrico en entornos vehiculares) [29]; *IEEE 1609* - capas superiores del sistema WAVE [30].

- **Salud:** *IEEE 11073* - comunicaciones de dispositivos sanitarios [31].

- **Energético:** *IEEE 2030.5* - protocolos de aplicación en redes eléctricas inteligentes [32]

- **Transductores:** *IEEE 1451* - interfaces de comunicación de sensores y actuadores a microprocesadores [33]; *IEEE 2700* - especificaciones de terminología, condiciones y limites de los tipos de sensores más comunes [34].

IEEE también puso en marcha en 2014 una iniciativa dedicada a IoT cuyo objetivo es servir de punto de encuentro para la comunidad técnica mundial que trabaja en el Internet de las Cosas.

2.5.6. Internet Engineering Task Force (IETF)

La IETF definió una pila de protocolos específica para IoT (figura 2.2), y sobre él ha desarrollado varios estándares.

[18] https://www.ieee802.org/

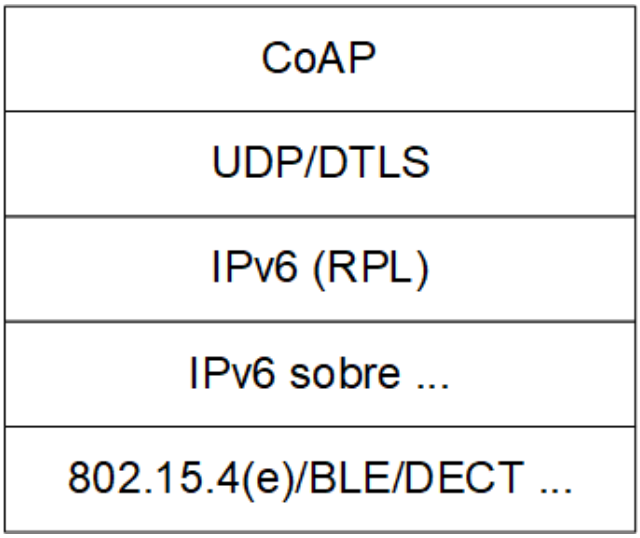

Figura 2.2: Pila de protocolos IoT de IETF

Podemos destacar los siguientes estándares:

- ***Constrained Application Protocol (COAP)*:** Protocolo a nivel de aplicación cuyo formato de mensaje está adaptado a dispositivos limitados (*RFC 7252* [35]), que sigue los mismos principios REST utilizados en HTTP.

- ***IPv6 over Low power Wireless Personal Area Networks (6LowPAN):*** Mecanismos de encapsulación y compresión que permiten el transporte de paquetes IPv6 sobre redes *IEEE 802.15.4* [27], definido en la *RFC 4944 [36]*.

- ***Routing Over Low power and Lossy networks (ROLL)*:** Es un grupo de trabajo enfocado a los mecanismos de enrutamiento sobre redes de baja capacidad y mucho ruido. En concreto la *RFC 6550* [37] define el protocolo de enrutamiento sobre este tipo de redes (RPL).

2.5.7. International Organization for Standardization (ISO)

ISO es una SDO de nivel global y cuenta con representación mundial de los NSO. La participación normalmente solo es posible a través de la acreditación

de un NSO. Son relevantes los comités **ISO TC 184** (Sistemas de automatización e integración) [19], **ISO TC 204** (Sistemas de transporte inteligentes) [20] e **ISO TC 215** (Informática sanitaria) [21].

2.5.8. International Electrotechnical Commission (IEC)

La IEC es una organización mundial de miembros sin ánimo de lucro, cuyo trabajo sustenta la infraestructura de calidad y el comercio internacional de productos eléctricos y electrónicos. Nuestro trabajo facilita la innovación técnica, el desarrollo de infraestructuras asequibles, el acceso eficiente y sostenible a la energía, la urbanización y los sistemas de transporte inteligentes, la mitigación del cambio climático y el aumento de la seguridad de las personas y el medio ambiente.

El comité técnico **ISO IEC JTC1** [22] sobre las tecnologías de la información y la comunicación han desarrollado múltiples estándares que han sido clave para el desarrollo y evolución del Internet de las Cosas, particularmente el grupo de trabajo WG10 ha definido múltiples estándares específicas de IoT. Entre los estándares más importantes podemos destacar:

- **ISO/IEC 30141:** Arquitectura de referencia de Internet de las Cosas [38].
- **ISO/IEC 20924:** Definiciones y vocabulario de Internet de las Cosas [39].
- **ISO/IEC 21823:** Interoperabilidad entre sistemas de Internet de las Cosas: *ISO/IEC 21823-1* (marco de referencia) [40], *ISO/IEC 21823-2* (interoperabilidad de transporte) [41] y el estándar que está en desarrollo *ISO/IEC 21823-3* (interoperabilidad semántica) [42].
- **ISO/IEC 29182:** Son un grupo de estándares que sentaron las bases para crear una arquitectura de referencia de redes de sensores, cubren desde la terminología y conceptos generales [43][44][45], modelos y entidades [46], interfaces [47], aplicaciones [48] e interoperabilidad entre distintas redes de sensores [49].

[19] https://www.iso.org/committee/54110.html
[20] https://www.iso.org/committee/54706.html
[21] https://www.iso.org/committee/54960.html
[22] https://www.iso.org/isoiec-jtc-1.html

- **ISO/IEC 20992:** Es una estándar que especifica el protocolo de transporte *Message Queuing Telemetry Transport* (MQTT). Es un protocolo de mensajería cliente-servidor con modelo publicación/suscripción. Es ligero, abierto, sencillo y diseñado para que sea fácil de implementar [50].

- **Estándares desarrollados por ISO/IEC SC27:** El comité SC27 abarca la elaboración de normas para la protección de la información y las TIC. Este incluye métodos, técnicas y directrices genéricas para abordar aspectos tanto de la seguridad como de la privacidad, entre ellas han sido y son especialmente relevante para el desarrollo y evolución del Internet de las Cosas: *ISO/IEC 29100* (marco de privacidad) [51], *ISO/IEC 29101* (marco de la arquitectura de la privacidad) [52], *ISO/IEC 29134* (directrices para la evaluación del impacto sobre la privacidad) [53], *ISO/IEC 29151* (código de prácticas para la protección de la Información Personal Identificable (PII)) [54], *ISO/IEC 27018* (código de prácticas para la protección de la PII en las nubes públicas que actúan como procesadores de PII) [55].

2.5.9. Unión Internacional de Telecomunicaciones (UIT)

La UIT (ITU por sus siglas en inglés) es una agencia especializada en el sector de las TIC que depende de la Organización de las Naciones Unidas. Está divida en tres sectores principales: La UIT-R que se encarga de la regulación internacional del espectro de radiofrecuencia, la UIT-T cuya misión es la estandarización internacional en el sector de las TIC y la UIT-D que cuyo foco es el impulso de las TIC en países en vías de desarrollo.

Los principales productos de la UIT-T son las Recomendaciones, es decir, estas no son obligatorias hasta que no se adopten en las legislaciones nacionales. No obstante, el nivel de cumplimiento es elevado.

El grupo de trabajo *SG20* es el encargado de redactar las Recomendaciones relacionadas con el Internet de las Cosas. Son muchas las recomendaciones redactadas por este grupo de trabajo, las más importantes y las que se han tenido en cuenta para realizar este trabajo de investigación son las siguientes:

- **Definición y caracterización del Internet de las Cosas:** Visión general [56], términos y definiciones [15], requisitos comunes [57] [58] y recomendaciones sobre el marco funcional y las capacidades del Internet de las cosas [59].

- **Redes de sensores y capa de dispositivos:** Requisitos de las redes de sensores ubicuas (USN) en las redes de próxima generación (NGN) y sus aplicaciones [11] [60] [61] [10] [62],

  Marco de gestión de redes de sensores basado en SNMP [63]. Redes de control de sensores y aplicaciones relacionadas en un entorno de red de próxima generación [62]. Marco de trabajo de las redes de dispositivos restringidos en los entornos del IoT [64]. Modelos arquitectónicos de referencia de dispositivos para aplicaciones de la Internet de las cosas [65]. Requisitos y casos de uso del módulo de comunicación universal de los dispositivos móviles del IoT [66]. Marco de software inteligente y ligero para los dispositivos del Internet de las cosas [67].

- **Redes de sensores y capa de dispositivos:** Requisitos para el soporte de aplicaciones y servicios de redes de sensores ubicuos (USN) en el entorno de las NGN [11]. Requisitos funcionales y arquitectura de la red de próxima generación para el soporte de aplicaciones y servicios de redes de sensores ubicuas [60] Descripción de servicios y requisitos para el "middleware" de redes de sensores ubicuas [61]. Marco de gestión de redes de sensores basado en SNMP [63]. Redes de control de sensores y aplicaciones relacionadas en un entorno de red de próxima generación [62]. Requisitos y arquitectura funcional de la plataforma abierta de servicios de redes de sensores ubicuos [10]. Marco de trabajo de las redes de dispositivos restringidos en los entornos del IoT [64]. Modelos arquitectónicos de referencia de dispositivos para aplicaciones de la Internet de las cosas [65]. Requisitos y casos de uso del módulo de comunicación universal de los dispositivos móviles del IoT [66]. Marco de software inteligente y ligero para los dispositivos del Internet de las cosas [67].

- **Pasarelas y conexión con la capa de red:** Requisitos y características comunes del identificador de IoT para el servicio de IoT [14]. Requisitos y capacidades comunes de la gestión de dispositivos en el Internet de las cosas [68]. Requisitos de la red para el Internet de las cosas [69]. Requisitos y capacidades comunes de una pasarela para aplicaciones del Internet de las cosas [70]. Arquitectura del Internet de las cosas basada en la evolución de la red de próxima generación [71]. Arquitectura funcional de la pasarela para aplicaciones del Internet de las cosas [72].

- **Seguridad y control de acceso:** Capacidades de seguridad que apoyan la seguridad del Internet de las cosas [73]. Requisitos de accesibilidad para las aplicaciones y servicios del Internet de las cosas [74]. Marco del servicio de delegación para los dispositivos del Internet de las cosas [75].

- **Otros:** Requisitos de la capacidad "plug and play" del Internet de las cosas [76]. Requisitos del Internet de las cosas para apoyar la computación de borde [77].

2.5.10. Open Services Gateway initiative (OSGI)

La Alianza OSGi es un consorcio mundial que promueve un proceso probado y maduro para crear especificaciones abiertas. Estas especificaciones permiten la conectividad dinámica de extremo a extremo y facilitan la subdivisión en varios componentes del software y las aplicaciones, aumentando así la productividad del desarrollo reduciendo el tiempo de comercialización y disminuyendo sustancialmente los costes de mantenimiento a largo plazo de la solución modular resultante. La tecnología también proporciona una gestión remota flexible e interoperabilidad para aplicaciones y servicios en una amplia variedad de dispositivos. Entre los sectores de las empresas miembros se encuentran los principales proveedores de servicios y contenidos, operadores de infraestructuras/redes, empresas de servicios públicos, proveedores de software empresarial, desarrolladores de software, puertas de enlace, etc. proveedores de software empresarial, desarrolladores de software, proveedores de pasarelas, proveedores de electrónica de consumo/dispositivos (cableados e inalámbricos) e instituciones de investigación.

OSGi responde intrínsecamente a muchos requisitos del IoT. Sus características más importantes se pueden enumerar como:

- Un entorno de ejecución modular que permite la reutilización funcional de los componentes en diversas plataformas.
- Un modelo flexible de Capacidades / Requisitos que permite el despliegue consciente del entorno y la gestión de dependencias.
- Un entorno dinámico que permite actualizar y/o reconfigurar los componentes del sistema sin necesidad de reiniciarlos.
- Componentes conscientes del ciclo de vida que son capaces de responder a los cambios en su entorno, por ejemplo, la adición/activación de un dispositivo de hardware.
- Soporte para el despliegue dinámico de bibliotecas nativas basado en las capacidades del sistema descubiertas.

- Un modelo de seguridad definido para determinar si los módulos de software son de confianza y las acciones que pueden realizar.

- API comunes para la conectividad de los dispositivos mediante varios protocolos de comunicación subyacentes.

- Una interfaz común estandarizada de gestión remota que utiliza diversos protocolos, como JMX y HTTP/REST.

- Modelos de programación para entornos distribuidos que utilizan invocaciones síncronas o asíncronas. Adecuado para su uso en entornos de borde o en la nube.

2.6. Interoperabilidad en la Capa física

2.6.1. Pasarelas existentes y ámbitos de aplicación

Como parte del estudio del estado del arte, es importante analizar las pasarelas IoT más utilizadas y sus ámbitos de aplicación; para a continuación, poder situar la pasarela IoT objeto de esta tesis doctoral, ubicarla en este mapa y poder listar sus elementos diferenciadores en la Sección 2.7. Es importante tener en cuenta en este punto que **solo se tiene en cuenta el Software que ejecuta la lógica de una pasarela**, puesto que el Hardware no es objeto de estudio en esta tesis.

Las pasarelas IoT más utilizadas hoy en día se pueden clasificar por su ámbito de aplicación **industrial** o de **hogar inteligente**. En la Figura 2.3 se clasifican por este ámbito de aplicación y por su forma de distribución que puede ser de **código abierto**, **propietarias** o **proveedores en la Nube**.

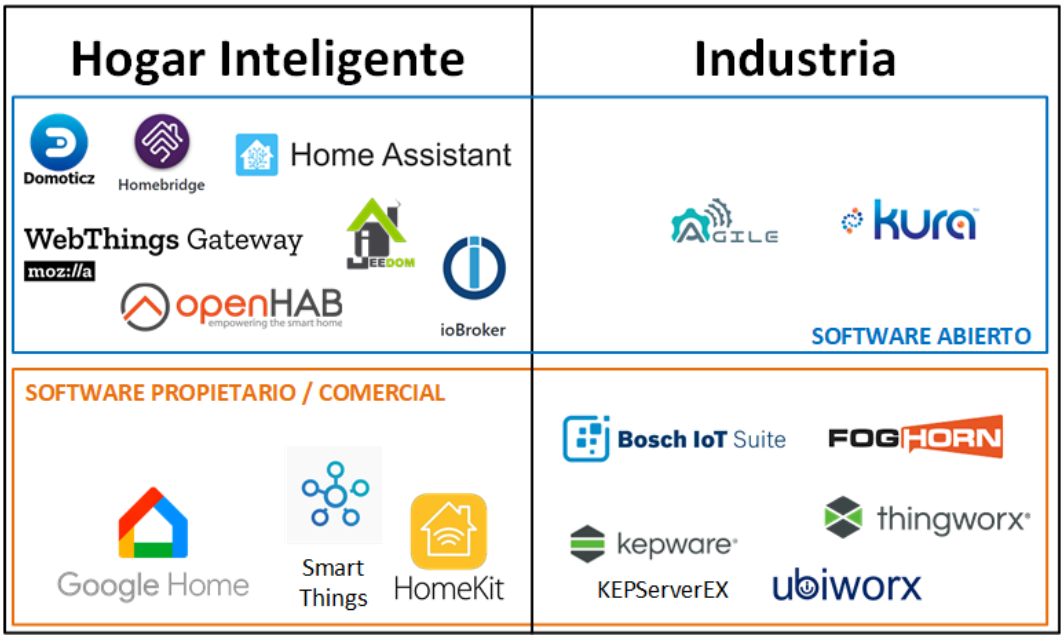

Figura 2.3: Comparativa actual de Pasarelas IoT

- **Ámbito de Hogar Inteligente:**
  - **Software Abierto:**
    - *Domoticz* - Es un sistema de automatización del hogar muy ligero que le permite supervisar y configurar diversos dispositivos, incluyendo luces, interruptores, varios sensores/medidores como la temperatura, la lluvia, el viento, la radiación ultravioleta (UV), el uso/producción de electricidad, el consumo de gas, el consumo de agua y muchos más. Se pueden enviar notificaciones/alertas a cualquier dispositivo móvil. La primera versión de Domoticz fue en diciembre de 2012, está escrito en el lenguaje de programación "C++". [23]
    - *Homebridge* - Permite integrarse con dispositivos domésticos inteligentes que no son compatibles de forma nativa con HomeKit. Hay más de 2.000 plugins de Homebridge que admiten miles de accesorios inteligentes diferentes. Esta solución solo añade una capa de compatibilidad con HomeKit, por lo que necesita de

[23] https://www.domoticz.com/

esta para poder controlar los dispositivos. El proyecto se inició en diciembre de 2014 y está escrito en "JavaScript/NodeJS". [24]

- *Home Assistant* - Es un software gratuito y de código abierto para la automatización del hogar que está diseñado para ser el sistema de control central para los dispositivos del hogar inteligente con enfoque en el control local y la privacidad. Se puede acceder a él a través de una interfaz de usuario web, a través de aplicaciones complementarias para Android e iOS, o utilizando comandos de voz a través de un asistente virtual compatible como "Google Assistant" o "Amazon Alexa". La primera versión aparece en septiembre de 2013 y está escrito en "Python". [25]
- *WebThings Gateway* - Es parte del "WebThings Framework" de la fundación "Mozilla", que es una plataforma abierta para supervisar y controlar dispositivos a través de la web. WebThings Gateway es una distribución de software para pasarelas domésticas inteligentes que permite a los usuarios supervisar y controlar directamente su hogar inteligente a través de la web, sin intermediarios. El proyecto de la pasarela se inicia en marzo de 2017 y está escrito en "JavaScript/NodeJS". [26]
- *JeeDom* - Se puede instalar en cualquier distribución de Linux, tiene una interfaz Web que permite crear escenarios, reglas, consultar históricos y crear interacciones. Se pueden instalar una serie de complementos para añadir compatibilidad con otros dispositivos, estos complementos pueden ser gratuitos o de pago. El proyecto se inicia en noviembre de 2014 y está escrito en "PHP". [27]
- *openHAB* - Empieza como un proyecto de la fundación "Eclipse" llamado "Eclipse SmartHome". Se despliega en las instalaciones y se conecta a dispositivos y servicios de diferentes proveedores. Las acciones, como el encendido de las luces, se activan mediante reglas, comandos de voz o controles en la interfaz de usuario de openHAB. Comienza el proyecto en el año 2010 y está escrito en "Java".
- *ioBroker* - Es una solución de software libre que conecta com-

[24] https://homebridge.io/
[25] https://www.home-assistant.io/
[26] https://webthings.io/
[27] https://www.jeedom.com/

ponentes de automatización de edificios de una amplia gama de proveedores de manera neutral en cuanto a fabricantes y protocolos en una sola plataforma. Surge del proyecto CCU.IO en 2014 y está escrito en "JavaScript/NodeJS". [28]

- **Software Propietario:**
  - *Google Home* - Ahora denominado "Google Nest", es un altavoz que tiene integrado el asistente virtual "Google Assistant" y una de sus múltiples funciones es como pasarela de dispositivos compatibles. Su conexión con otros dispositivos es a través de red, puesto que se conecta con la red del hogar a través de "Wi-Fi". También tiene soporte para dispositivos a través de "Bluetooth". El producto aparece en 2016 y en 2018 se fusiona con "Nest" para crear "Google Nest". [29]
  - *Samsung Smart Things* - Es una plataforma IoT y pasarela de dispositivos compatibles, además, también fabrica sus propios dispositivos. Se funda en 2012 y es adquirido por Samsung en 2014. [30]
  - *Apple HomeKit* - Es una plataforma de hogar inteligente que se integra con el asistente virtual de Apple "Siri". Es similar a "Google Home", en cuanto a que la pasarela se conecta a través de la red del hogar y funciona sobre el altavoz "HomePod" o en un "iPad", y se conecta a dispositivos compatibles. [31]

- **Ámbito Industrial:**
  - **Software Abierto:**
    - *Eclipse Kura.* - Eclipse Kura es un marco extensible de código abierto de IoT Edge basado en Java/OSGi. Kura ofrece acceso por API a las interfaces de hardware de las pasarelas IoT (puertos serie, GPS, watchdog, GPIOs, I2C, etc.). Cuenta con protocolos de campo listos para usar (incluyendo MODBUS, OPC-UA, S7), un contenedor de aplicaciones y una programación de flujo de datos visual basada en la web para adquirir datos del campo, procesarlos en el borde y publicarlos en las

[28] https://www.iobroker.net/
[29] https://store.google.com/us/product/google_home_mini_first_gen
[30] https://www.smartthings.com/
[31] https://www.apple.com/ios/home/

principales plataformas de nube de IoT a través de la conectividad MQTT. [32]

- *Agile* - AGILE (Adaptive Gateways for dIverse muLtiple Environments) construye una pasarela modular de hardware y software para el Internet de las Cosas con soporte para la interoperabilidad de protocolos, la gestión de dispositivos y datos, la ejecución de aplicaciones IoT y la comunicación externa en la nube, con diversas actividades piloto, convocatorias abiertas y creación de comunidades. [33]

- **Software Propietario:**
  - *Bosch IoT Suite* - Es una solución completa de IoT incluyendo una pasarela inteligente. Permite conectar y gestionar de forma fiable dispositivos, sensores y microcontroladores, visualizar los datos de diversas fuentes y ejecutar procesos de actualización de forma remota. [34]
  - *FogHorn* - Es también una solución completa que utiliza inteligencia artificial en el "Edge" de forma segura. Ofrece análisis en tiempo real sobre grandes volúmenes, variedades y velocidades de datos de sensores y máquinas en vivo, y está optimizado para una computación y conectividad limitadas. [35]
  - *KEPServerEX* - También ofrece una solución IoT completa, por lo que no es solamente una pasarela. Proporciona una única fuente de datos de automatización industrial a todas sus aplicaciones. Y permite a los usuarios conectar, gestionar, supervisar y controlar diversos dispositivos de automatización y aplicaciones de software a través de su interfaz. [36]
  - *Thingworx* - Es una solución que incluye una plataforma y pasarelas IoT y conectan de forma segura a las empresas con sus fábricas, productos y entornos de servicio posventa. [37]
  - *Ubiworx* - Es un software IoT para sistemas embebidos, permitiéndoles actuar como pasarelas que conectan sensores y actuadores con sistemas de análisis y almacenamiento de datos en la

[32] https://www.eclipse.org/kura/
[33] http://agile-iot.eu/
[34] https://bosch-iot-suite.com/
[35] https://www.foghorn.io/
[36] https://www.kepserverexopc.com/kepware-kepserverex-features/
[37] https://www.ptc.com/es/products/thingworx

nube también ofrecidos por Ubiworx. [38]

Además, existen también una serie de **proveedores en la Nube** que se categorizan más como plataformas IoT entre ellas: *Azure IoT Hub* [39], *AWS IoT Core* [40], *Oracle IoT Cloud* [41] y *Google IoT Core* [42]. Pero dada su alta ubicuidad y disponibilidad, a su vez que la facilidad de integración a través de sus APIs y SDKs, permiten que muchos dispositivos con capacidades menos limitadas y con acceso a internet puedan ser gestionados directamente por estas plataformas.

2.6.2. Tipos de sensores y actuadores más comunes

El IoT se compone de varias capas tecnológicas que permiten a las cosas normales compartir los datos que recogen a través de Internet para, en última instancia, ofrecer inteligencia, acciones autónomas y valor que dependen en gran medida de la calidad de los propios datos. Por lo tanto, los sensores y los actuadores son una parte indispensable de la pila tecnológica de IoT y un factor decisivo en el desarrollo de todo sistema de IoT.

Un sensor, también llamado transductor, es un dispositivo cuya tarea es detectar eventos o cambios en su entorno inmediato y convertir estos fenómenos físicos en impulsos eléctricos que luego pueden interpretarse de forma significativa. Un actuador, en cambio, puede considerarse una herramienta que funciona de forma inversa al sensor. Al interpretar los impulsos eléctricos enviados desde el sistema de control y convertirlos en movimiento mecánico, introduce realmente cambios en su entorno físico mediante una serie de acciones sencillas.

Aunque los sensores y actuadores eléctricos ordinarios existen desde hace décadas y están omnipresentes en las aplicaciones industriales modernas, la aparición del Internet de las Cosas ha abierto posibilidades completamente nuevas de aplicación de los sensores y actuadores IoT no solo en el sector industrial, sino también en el ámbito del uso comercial y doméstico. Como habilitadores indispensables de IoT, los sensores y actuadores ayudan a supervisar, controlar y agilizar las operaciones en casi todo tipo de sectores.

[38] https://ubiworx.com/
[39] https://azure.microsoft.com/en-us/services/iot-hub/
[40] https://aws.amazon.com/iot-core/
[41] https://www.oracle.com/internet-of-things/
[42] https://cloud.google.com/iot-core

A continuación, se listan los tipos de sensores más comunes en IoT:

- **Movimiento:** Acelerómetros, Giroscopios y de posición (GPS)
- **Ambiente:** Temperatura, Humedad, Presión, Magnetómetros, Ópticos (cantidad de luz, de presencia o "P.I.R", de proximidad), Químicos, Acústicos
- **Biológicos:** Tensiómetro, Temperatura corporal, Oxímetros, Electrocardiograma
- **Eléctricos:** Sensores de corriente, voltaje, impedancia, etc.

Los actuadores más utilizados en IoT son eléctricos, puesto que traducen la señal eléctrica en un cambio físico. Muchos actuadores realmente se basan en los siguientes tipos básicos (por ejemplo, los termostatos normalmente se basan en motores de pasos):

- **Eléctricos:** La gran mayoría de los actuadores son eléctricos. En este tipo de actuadores se incluyen los que ajustan salidas de voltaje/amperaje específico (por ejemplo, para ajustar la cantidad de luz) y también relés o solenoides para activar/desactivar un circuito eléctrico de potencia.
- **Movimiento lineal:** Se utilizan en aplicaciones industriales y permiten ajustar una posición específica. Se pueden encontrar, por ejemplo, en válvulas y amortiguadores. Muchos de estos actuadores generan el movimiento lineal a partir de un movimiento circular.
- **Movimiento circular:** Son también muy comunes, incluyen servomotores (ajustan con precisión el ángulo, la velocidad o la aceleración, pero tienen poca fuerza), motores de pasos (con divisiones discretas del ángulo de rotación o "pasos") y motores de movimiento continuo (giran a gran velocidad con base en una corriente de entrada).

2.7. Elementos diferenciadores de la Pasarela

Tras analizar las pasarelas existentes en Subsección 2.6.1 y según podemos ver en la Figura 2.3, es notable la falta de pasarelas de código abierto orientada para la industria [78]. Además, estas pasarelas tienen importantes carencias en cuanto a la interoperabilidad de dispositivos y la flexibilidad en su despliegue y funcionamiento.

Por tanto, podemos listar los elementos diferenciadores de la pasarela física/virtual desarrollada con respecto a las soluciones de código abierto enfocadas a la industria:

- **Flexibilidad de despliegue:** La separación en una parte física y otra virtual posibilita el despliegue en numerosas configuraciones diferentes. Puede estar la parte física y la virtual en el mismo dispositivo con grandes capacidades, o se puede separar de forma que un dispositivo de capacidades limitadas ejecute la parte física y la parte virtual puede estar desplegada en la nube o incluso en un servidor en una red cercana ("Edge/Fog computing").
- **Modularidad completa:** La pasarela es completamente modular, se pueden escoger numerosas extensiones e instalarlas de forma dinámica. De forma que no hace falta instalar todo el set de funcionalidades si no se van a utilizar, liberando espacio en memoria y evitando complejidades innecesarias.
- **Pasarela multi-propósito:** Existen módulos que permiten el despliegue de la pasarela virtual junto con un motor de reglas y una API REST para que no sea necesaria la conexión a una plataforma "middleware" IoT en despliegues sencillos. En despliegues más complejos o que requieran una plataforma IoT la pasarela es capaz de conectarse a ella y delegar la lógica.
- **Facilidad de extensión:** Crear extensiones para la pasarela es bastante sencillo tal y como se verá en la Sección 4.6.
- **Enfoque industrial y sanitario:** Puesto que la pasarela ha sido probada en dos pilotos muy complejos de estos dos entornos, tal y como veremos en el Capítulo 5.

Capítulo 3

Arquitectura

3.1. Introducción

La pasarela desarrollada en este estudio de interoperabilidad, se encuadra, tal y como se ha mencionado en el Capítulo 1, en el trabajo realizado durante el proyecto INTER-IoT. La complejidad del proyecto escapa al objetivo de esta tesis, puesto que el estudio de investigación planteado en esta tesis, se enfoca en uno de los componentes de dicho proyecto.

INTER-IoT presenta una novedosa solución de interoperabilidad orientada a capas [79], para proporcionar interoperabilidad en cualquier capa y a través de capas entre diferentes sistemas y plataformas de IoT [80]. A diferencia de un enfoque global más general, el enfoque por capas de INTER-IoT tiene un mayor potencial para proporcionar interoperabilidad [12]. Facilita una estrecha integración bidireccional, un mayor rendimiento, una completa modularidad, una gran adaptabilidad y flexibilidad, y presenta una mayor fiabilidad. Esta solución orientada a las capas se consigue mediante INTER-Layer [81], varias soluciones de interoperabilidad dedicadas a capas específicas. Cada capa de infraestructura de interoperabilidad tiene un fuerte acoplamiento con las capas adyacentes y proporciona una interfaz. Las interfaces serán controladas por un marco de metaniveles para proporcionar una interoperabilidad global. Se puede acceder a cada mecanismo de interoperabilidad a través de una API. Las capas de la infraestructura de interoperabilidad pueden comunicarse e interoperar a través de las interfaces. Esta estratificación cruzada permite lograr una integración más profunda y completa.

3.2. Visión general

La arquitectura más extendida para la organización y gestión de datos y procesos en el Internet de las Cosas se basa en un modelo jerarquizado en tres dominios: la abstracción de los datos, el procesado de los datos y los servicios de interconexión. Estos dominios se plasman en el modelo funcional de la arquitectura de referencia del Internet de las Cosas, tal y como podemos observar en la Figura 3.1 [82, 83].

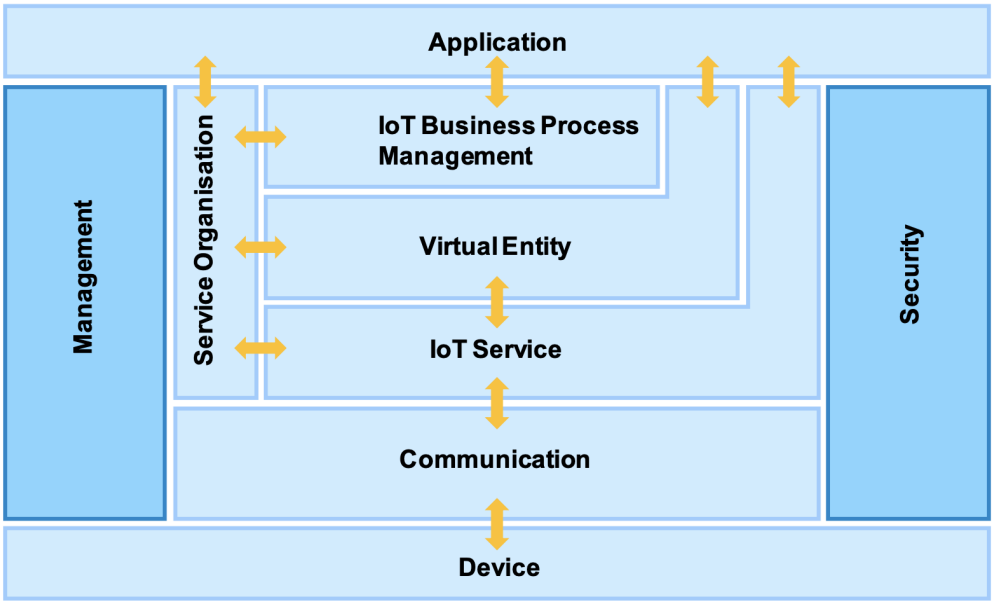

Figura 3.1: Modelo funcional de la arquitectura de IoT

- **Dominio de Dispositivos:** Generalmente compuesto por sensores, actuadores y pasarelas. En el modelo funcional está compuesto por las capas de dispositivo y comunicación.
- **Dominio de Servicios:** Compuesto por microservicios de agregación, procesado de datos y control de acceso a los datos. En el modelo funcional está compuesto por las capas de servicio y entidad virtual.
- **Dominio de Aplicación:** Compuesto por agentes y entidades externas a la propia red IoT y que solicitan el acceso para escritura/lectura/control de los datos. En el modelo funcional está compuesto por la capa de procesamiento y gestión de negocio y la capa de aplicación.

En la Tabla 3.1, se resumen las capacidades que tienen, generalmente, los diferentes elementos de Internet de las Cosas en función de su ámbito de actuación:

Dominio	**Nivel de abstracción de datos**	**Nivel de procesamiento de datos**	**Nivel de red**
Dispositivos	Bajo: datos en crudo, tipos de datos específicos o complejos.	Bajo: generación/consumo de datos y agregación.	Local
Servicios	Medio: identificadores esenciales, tipos de datos simples.	Alto: agregación, histórico, reglas, ejecutores ("hooks")	"Cloud"
Aplicación	Alto: tratamiento de conjuntos y estados globales, acceso limitado.	Variable	Externas

Tabla 3.1: Capacidades de los elementos de Internet de las Cosas en función de su dominio.

Un despliegue típico de un entorno de Internet de las Cosas, establece sus elementos de forma jerarquizada adecuándose a los tres dominios expuestos anteriormente de la siguiente manera (Figura 3.2):

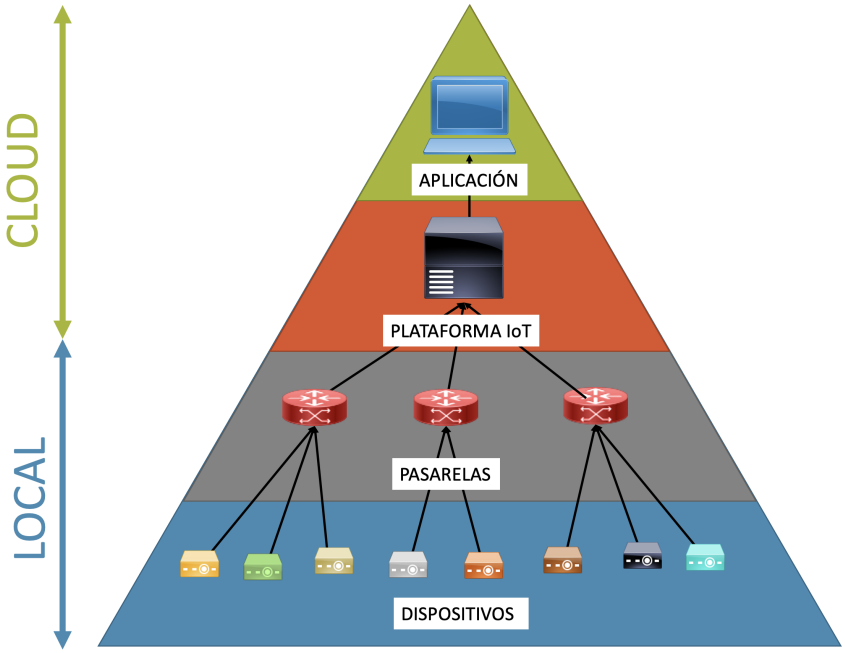

Figura 3.2: Despliegue tradicional jerárquico de un entorno IoT

En estos despliegues tradicionales, las pasarelas de Internet de las Cosas se limitan a la agregación de datos de los diferentes dispositivos y las plataformas IoT "middleware" limitan sus funciones a la organización de datos, gestión y ejecución de reglas y alarmas, conexión a servicios en redes externas, volcado de datos históricos, etc. y en general, los procesos que requieran una mayor computación.

Sin embargo, en los últimos años y gracias a la aparición de elementos de bajo coste y mayor poder de computación, ciertas funciones ligadas, típicamente, al ámbito de procesamiento, se han trasladado al ámbito de dispositivos. Estos elementos se sitúan en el "Edge" o "Fog" y pueden ofrecer funciones que requieren mayor complejidad tales como: tratamiento/pre-procesado de datos, reglas simples, acceso a los datos de ámbito local, etc.

Por tanto, con la aparición de estos elementos en el "Edge", se han flexibilizado los despliegues de entornos de Internet de las Cosas en cuanto a la distribución de sus elementos, pudiendo, por ejemplo, crear despliegues locales sencillos pero con funcionalidades avanzadas.

Dentro de la jerarquía expuesta en la figura Figura 3.2 y encuadrado en el proyecto de interoperabilidad INTER-IoT se identifica la necesidad de una pasarela de Internet de las Cosas flexible y modular, que pueda ser ejecutado

tanto en despliegues "tradicionales" (ofreciendo la capa de abstracción necesaria para las plataformas "Middleware") como en despliegues con funciones desplazadas al "Edge" y que sea fácilmente extensible para cubrir cualquier tipo de dispositivo y poder solventar los problemas de interoperabilidad entre dispositivos. El objetivo de esta tesis es la definición, desarrollo e implementación de una pasarela de Internet de las Cosas que cumpla con estos requisitos de manera modular y flexible.

3.2.1. Interoperabilidad en Internet de las Cosas

Esta pasarela se encuadra dentro de un proyecto cuyo objetivo es facilitar la interoperabilidad de los diferentes componentes que forman un entorno de Internet de las Cosas. De acuerdo al análisis previo de los ámbitos de actuación en el ecosistema de Internet de las Cosas, se han identificado los componentes de interoperabilidad en función de su ámbito de actuación. [16]

Al estar dichos ámbitos de actuación jerarquizados en cuanto a su nivel de abstracción al origen/destino de los datos procesados por los sensores y actuadores, podemos denominarlas "capas" de interoperabilidad.

Las capas de interoperabilidad, de menor a mayor nivel de abstracción al origen de los datos son (Figura 3.3):

- **Interoperabilidad entre dispositivos:** A nivel de dispositivos, la interoperabilidad a este nivel la inclusión de nuevos dispositivos IoT y su interoperabilidad con los ya existentes. [84, 85]
- **Interoperabilidad entre redes:** La interoperabilidad entre redes permite una movilidad transparente de los objetos inteligentes y el apoyo al enrutamiento de la información. También impide la sobrecarga y permite la itinerancia, lo que implica la interconexión de pasarelas y plataformas a través de la red. [86]
- **Interoperabilidad entre plataformas IoT:** A nivel de middleware, la interoperabilidad permite el descubrimiento y gestión de recursos para los dispositivos IoT en plataformas IoT heterogéneas. [87]
- **Interoperabilidad entre servicios:** La interoperabilidad de servicios heterogéneos entre diferentes plataformas de IoT permite descubrir, catalogar, utilizar e incluso componer servicios de diferentes plataformas. [88]

- **Interoperabilidad semántica:** A nivel semántico, una interpretación común de los datos y la información entre diferentes plataformas IoT y fuentes de datos heterogéneas que suelen emplear diferentes formatos de datos y ontologías, y que no pueden compartir información directamente entre ellas. [89, 90]

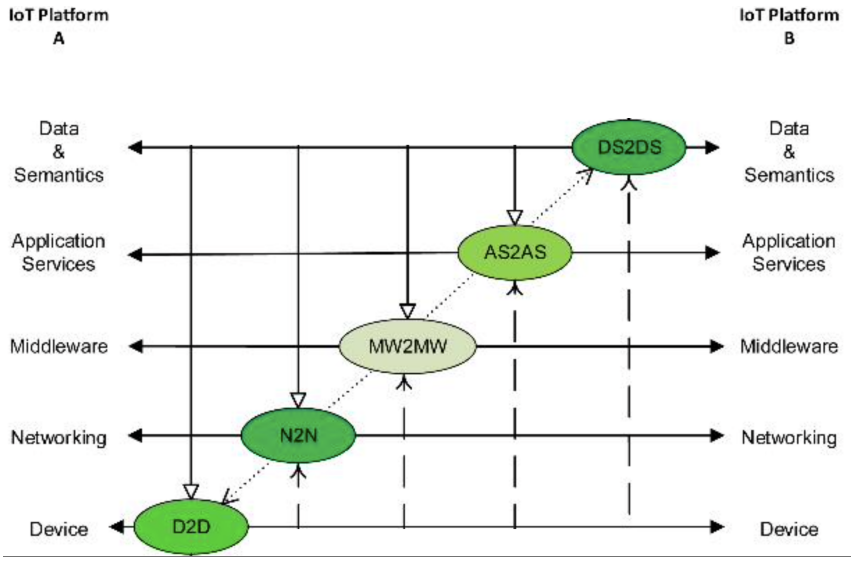

Figura 3.3: Capas de interoperabilidad en IoT

El objeto de esta tesis, la creación de una pasarela de Internet de las Cosas para la interoperabilidad entre dispositivos, se centra, según la definición de las capas de interoperabilidad expuesta anteriormente, en la capa más baja de interoperabilidad.

A su vez, además de ofrecer la interoperabilidad entre dispositivos, también ha de ofrecer el acceso a los dispositivos, con la suficiente abstracción, a las capas superiores. Esta abstracción se cumple con un modelo de datos común e independiente a los dispositivos, que pueden ser heterogéneos. No se realizará, por tanto, ningún tipo de operación semántica sobre los datos, puesto que escapa de las funciones de una pasarela de Internet de las Cosas (y al objeto de esta tesis).

3.3. Requisitos

La primera fase del estudio empezó con la captura de requisitos. La captura de requisitos siguió la metodología *Volere* [91] que puede ser resumida de la siguiente manera:

1. Definición del propósito del proyecto.
2. Identificación y análisis de los "Stakeholders" (partes interesadas).
3. Definición de los casos de uso de negocio.
4. Definición de los escenarios.
5. Captura de los requisitos: *funcionales* y *no-funcionales*.
6. Validación de los requisitos: relevancia, testabilidad, coherencia y trazabilidad entre otros.
7. Coordinación y diseminación de los requisitos entre las diferentes partes del proyecto.
8. Valoración del grado de completitud de cada requisito.

Es importante entender, que esta metodología de captura y análisis de los requisitos es un proceso iterativo que se desarrolla de manera continua durante las primeras fases del proyecto.

Los requisitos se engloban en dos grupos (*funcionales* y *no-funcionales*) y se les asigna un grado de prioridad. Los requisitos *funcionales* son aquellos que definen un aspecto fundamental del producto (por ejemplo, una acción que el producto ha de realizar) y los requisitos *no-funcionales* definen las cualidades y el comportamiento que el producto debe tener en términos de usabilidad, apariencia, "performance", seguridad, etc.

Existe cierto grado de libertad a la hora de utilizar un sistema de prioridades dentro de la metodología *Volere*, para el desarrollo de la pasarela, se utilizó la técnica *MoSCoW* [92, 93, 94] (derivado del acrónimo en inglés de "Must", "Should", "Could" y "Won't") y que define 4 categorías de prioridad en los requisitos:

- **Necesario** ("Must"): El requisito ha de ser cumplido, y de no ser así el proyecto se considera fracasado

- **Aconsejable** ("Should"): El requisito es crítico para la realización correcta del proyecto
- **Posible** ("Could"): El requisito es conveniente, pero no necesario, si el tiempo y los recursos lo permiten debe ser cumplido
- **No aconsejable** ("Won't"): El requisito no es necesario o no es adecuado para la fase actual. Puede ser reconsiderado en futuras iteraciones

En las siguientes subsecciones, se especifican los requisitos necesarios que definen las propiedades que ha de tener la pasarela. Estos requisitos han sido revisados durante el ciclo de desarrollo de la pasarela, y han sido refinados según las necesidades que surgían por las partes interesadas: los usuarios y despliegues en los pilotos definidos en el Capítulo 5 y en el Capítulo 6 [94, 95, 96, 97].

3.3.1. Requisitos no-funcionales

Direccionamiento y alcance

La pasarela debe tener una dirección unívoca y debe poder ser alcanzable por otros dispositivos dentro de la misma red o desde redes externas.

- **Criterio de aceptación:** La pasarela está identificada de forma unívoca en la red, con una dirección o nombre en la red conocidos. Se puede establecer conexión y comunicación a través de un protocolo de red desde otro dispositivo en la red.
- **Prioridad:** Necesario.

Soporte de datos en tiempo real

La pasarela debe soportar la transmisión y recepción de datos de sensores y actuadores en tiempo real.

- **Criterio de aceptación:** La transferencia de datos de sensores y actuadores en tiempo real ha de realizarse bajo un retardo inferior al umbral especificado por el caso de uso en el cual se despliegue la pasarela.
- **Prioridad:** Necesario.

Restricciones y limitaciones de la comunicación

INTER-Layer debe cumplir las normas de comunicación. La comunicación debe respetar las restricciones y limitaciones del protocolo, por ejemplo, si se utiliza un protocolo de comunicación como LoRa, la pasarela no debe forzar la comunicación sobre la línea.

- **Criterio de aceptación:** Utiliza protocolos, transmisiones y/o transceptores. Implementa todas las restricciones descritas en la especificación oficial de los protocolos, y, en su caso, las cuestiones de legislación y derecho de estos.
- **Prioridad:** Necesario

Soporte de las principales plataformas del Internet de las cosas

INTER-Layer debe ser compatible con las plataformas de IoT existentes. INTER-Layer requiere conectores a diferentes plataformas IoT (Fiware, OpenIoT, OM2M, Sofia2...) para acceder a sus servicios como descubrimiento, acceso, asignación de tareas, localización, etc.

- **Criterio de aceptación:** La plataforma debe garantizar la conexión con Fiware, OM2M y WSO2.
- **Prioridad:** Necesario

Virtualización de objetos/dispositivos

INTER-Layer debe virtualizar los objetos. Las plataformas IoT utilizan objetos virtuales de sus entidades físicas para gestionar los datos de diferentes fuentes. Para facilitar los datos de los sensores a las otras capas, la pasarela debe almacenar una imagen virtual para cada objeto/dispositivo que tiene que reflejar el valor en tiempo real de cada sensor de ese objeto/dispositivo. De esta manera, se pueden coordinar múltiples peticiones y no hay sobrecarga en la red de acceso de ese sensor. La representación virtual también debe manejar la interacción con los actuadores de cada sensor.

- **Criterio de aceptación:** Cada objeto/dispositivo debe tener una representación uno a uno de cada sensor que debe ser expuesto. Esa representación virtual debe ser lo más real posible. Los actuadores pueden ser controlados desde esa representación virtual.

- **Prioridad:** Necesario

Escalabilidad. Diseño

INTER-Layer debe ser escalable. La escalabilidad está relacionada con la capacidad de los sistemas para atender sin problemas una mayor demanda de recursos informáticos de datos, dispositivos, personas y aplicaciones. El sistema debe estar diseñado para ser escalable.

- **Criterio de aceptación:** La escalabilidad se obtiene normalmente a través de un enfoque de escalabilidad y utilizando servicios en la nube, esto se dirige principalmente a las capas superiores de INTER-Layer. INTER-IoT debería, al menos, introducir los enfoques de escalabilidad actualmente disponibles en los servicios en la nube (por ejemplo, Amazon, Azure).
- **Prioridad:** Aconsejable

Apoyo a las comunicaciones oportunistas para evitar la pérdida de datos

INTER-Layer deberá soportar comunicaciones oportunistas. El sistema deberá ser capaz de soportar comunicaciones oportunistas para garantizar la disponibilidad de los datos. Cuando la conectividad a Internet no esté disponible (por ejemplo, debido a la movilidad, las interferencias, etc.), las tecnologías de comunicación oportunistas deberán ser capaces de evitar la pérdida de datos.

- **Criterio de aceptación:** Los dispositivos multimodo, cuando son aplicables, se utilizan para construir redes ad-hoc y así preservar la conectividad o se utiliza algún servicio de almacenamiento temporal (cuando es aplicable) para retener los datos que luego se envían automáticamente al sistema cuando la comunicación de red está disponible de nuevo.
- **Prioridad:** Aconsejable

Extensibilidad

INTER-Layer debe ser extensible. Hay que tener en cuenta la extensibilidad de todos los componentes del sistema, desde el suministro de plataformas de

hardware para integrar múltiples sensores hasta el software del middleware, pasando por las infraestructuras de los bancos de pruebas. El middleware M2M debe ser capaz de recibir los datos de múltiples tipos de sensores: físicos o emulados.

- **Criterio de aceptación:** INTER-Layer (e INTER-FW) deberían ser capaces de soportar fácilmente las extensiones, las actualizaciones y la inclusión de nuevos módulos a medida que se van integrando. Además, a medida que los SDO y los protocolos soportados evolucionan, este hecho debería reflejarse en una forma fácil de ampliar INTER-Layer e INTER-FW.
- **Prioridad:** Aconsejable

Deben admitirse los protocolos comunes de comunicación del IoT

INTER-Layer debe soportar los protocolos de comunicación de IoT. La pasarela IoT debe ser capaz de utilizar los protocolos de comunicación más comunes para IoT.

- **Criterio de aceptación:** Se puede utilizar cualquier protocolo de comunicación. Los protocolos de comunicación más utilizados en IoT, en diferentes capas como: BLE, IEEE 802.15.5, IEEE 802.11 en físico, IPv6 y OpenFlow en red, o MQTT y CoAP en middleware deben ser soportados por la solución de interoperabilidad. La capa intermedia debe implementar estos protocolos e intercambiar con éxito la información entre los sistemas implicados.
- **Prioridad:** Aconsejable

Soporte de interconexión

INTER-Layer debe soportar las comunicaciones con otros sistemas. Los sensores, los datos, las redes y las plataformas de otras fuentes deben poder acoplarse a las aplicaciones de middleware para ampliar el análisis o utilizar algoritmos avanzados. Estos sensores y dispositivos pueden funcionar a través de diferentes middleware.

- **Criterio de aceptación:** Los dispositivos, las redes y las plataformas de IoT tienen que estar interconectadas mediante soluciones de INTER-IoT. Las nuevas plataformas deben ser automáticamente añadidas y aceptadas.
- **Prioridad:** Aconsejable

Soporte de red dinámico

INTER-Layer debe soportar una red dinámica. Debe permitirse un cambio continuo de redes y dispositivos. Especialmente las redes de sensores pueden ser muy dinámicas por naturaleza. Nuevos sensores pueden entrar en línea, mientras que otros mueren. Los sensores pueden estar fuera de línea o en hibernación durante largos períodos de tiempo. INTER-IoT debe ser capaz de gestionar estos cambios constantes en la red. Las redes inalámbricas, como una red Zigbee con múltiples dispositivos sencillos, deben poder conectarse a través de la pasarela/interruptor/hub que contiene la inteligencia.

- **Criterio de aceptación:** Debe ser posible realizar cambios rápidos y dinámicos en la red. Es posible ampliar y reducir los dispositivos y las redes LAN, y las redes completas deben poder conectarse al sistema IoT.
- **Prioridad:** Aconsejable

Salida en tiempo real

INTER-Layer debe tener salida en tiempo real. Para que el sistema funcione en tiempo real, se permite un pequeño retraso. Lo ideal es que el retraso no sea perceptible.

- **Criterio de aceptación:** Los retrasos en tiempo real no deben interferir en el buen funcionamiento del sistema (menos de 5 segundos).
- **Prioridad:** Aconsejable

Descubrimiento de servicios IoT

INTER-Layer debe tener capacidad de descubrimiento de los servicios IoT. Los servicios IoT suelen estar disponibles sin intervención humana. Sin embargo, esto no significa que los humanos (usuarios de los servicios IoT) no

necesiten conocer la existencia de los servicios IoT que rodean a los usuarios. Cuando los servicios IoT se ponen a disposición de un usuario, se recomienda que este pueda darse cuenta de la presencia de los servicios IoT y hacerlo de forma coherente con la normativa pertinente. Debe ponerse a disposición del usuario una colección de servicios disponibles para que pueda navegar y buscar.

- **Criterio de aceptación:** Los diferentes servicios, puestos a disposición de los pilotos, podrán ser descubiertos a través de la plataforma, y los pilotos deberán hacer uso de las funciones de descubrimiento para conectar los servicios con los datos.
- **Prioridad:** Aconsejable

Prioridad de enrutamiento y procesamiento de mensajes críticos sobre datos de sensores de baja prioridad

INTER-Layer debe priorizar el enrutamiento y el procesamiento de los mensajes críticos. Los dispositivos u objetos inteligentes son semiautónomos, tienen que enviar mucha información a los servidores de Big Data, pero solo reciben unas pocas órdenes. Es muy importante dar prioridad y seguridad a las órdenes. También, por ejemplo, en INTER-Health cualquier información que pueda desencadenar el deterioro del estado de salud debe transmitirse con prioridad de emergencia. La capacidad de alarma debe ser de varios niveles, ya que pueden darse múltiples situaciones de emergencia. La alarma debe ser activada por el dispositivo de monitorización a partir de una lista de situaciones de emergencia predeterminadas. La alarma debe restablecerse manualmente para garantizar un control humano de la situación. El sistema debe permitir que se dé prioridad al tratamiento y la transmisión de datos de alta prioridad, como los relativos a cuestiones delicadas, alarmas, órdenes, etc.

- **Criterio de aceptación:** Definir situaciones de enrutamiento prioritario y habilitar el enrutamiento prioritario para la información relacionada con esas situaciones. Deben preverse al menos dos niveles de prioridad. El nivel más alto corresponde a las alarmas, órdenes, etc. y requiere seguridad y confirmación del mensaje. El resto podría ser sin confirmación (por lo que se podría utilizar UDP).
- **Prioridad:** Aconsejable

Virtualización de la pasarela

INTER-Layer debería virtualizar parte de la pasarela. Una pasarela IoT puede dividirse en dos partes, una que permita una red de acceso diferente para el objeto/dispositivo (parte física); y las funciones y servicios propios de la pasarela que pueden ser totalmente virtualizados (parte virtual).

- **Criterio de aceptación:** La conexión por el dispositivo a través de la red de acceso situada en la parte física y el acceso por la plataforma a los servicios de la pasarela por la virtual.
- **Prioridad:** Aconsejable

Seguimiento y autoconocimiento del sistema

INTER-Layer podría tener autoconciencia del sistema. El sistema debe recoger pruebas de sus componentes para comprobar que realmente están funcionando.

- **Criterio de aceptación:** Un sistema IoT debe tener autoconciencia de sus elementos. Los sistemas necesitan información sobre el estado y el rendimiento de sus elementos. INTER-Layer necesita garantizar la fiabilidad entre sus componentes.
- **Prioridad:** Posible

Comunicación con protocolos eficientes en cuanto al tamaño de los mensajes

INTER-Layer podría tener protocolos eficientes para las comunicaciones. La comunicación debe realizarse utilizando protocolos que sean eficientes en términos de cantidad de información intercambiada sobre la cantidad de datos intercambiados medidos en bytes.

- **Criterio de aceptación:** Selección de protocolos de comunicación comúnmente aceptables, transmisión de datos eficiente.
- **Prioridad:** Posible

3.3.2. Requisitos funcionales

API de acceso a la pasarela

INTER-Layer debe proporcionar una API para acceder a la pasarela. La API es obligatoria para recuperar datos de objetos virtuales/dispositivos, control de actuadores, etc. desde otra capa.

- **Criterio de aceptación:** Todas las funciones expuestas de la pasarela son accesibles desde la API.
- **Prioridad:** Necesario.

Itinerancia entre redes

INTER-Layer debe soportar la itinerancia entre redes. Los dispositivos y el IoT deben ser resistentes a la pérdida de señal y ser capaces de reconectarse cuando se restablezca la cobertura. El sistema debe ser capaz de reconocer el dispositivo de nuevo, los volcados de datos deben ser soportados. Un objeto cambia de ubicación haciendo un cambio en la plataforma que está conectada. El cambio es automático, desatendido y transparente para el usuario. Algunos estándares de comunicación se basan en la comunicación unidireccional, por lo que deben soportarse ambos principios de comunicación.

- **Criterio de aceptación:** El dispositivo puede viajar de una red de acceso a otra sin perder las conexiones. El dispositivo debe ser reconocido de nuevo y se le permite hacer un volcado de datos de registro. El cambio automático a través de plataformas y cualquier estándar de comunicación puede ser utilizado.
- **Prioridad:** Aconsejable.

Capacidades de la pasarela

La pasarela debe soportar la interoperabilidad de múltiples tecnologías. Soporte de múltiples interfaces: En la capa de dispositivo, las capacidades de la pasarela admiten dispositivos conectados a través de diferentes tipos de tecnologías alámbricas o inalámbricas, como un bus de red de área de controlador (CAN), ZigBee, Bluetooth o Wi-Fi. En la capa de red, las capacidades de la

pasarela pueden comunicarse a través de diversas tecnologías, como la red telefónica pública conmutada (RTPC), las redes de segunda o tercera generación (2G o 3G), las redes de evolución a largo plazo (LTE), Ethernet o las líneas de abonado digital (DSL). Conversión de protocolos: Hay dos situaciones en las que se necesitan capacidades de pasarela. Una situación es cuando las comunicaciones en la capa de dispositivo utilizan protocolos de capa de dispositivo diferentes, por ejemplo, protocolos de tecnología ZigBee y protocolos de tecnología Bluetooth, y la otra es cuando las comunicaciones que implican tanto la capa de dispositivo como la capa de red utilizan protocolos diferentes, por ejemplo, un protocolo de tecnología ZigBee en la capa de dispositivo y un protocolo de tecnología 3G en la capa de red.

- **Criterio de aceptación:** La capa de red debe demostrar las capacidades de interconexión entre diferentes tecnologías con los pilotos.
- **Prioridad:** Aconsejable

Gestionar un sensor o actuador

INTER-Layer debe ser capaz de gestionar los actuadores. Además de recibir información de sensores y actuadores, es necesario poder enviar cambios de configuración o acciones específicas.

- **Criterio de aceptación:** Desarrollo de un método para enviar una acción a un actuador específico.
- **Prioridad:** Aconsejable

Control de dispositivos a distancia

INTER-Layer podría ser capaz de controlar los dispositivos de forma remota. Las apps de los fabricantes deben ser compatibles y permitir tomar el control de sus dispositivos.

- **Criterio de aceptación:** Una aplicación del fabricante sigue siendo funcional una vez que el sistema está conectado al IoT. Los dispositivos compatibles deben poder conectarse y controlarse juntos.
- **Prioridad:** Posible

3.4. Arquitectura de una pasarela modular

Según los requisitos analizados en la sección 3.3 y en respuesta a la necesidad de crear una pasarela flexible que permita la ejecución de funciones desplazadas al "Edge", se ha diseñado una pasarela separada en dos partes: la parte "física" y la parte "virtual". La parte física se encarga de la conexión a las diferentes redes de acceso de los sensores/actuadores, y la agregación de los datos. La parte virtual ejecutará de manera opcional las funciones desplazadas al "Edge" y/o la conexión a plataformas IoT "Middleware".

El diseño de la pasarela ha de permitir que pueda ser ejecutado en dos entornos diferentes:

- **Despliegues tradicionales:** Tanto la parte física como la parte virtual se ejecutan en el mismo dispositivo, las funciones se limitan a la agregación de datos e interconexión con plataformas "Middleware" de Internet de las Cosas.
- **Despliegues Edge:** La parte física se ejecuta en dispositivos con capacidad de procesamiento baja y hardware dedicado a la interconexión con diferentes redes de acceso y agregación de datos. La parte virtual se ejecuta en dispositivos con mayor capacidad, cercanas a la parte física (uno o dos saltos de red), ejecuta funciones desplazadas al "Edge" y opcionalmente la interconexión con plataformas "Middleware".

Por tanto, es inmediato deducir que en los despliegues tradicionales no es necesario un canal de comunicación entre la parte física y virtual, mientras que en los despliegues "Edge" la pasarela debe comunicar su parte física y su parte virtual a través de un canal de comunicación.

En la figura 3.4 se definen los bloques funcionales que componen la pasarela física-virtual desarrollada:

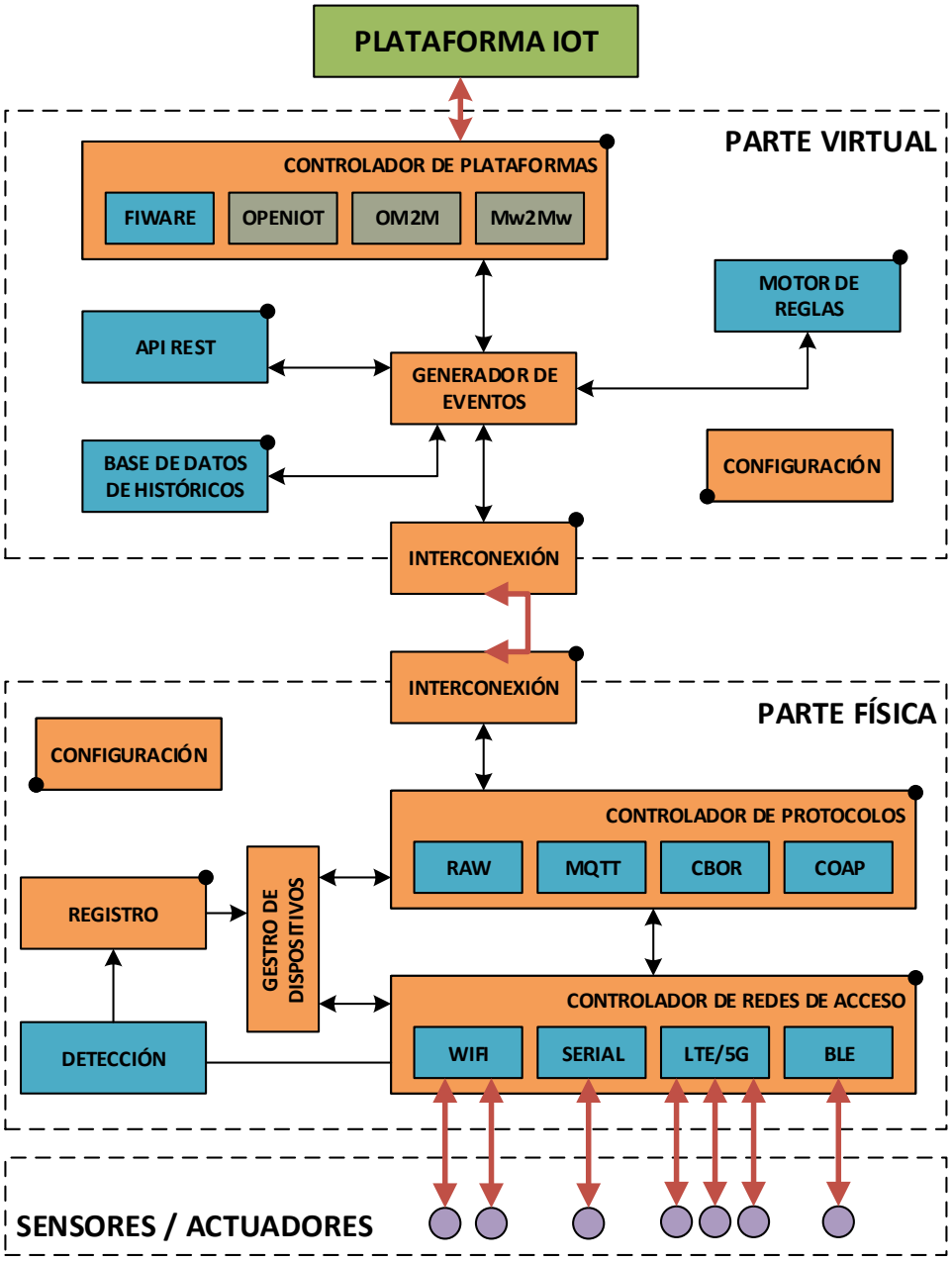

Figura 3.4: Arquitectura de bloques funcionales de la pasarela física y virtual

Existen dos tipos de módulos en la pasarela: los módulos *estáticos* (en naranja) y los módulos *dinámicos* (en azul). Los módulos estáticos son necesarios para el funcionamiento de la pasarela y se cargan una vez al empezar la ejecución de la pasarela. El fallo de inicio de cualquiera de estos módulos impide el inicio de la pasarela en su conjunto. Los módulos estáticos suelen tener

mayor interdependencia entre ellos y estas están marcadas por un sistema de versionado fijo.

Por el contrario, los módulos dinámicos son opcionales y los puntos principales de extensión de la pasarela. El fallo de alguno de estos módulos no impide la ejecución de la pasarela en su conjunto y deben permitir la desactivación en cualquier momento sin afectar la pasarela en su conjunto. Los módulos dinámicos suelen tener un campo de actuación y dependencia más limitados y están marcados por un versionado de rango compatible.

Los módulos dinámicos son los que ofrecen también las principales características únicas al diseño de esta pasarela de Internet de las Cosas, puesto que son los puntos de extensión que permiten múltiples redes de acceso, protocolos e interconexión con plataformas "Middleware" para facilitar la correcta interoperabilidad. También son módulos dinámicos los que soportan las funciones desplazadas al "Edge", al ser opcionales, pueden estar presentes solamente en despliegues de Internet de las Cosas dónde la pasarela virtual se encuentra en el "Fog" y hay suficiente capacidad de computación para ejecutar correctamente estos módulos.

3.4.1. Bloques funcionales comunes

Módulo de Configuración

- **Funcionalidades:** Este módulo ofrece una interfaz común al resto de módulos y no depende de ningún otro. Puede tener diferentes implementaciones dependiendo de la fuente de datos en la que se basa para leer la configuración. Es la única fuente de configuración y el resto de módulos han de utilizar este módulo para obtener los parámetros necesarios para su funcionamiento.
- **Tipo de módulo:** Estático.
- **Interrelación con otros bloques funcionales:** Dado que el módulo de configuración publica un servicio interno para la lectura/escritura de datos de configuración, cualquier módulo puede depender de este.

Módulo de interconexión

- **Funcionalidades:** Es el módulo que interconecta ambas pasarelas. Debe ofrecer una interfaz abstracta para el controlador de protocolos (en

la parte física) y el generador de eventos (en la parte virtual) para el envío/recepción de mensajes. Esta interfaz puede ser implementada dependiendo del formato de mensajes y/o el protocolo de red a utilizar. También es obligatorio, que ofrezca la posibilidad de enviar estos mensajes a través de un canal seguro.

- **Tipo de módulo:** Estático.
- **Interrelación con otros bloques funcionales:**
  - Configuración
  - Controlador de protocolos (parte física)
  - Generador de eventos (parte virtual)

3.4.2. Bloques funcionales de la parte física

Módulo de Registro

- **Funcionalidades:** Este componente es responsable de mantener un registro unívoco de los diferentes sensores y actuadores, sus propiedades (red de acceso, identificadores de acceso de red, estado, etc.) y sus metadatos asociados.
- **Tipo de módulo:** Estático.
- **Interrelación con otros módulos:**
  - Configuración
  - Gestor de dispositivos
  - Descubrimiento

Módulo Gestor de dispositivos

- **Funcionalidades:** Gestiona en memoria la asociación de cada dispositivo con su módulo de red de acceso, su módulo de protocolo, y la configuración específica de cada sensor y actuador por separado o su posible asociación a dispositivos agregadores.
- **Tipo de módulo:** Estático.
- **Interrelación con otros bloques funcionales:**

- Registro
- Controlador de redes de acceso
- Controlador de protocolo

Módulo Controlador de redes de acceso

- **Funcionalidades:** Este módulo se encarga de abstraer en una interfaz común para el resto de módulos, la red de acceso específica que utiliza cada sensor/actuador/dispositivo. Además, tiene como función arbitrar la ejecución y parada en cualquier momento de un módulo de red de acceso.
- **Tipo de módulo:** Estático.
- **Interrelación con otros bloques funcionales:**
  - Configuración
  - Controlador de protocolos
  - Módulo(s) de red de acceso

Módulo de red de acceso

- **Funcionalidades:** Son módulos que controlan de forma específica una red de acceso (lectura/escritura en puertos, llamadas a subrutinas del Sistema Operativo, control de tarjetas de red externas, etc.). Tienen una dependencia directa con el Hardware y el Sistema Operativo del dispositivo donde se está ejecutando la parte física de la pasarela (incluso puede haber diferentes versiones de un mismo módulo para diferentes arquitecturas de computadores).
- **Tipo de módulo:** Dinámico.
- **Interrelación con otros bloques funcionales:**
  - Configuración
  - Controlador de redes de acceso

Módulo Controlador de protocolos

- **Funcionalidades:** Al igual que el controlador de redes de acceso, este módulo se encarga de abstraer en una interfaz común para el resto de módulos, independientemente del módulo de protocolo que se encargue de la traducción de cada mensaje. Los mensajes traducidos serán delegados al módulo de interconexión para su transmisión a la pasarela virtual o al controlador de red de acceso para su transmisión a los dispositivos.
- **Tipo de módulo:** Estático.
- **Interrelación con otros bloques funcionales:**
  - Configuración
  - Controlador de redes de acceso
  - Módulo(s) de protocolo
  - Módulo de interconexión

Módulo de protocolo

- **Funcionalidades:** Estos módulos se encargan de la traducción de un formato específico de mensaje a una representación genérica de los datos y viceversa.
- **Tipo de módulo:** Dinámico.
- **Interrelación con otros bloques funcionales:**
  - Configuración
  - Controlador de protocolos

3.4.3. Bloques funcionales de la parte virtual

Módulo de generación de eventos

- **Funcionalidades:** Este módulo es la pieza central en la pasarela virtual. Los mensajes recibidos por el módulo de interconexión se procesan y se publicarán los eventos correspondientes. De igual forma, cualquier instrucción recibida por el controlador de plataformas se procesará a su evento correspondiente. Se utiliza un método "PubSub", de forma

que los eventos pertenecerán a un "topic" y el resto de módulos pueden subscribirse para recibir eventos de ese "topic".

- **Tipo de módulo:** Estático.
- **Interrelación con otros bloques funcionales:**
  - Configuración
  - Controlador de plataformas
  - Cualquier otro módulo dinámico que escuche eventos

Motor de reglas

- **Funcionalidades:** Es un módulo opcional para dotar de lógica a la pasarela virtual. Ha de subscribirse a todos los eventos provenientes de los sensores y aplicar reglas complejas con base en una agregación de los últimos eventos recibidos (en esencia, debe ser un CEP); estas reglas pueden a su vez, generar un mensaje para enviar a los actuadores a través del módulo de interconexión, o enviar los datos procesados a la plataforma IoT a través del controlador de plataformas. Es por tanto, un módulo que requiere que la pasarela virtual esté desplegada en el "Edge" puesto que requiere bastantes recursos computacionales.
- **Tipo de módulo:** Dinámico.
- **Interrelación con otros bloques funcionales:**
  - Configuración
  - Generador de eventos

API REST

- **Funcionalidades:** Este módulo opcional debe ofrecer una capa de acceso a los datos y al control de la pasarela a través de una interfaz REST. También ofrecerá a otros módulos la posibilidad de extender el API con "endpoints" específicos.
- **Tipo de módulo:** Dinámico.
- **Interrelación con otros bloques funcionales:**
  - Configuración
  - Generador de eventos

Base de datos

- **Funcionalidades:** Este módulo opcional ofrece la posibilidad de almacenar un histórico de datos de los sensores en una base de datos ya sea local o remota. Debe identificar cada medida de forma unívoca y ofrecer una interfaz de acceso a los datos al resto de módulos.
- **Tipo de módulo:** Dinámico.
- **Interrelación con otros bloques funcionales:**
  - Configuración
  - Generador de eventos

Controlador de plataformas

- **Funcionalidades:** Similar al controlador de redes de acceso y de protocolos en la pasarela física, este módulo abstrae en una interfaz común cualquier plataforma IoT independientemente del módulo específico que se ejecute. Solamente un módulo de plataforma puede estar activo a la vez, puesto que de lo contrario se rompería con la jerarquía y daría lugar a inconsistencias de datos entre las plataformas IoT.
- **Tipo de módulo:** Estático.
- **Interrelación con otros bloques funcionales:**
  - Configuración
  - Generador de eventos
  - Módulo de plataforma

Módulo de plataforma

- **Funcionalidades:** Estos módulos se encargan de establecer conexión y comunicación con una plataforma IoT específica y traducir de una representación genérica de los datos al formato de la plataforma IoT y viceversa.
- **Tipo de módulo:** Dinámico.
- **Interrelación con otros bloques funcionales:**

- Configuración
- Controlador de plataformas

3.5. Modelos de interacción

La pasarela puede ser desplegada con dos configuraciones posibles. En un despliegue IoT típico, la pasarela virtual tendrá activado el módulo de plataforma IoT y transmitirá los datos agregados a dicha plataforma; de igual manera, recibirá de la plataforma los datos a enviar a los actuadores. Pero para despliegues IoT donde no es necesario una plataforma IoT para coordinar y gestionar los datos de sensores y actuadores, se puede optar por no activar ningún módulo de plataforma IoT y seguir ofreciendo la posibilidad de interoperar dispositivo a dispositivo mediante los módulos de "Motor de Reglas" y "API".

A continuación veremos los ejemplos de interacción posibles y los niveles de red que atraviesan los datos en cada caso. Se utiliza como canal de comunicación entre la pasarela física y la virtual el protocolo "WebSocket" pero como veremos en el Capítulo 4, la implementación puede ser distinta.

3.5.1. Interacción Dispositivo-Plataforma

En este caso, el módulo de plataforma IoT específica estará activado y los datos agregados serán transmitidos a la plataforma para su posterior procesamiento. En la Figura 3.5 podemos ver un ejemplo de los niveles de red que atraviesan los datos en esta configuración.

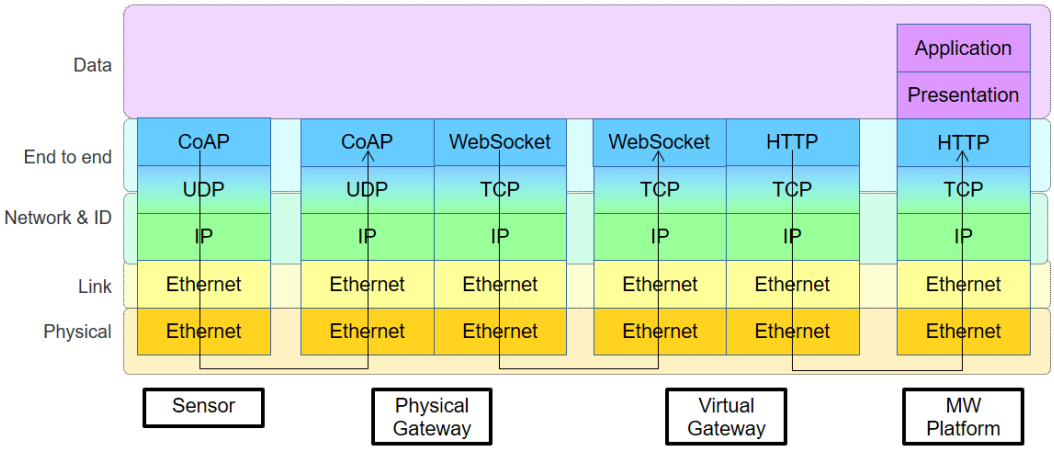

Figura 3.5: Niveles de red en la interacción dispositivo a plataforma

3.5.2. Interacción Plataforma-Dispositivo

En este caso también estará activo el módulo de plataforma IoT y los datos hacia la los actuadores son transmitidos por la plataforma a la pasarela virtual. En la Figura 3.5 podemos ver un ejemplo de los niveles de red que atraviesan los datos en esta configuración.

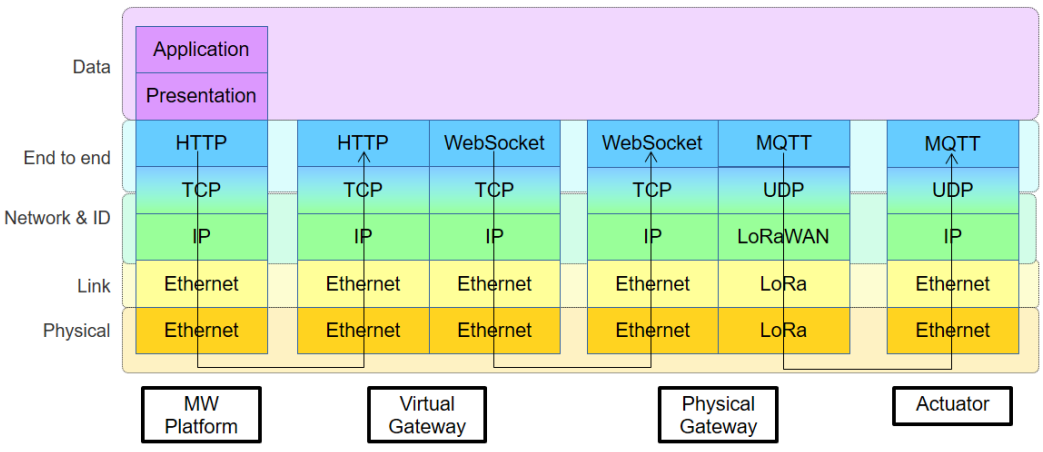

Figura 3.6: Niveles de red en la interacción plataforma a dispositivo

3.5.3. Interacción Dispositivo-Dispositivo

Si la pasarela se despliega sin estar activo ningún módulo de plataforma IoT, la única interacción posible para ofrecer la interoperabilidad entre dispositivos es a través del módulo de motor de reglas de la pasarela virtual o del módulo de API REST. En la Figura 3.7 podemos ver un ejemplo de los niveles de red que atraviesan los datos en esta configuración.

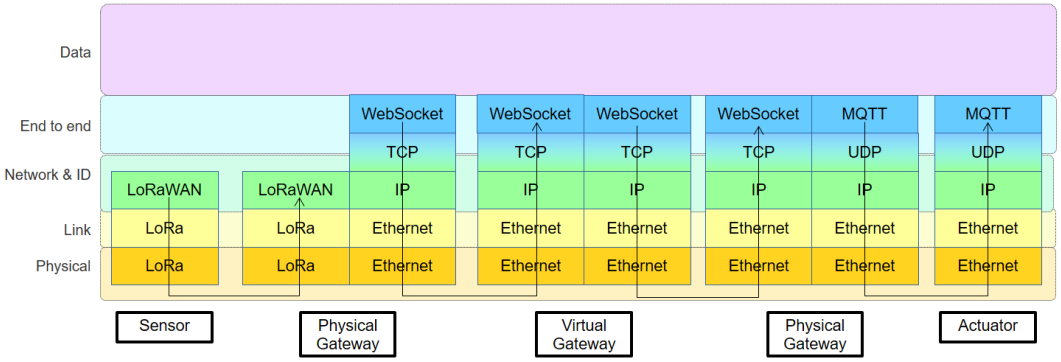

Figura 3.7: Niveles de red en la interacción dispositivo a dispositivo

3.6. Modelo de datos

La pasarela debe implementar un modelo de datos consistente y lo suficientemente genérico para que pueda soportar cualquier tipo de dispositivo y plataforma IoT. En esta sección se describirán los modelos de datos de que describen los elementos clave de la pasarela física y virtual.

Los tipos de atributos pueden ser:

- `string`: una cadena de caracteres.
- `enum <valores...>`: un único valor posible de un conjunto finito de posibilidades.
- `float`: un número decimal.
- `int`: un número entero.
- `byte`: un byte.

- `<type>[]`: cualquiera de los tipos anteriores pero siendo un conjunto.
- `[<type>:<type>]`: cualquiera de los tipos anteriores pero siendo un diccionario de clave-valor.

Pasarela (*Gateway*)

Atributo	Tipo	Ejemplo
uuid	string	73f18ffe-6497-4533-9fe0-57a85448f4e6
extensions	string[]	[api, rules-engine]
version	string	1.0.4
specVersion	string	1.0.4
build	string	1544371823486
type	enum <PHYSICAL|VIRTUAL>	PHYSICAL
vendor	string	INTER-IoT
specVendor	string	INTER-IoT

Tabla 3.2: Modelo de datos: Descripción de la pasarela

Dispositivo (*Device*)

Atributo	Tipo	Ejemplo
id	string	TH001
type	string	temperature-humidity-pressure
description	string	BME280
deviceIOs	[string:DeviceIO]	temp:...,hum:...,pres:...
controller	string	arduino
config	[string:string]	outputPin:03

Tabla 3.3: Modelo de datos: Descripción del dispositivo

Interfaz de Dispositivo (*DeviceIO*)

Atributo	Tipo	Ejemplo
`type`	`enum <SENSOR|ACTUATOR>`	`SENSOR`
`attribute`	`Attribute`	`...`
`config`	`[string:string]`	`unit:celsius`

Tabla 3.4: Modelo de datos: Descripción de una interfaz del dispositivo

Atributo (*Attribute*)

Atributo	Tipo	Ejemplo
`name`	`string`	`temperature`
`type`	`enum <INTEGER|FLOAT|STRING|BOOLEAN>`	`FLOAT`

Tabla 3.5: Modelo de datos: Descripción de un atributo

Medida (*Measurement*)

Atributo	Tipo	Ejemplo
`timestamp`	`int`	`1503583064000`
`data`	`MeasurementData[]`	`...`

Tabla 3.6: Modelo de datos: Descripción de una medida

Dato de medida (*MeasurementData*)

Atributo	Tipo	Ejemplo
`attribute`	`Attribute`	`...`
`value`	`byte[]`	`0x41bb3333`

Tabla 3.7: Modelo de datos: Descripción de un dato de una medida

Acción (*Action*)

Atributo	Tipo	Ejemplo
`timestamp`	`int`	`1503583064000`
`data`	`ActionData[]`	`...`

Tabla 3.8: Modelo de datos: Descripción de una acción

Dato de acción (*ActionData*)

Atributo	Tipo	Ejemplo
`attribute`	`Attribute`	`...`
`value`	`byte[]`	`0x01`

Tabla 3.9: Modelo de datos: Descripción de un dato de una acción

Capítulo 4

Implementación

4.1. Introducción

La pasarela IoT ha sido desarrollada con una licencia de código abierto "Apache 2.0", utilizando un lenguaje de programación y librerías de código abierto también.

El lenguaje de programación utilizado para el desarrollo ha sido "Java" en su versión 8.0[1] pudiendo también ser compilado en perfiles "Compact 2", "Compact 3". Estos perfiles permiten ejecutar la pasarela en más reducidas, especialmente interesante para dispositivos con capacidades más limitadas.

Tal y como hemos especificado en la arquitectura, la pasarela está dividida en dos partes: la física (que se ejecutará en un dispositivo físico), y la virtual (que se ejecutará en el "Fog"/"Edge" o en la nube).

Según también la arquitectura, la pasarela es completamente modular, por lo que la diferencia entre la parte física y la parte virtual son los módulos base que se ejecutan, sin embargo, el "Framework" (o marco) de ejecución es común.

En las siguientes secciones detallaremos en qué consiste este "Framework" común de ejecución y la implementación de los diferentes módulos específicos de cada parte de la pasarela.

[1] https://jdk.java.net/java-se-ri/8-MR3

4.2. Framework de ejecución común

El marco de ejecución común es el punto de entrada de la pasarela, tanto en la parte física como en la virtual. Después de realizar una serie de comprobaciones (argumentos de ejecución, archivos de configuración y lectura inicial de estado) cede la ejecución al controlador OSGI. Para la implementación propuesta se ha utilizado "Eclipse Concierge"[2] que está optimizado para dispositivos de capacidades limitadas. Sin embargo, se puede utilizar cualquier otra implementación OSGI compatible, como puede ser "Apache Felix" [3] o "Eclipse Equinox" [4].

El hilo principal de ejecución es el encargado de iniciar el "framework" OSGI, cargar la configuración y los módulos principales, extensiones y librerías; para finalmente delegar la ejecución al "runtime" específico (físico o virtual dependiendo del caso). En la Figura 4.1 se esquematiza la lógica de ejecución de este hilo principal.

[2] https://www.eclipse.org/concierge/
[3] https://felix.apache.org/documentation/index.html
[4] https://www.eclipse.org/equinox/

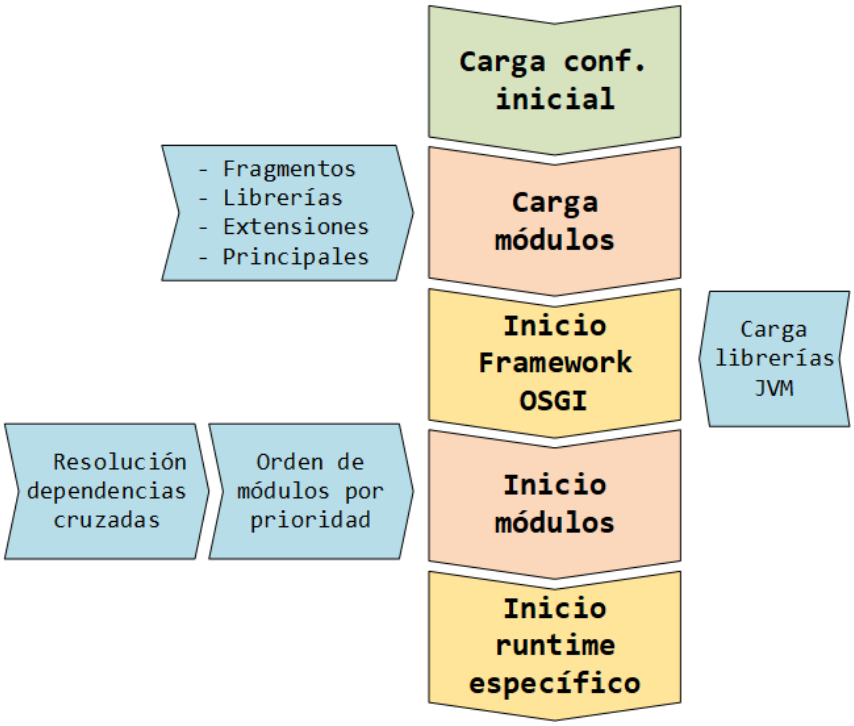

Figura 4.1: Lógica de ejecución del hilo principal

4.3. Implementación de la pasarela física

Tras la ejecución del hilo principal expuesta en la Sección 4.2 se delega la ejecución a la clase principal de la pasarela física. Esta ejecuta, por orden, las siguientes acciones:

- Lee los valores de configuración relevantes (Sección B.1 del Anexo B).
- Descubre los módulos de extensión relevantes para la ejecución.
- Lee la configuración de los dispositivos, los registra e inicia los hilos del gestor de dispositivos que escuchan a los dispositivos activos.
- Inicia el hilo de ejecución del módulo del conector para establecer conexión. Si no puede, reintenta la conexión de manera incremental en base a los parámetros establecidos en la configuración. Tras establecer la conexión, envía la información de la pasarela y de los dispositivos presentes a la pasarela virtual a través del conector (Sección B.2 del Anexo B).

- Inicia los hilos de las extensiones que necesiten una ejecución en paralelo (como la extensión de interfaz de consola).

En la figura Figura 4.2 se muestra un esquema de la ejecución de los módulos tras la finalización de ejecución del "framework" explicada en la Sección 4.2.

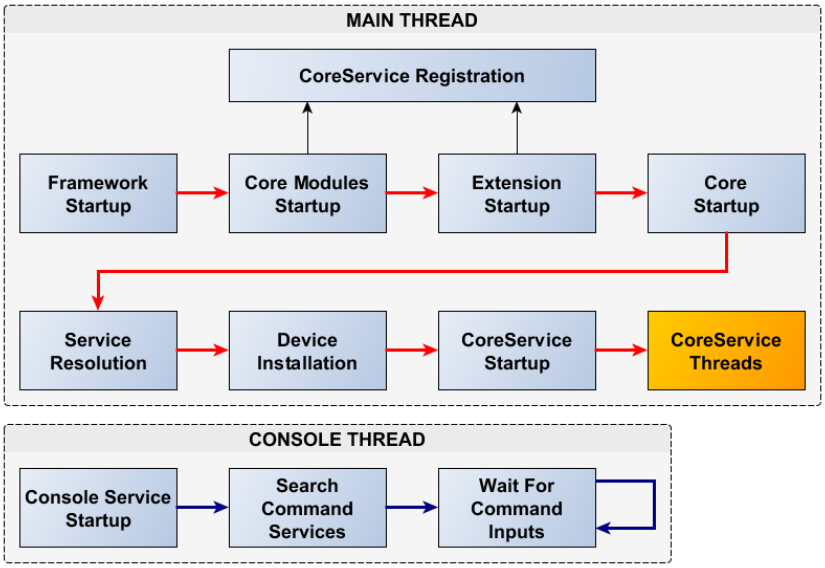

Figura 4.2: Lógica de ejecución de los hilos en la pasarela física

Para implementar la pasarela física, junto con los módulos principales, módulos de extensión y el "framework" OSGI, se utilizan también dependencias de librerías de terceros. En la Figura 4.3 se puede ver un esquema de los módulos y las librerías utilizadas en la pasarela física.

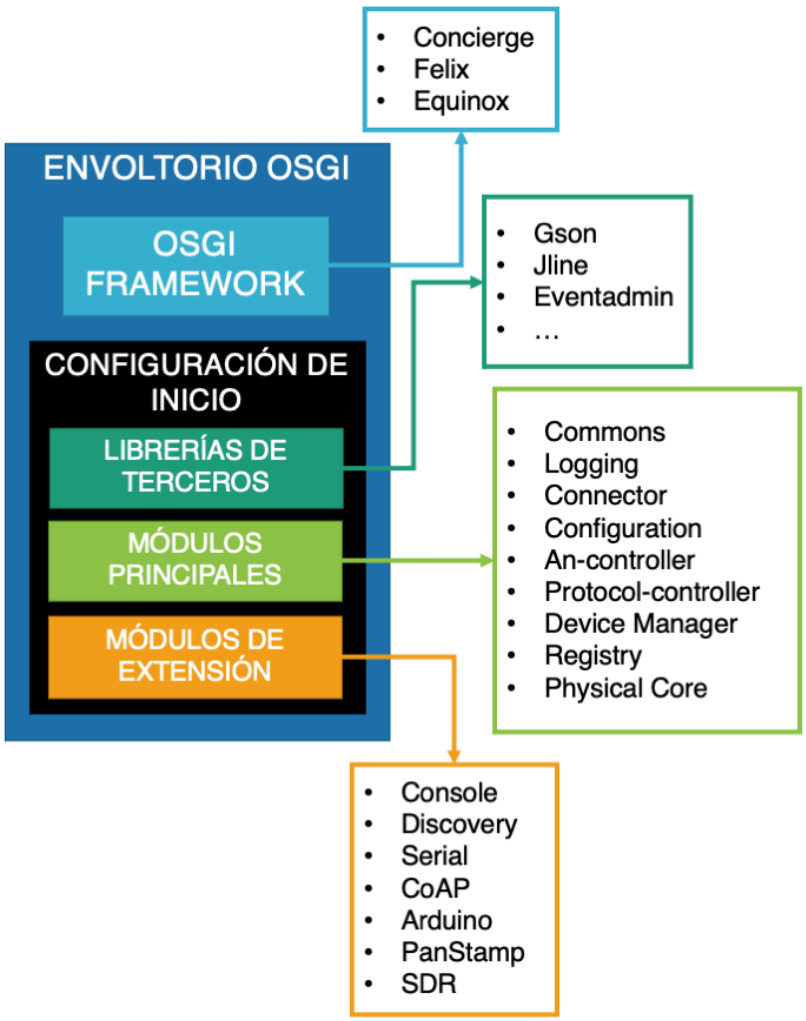

Figura 4.3: Módulos y librerías de la pasarela física

Además, tal y como hemos visto en la Sección 3.4, los módulos tienen interdependencias entre sí. Tras completar el desarrollo de la implementación de la pasarela física, se puede ver en la Figura 4.4, un esquema de las dependencias que existen entre las extensiones, módulos principales, y módulos comunes junto con el "framework".

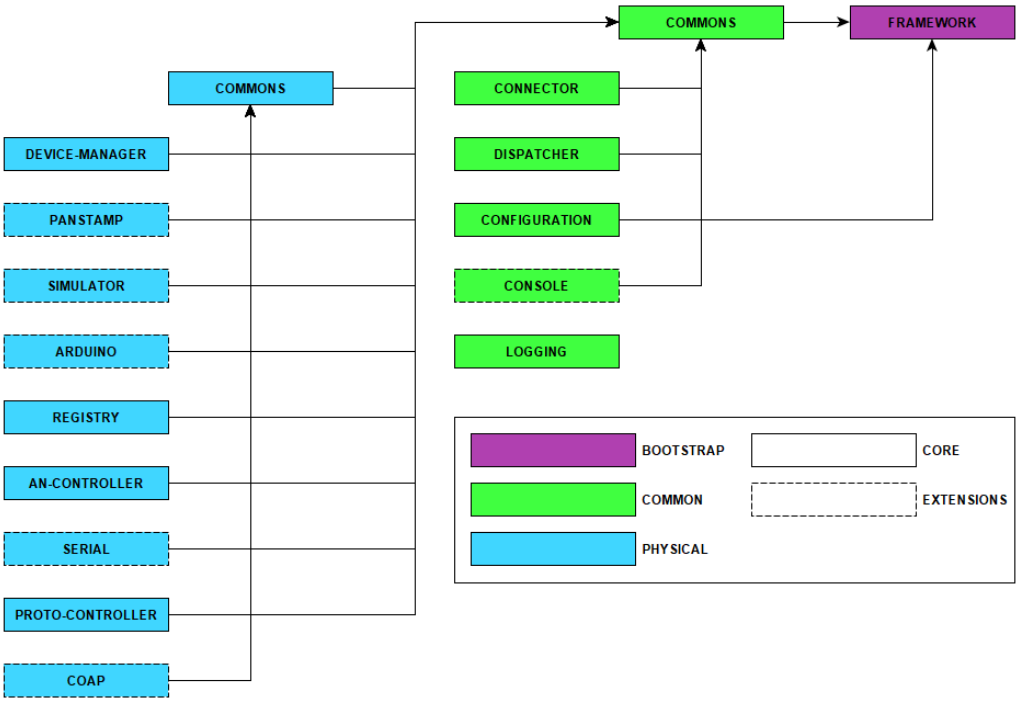

Figura 4.4: Dependencias de los módulos de la pasarela física

4.3.1. Hardware

El mayor condicionante con respecto al Hardware para ejecutar la pasarela es el lenguaje de programación utilizado, tal y como hemos visto en la Sección 4.1 se ha utilizado "Java 8.0". Si utilizamos una compilación "Compact 2 - Headless" para reducir el tamaño de la necesaria, los siguientes son los requisitos mínimos que ha de cumplir el dispositivo para la correcta ejecución de la pasarela física:

- **CPU:** x86-64, ARM (también otros en desuso como PowerPC o SPARC)
- **OS:** Windows, Linux, macOS, (y otros en desuso como freeBSD o Solaris)
- **RAM:** Depende de la complejidad/cantidad de los dispositivos. El mínimo requerido por la son 32MB. El mínimo para una correcta ejecución de la pasarela son 512MB.

- **Memoria no volátil (ROM/Flash/Disco):** Mínimo 16MB ("Compact 2 - Headless") y 5MB de la pasarela. En total 21MB.
- **Interfaces de comunicación:** Una interfaz de red para conectar a la pasarela virtual, y el resto de interfaces necesarias dependen de los sensores/actuadores que se vayan a controlar.

Como podemos ver, hemos logrado reducir la pasarela física a requerimientos mínimos de ejecución, pudiendo ser instalada en una gran variedad de dispositivos con mayor o menor capacidad. Como veremos en el Capítulo 5 en los pilotos se han utilizado dispositivos como la "Raspberry Pi 3" y "Simatic IoT 2000".

4.4. Implementación de la pasarela virtual

Al igual que en la implementación de la pasarela física, tras la ejecución del hilo principal expuesta en la Sección 4.2 se delega la ejecución a la clase principal de la pasarela virtual. En este caso, las acciones que ejecuta la clase principal de la pasarela virtual son:

- Lee los valores de configuración relevantes (Sección B.3 del Anexo B).
- Descubre los módulos de extensión relevantes para la ejecución.
- Inicia el generador de eventos y se subscribe a los mensajes de información de pasarela.
- Inicia el hilo de ejecución del módulo del conector, abriendo los puertos necesarios. Espera la recepción del mensaje de descripción de la pasarela física, tras recibirlo, envía el mensaje de descripción de la pasarela virtual.
- Inicia los hilos de las extensiones que necesiten una ejecución en paralelo (como la extensión de API REST o el motor de reglas). Estos leerán la configuración necesaria del módulo de configuración (Sección B.4 del Anexo B).

De igual manera que en la implementación de la pasarela física, en la pasarela virtual se utilizan (junto con los módulos principales, módulos de extensión y el "framework" OSGI) dependencias de librerías de terceros. En la Figura 4.5

se puede ver un esquema de los módulos y las librerías utilizadas en la pasarela física.

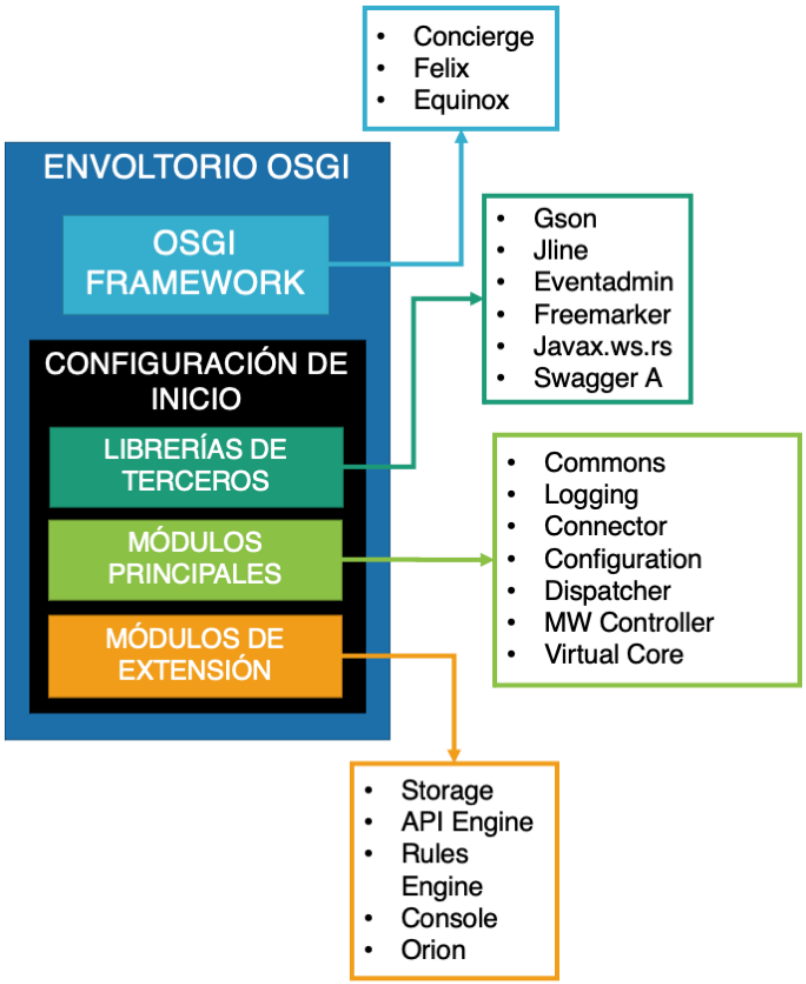

Figura 4.5: Módulos y librerías de la pasarela virtual

En la pasarela virtual los módulos también tienen interdependencias entre sí. En la Figura 4.6 se puede ver el esquema de las dependencias entre las extensiones, módulos principales, y módulos comunes junto con el "framework" tras completar el desarrollo de la implementación.

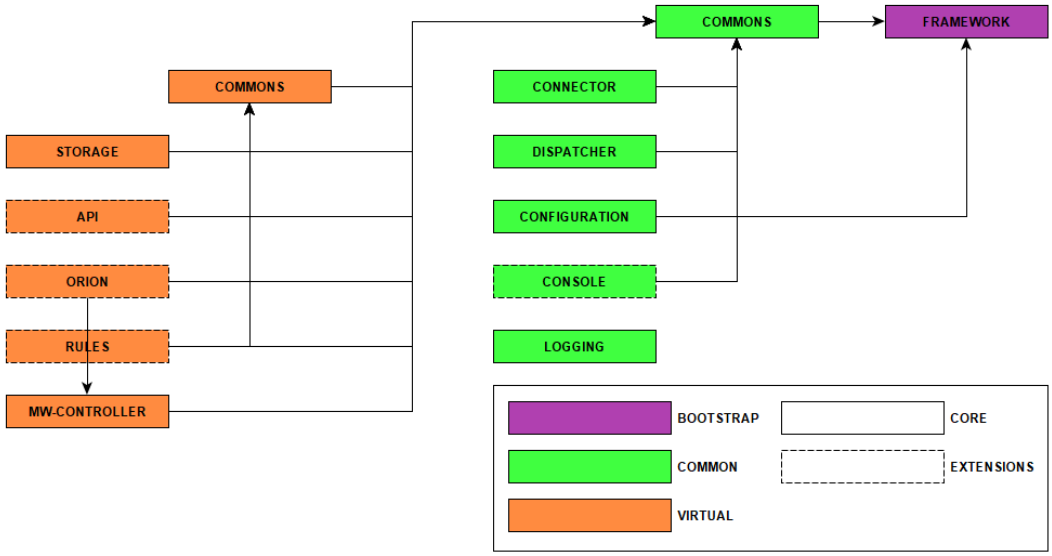

Figura 4.6: Dependencias de los módulos de la pasarela virtual

4.4.1. Plataformas de despliegue

La pasarela virtual está pensada para poder ser desplegada en el "Fog/Edge" o directamente en la Nube, en máquinas que tengan mayores capacidades que las que hemos visto en la Subsección 4.3.1 para la pasarela física.

Para la pasarela virtual no es necesario por tanto una compilación "Compact" como en la pasarela física, y se puede instalar una distribución de JVM "Full". Los requisitos mínimos de la máquina donde se ejecuta la pasarela virtual serán por tanto:

- **CPU:** x86-64, ARM
- **OS:** Windows, Linux, macOS
- **RAM:** 512MB
- **Disco:** 300MB
- **Interfaces de comunicación:** Al menos una interfaz de red para establecer la conexión con la pasarela física. Se puede utilizar esta misma interfaz para los módulos dinámicos como el controlador de plataforma IoT, el módulo API REST, etc.

Una posibilidad para el despliegue automatizado en un "contenedor" donde se facilita el aislamiento de la máquina y permite un despliegue masivo de pasarelas virtuales en un mismo "Host" es utilizar "Docker" [5]. Es muy sencillo generar una imagen de "Docker" con la pasarela virtual ya compilada, en la Sección D.1 del Anexo D se muestra el archivo de generación de esta imagen.

4.5. Interconexión Física-Virtual. Seguridad

El módulo de conector puede tener diferentes implementaciones dependiendo del caso de uso y capacidad de la red. Para los casos donde la capacidad de red no es limitante, la implementación basada en "WebSocket" y utilizando un formato de mensajes en "Json" es conveniente porque permite la depuración del protocolo de comunicación puesto que es más legible. Se puede ver un ejemplo de mensajes intercambiados entre las pasarelas en Anexo A.

Además, este módulo implementa una "cache" de mensajes tanto en la parte física como la virtual, y marca cada mensaje con un identificador único. De esta forma, si se pierde la conexión de manera espontánea, la pasarela física comenzará una rutina de reconexión automática para poder establecer de nuevo la conexión. Una vez establecida, la "cache" de mensajes inyectará de manera ordenada los mensajes que no han podido ser enviados anteriormente, de forma que no se pierda la sincronía.

Otra implementación está basada en "Protobuf 3.x" [6] que permite el intercambio de mensajes más tipados y eficientes, puesto que se trata de un protocolo binario para serializar datos estructurados.

En el módulo de interconexión entre la pasarela física y virtual, también se debe garantizar la seguridad en el intercambio de mensajes [98]. En esta implementación, se garantiza mediante el uso de una infraestructura de clave pública ("PKI"). En concreto, durante el establecimiento de conexión "SSL", se confiarán únicamente en certificados que hayan sido firmados por un certificado raíz de confianza. En la Sección D.2 del Anexo D se especifica los comandos necesarios mediante la herramienta "openssl" necesarios para generar esta cadena de certificados.

[5] https://www.docker.com/
[6] https://github.com/protocolbuffers/protobuf

4.6. Extensibilidad

En la pasarela existen cuatro interfaces de extensión e interacción diferentes:

- **Línea de comandos:** La extensión de la consola de la pasarela proporciona una interfaz de línea de comandos (CLI) para controlar la instancia de la pasarela física o virtual.
- **API REST:** Expuesta por el módulo de extensión API de la pasarela virtual para interactuar con la pasarela virtual y física.
- **API comunicación físico-virtual:** Mensajes intercambiados entre la física y la virtual a través del módulo conector. Si se cumple el protocolo de intercambio de mensajes se puede sustituir la parte física o virtual por una implementación propia.
- **API programática:** Bibliotecas e interfaces necesarias para desarrollar nuevos módulos de extensión para la pasarela. [7]

Para la creación de nuevas extensiones se debe incluir en la raíz del compilado un archivo de descripción (Sección C.1, Sección C.2 del Anexo C). Para facilitar el desarrollo de extensiones, además del "API programática" también se han desarrollado arquetipos "Maven" para la creación rápida de proyectos de desarrollo de extensiones para controladores de dispositivos [8].

4.7. Indicadores clave de rendimiento

Dentro del contexto del proyecto INTER-IoT, se han medido una serie de indicadores clave de rendimiento (KPI) tanto de forma cuantitativa como de forma cualitativa. Durante el proyecto se midieron en varias etapas y en las siguientes subsecciones se detallan los KPI al final del proyecto.

[7] https://inter-iot.github.io/gateway-javadocs/0.5.1-SNAPSHOT/

[8] http://nexus.inter-iot.eu/repository/maven-snapshots/eu/interiot/gateway/archetypes/device-controller.archetype/0.5.1-SNAPSHOT/device-controller.archetype-0.5.1-20190312.123152-1.jar

4.7.1. KPI cualitativos

Un KPI cualitativo es una característica descriptiva, una propiedad del sistema (en este caso la pasarela IoT desarrollada y expuesta en esta tesis doctoral). Los valores indican propiedades no mensurables y se encuadran más en una descripción del sistema en un momento concreto.

A continuación se detallan los KPI cualitativos obtenidos al final del desarrollo e implementación de la pasarela descrito en el Capítulo 4 [99]:

- Separación de una pasarela IoT en una parte física y otra virtual que se ejecutan de manera independiente pero coordinada.
- Se ejecutan en cualquier sistema operativo con una JVM.
- Ambos son modulares, consisten en módulos estáticos (obligatorios) y dinámicos (extensiones).
- Los módulos (tanto estáticos como dinámicos) tienen una interfaz totalmente desacoplada, por lo que diferentes implementaciones que cumplen la misma interfaz pueden ser utilizadas.
- Parte física:
  - Soporte de múltiples controladores de dispositivos físicos simultáneos, redes de acceso y protocolos.
  - Fácilmente ampliable con controladores de dispositivos personalizados.
  - Soporte para sensores (pasivos y activos) y actuadores.
  - Gestión remota (a través de la pasarela virtual).
  - Gestión local (a través de la extensión de interfaz de línea de comandos).
- Parte virtual:
  - Soporte de múltiples plataformas “Middleware” IoT (solo una activa).
  - Extensión de base de datos para el almacenamiento histórico de datos de los dispositivos.
  - Extensión de API REST para la gestión y consulta remotas.

- Extensión de motor de reglas CEP para reglas simples definidas con expresiones tipo "SQL" e instrucciones en Javascript (motor "Nashorn"[9]).
- Gestión local (a través de la extensión de interfaz de línea de comandos).

4.7.2. KPI cuantitativos

Un KPI cuantitativo es el más común e intuitivo. Son características mensurables que ofrecen una descripción del rendimiento de la IoT. Algunos valores dependen directamente del entorno de ejecución, por lo que este debe ser descrito también. A continuación se detallan las medidas obtenidas durante las fases de implementación (Capítulo 4) y validación (Capítulo 5, Capítulo 6 y Capítulo 7) [100, 101, 102].

En la Tabla 4.1 se especifican KPI cualitativos independientes del entorno. Las medidas dependientes del entorno se han realizado en un despliegue que consta de una pasarela física[10] y una pasarela virtual[11] conectadas a través de internet.

Se han realizado medidas en tres entornos diferentes:

- **Entorno 1:** 5 dispositivos transmitiendo 1 medida (coma flotante) cada 50ms. Tabla 4.2, Tabla 4.3, Figura 4.7, Figura 4.8.
- **Entorno 2:** 10 dispositivos transmitiendo 1 medida (coma flotante) cada 100ms. Tabla 4.4, Tabla 4.5, Figura 4.9, Figura 4.10.
- **Entorno 3:** 100 dispositivos transmitiendo 1 medida (coma flotante) cada 1s. Tabla 4.6, Tabla 4.7, Figura 4.11, Figura 4.12.

[9] https://openjdk.java.net/projects/nashorn/

[10] HW: Raspberry PI 3 (Quad Core 1.2GHz 64bit CPU, 1GB RAM) - OS: Raspbian - JVM:OpenJDK1.8

[11] HW: Azure Container Instances (8GB RAM, 1vCPU) - OS: alpine3.8 - JVM: OpenJDK1.8

Nombre	**Valor**
Extensiones desarrolladas	4
Arquetipos Maven desarrollados	2
Módulos de protocolo soportados	5
Módulos de plataforma soportados	3

Tabla 4.1: Indicadores clave de rendimiento cuantitativos independientes del entorno

Nombre	**Valor**
Max. Memoria RAM utilizada (MB)	75
Max. CPU utilizado (%)	9

Tabla 4.2: Indicadores clave de rendimiento cuantitativos - Entorno 1 - Parte física

Nombre	**Valor**
Max. Memoria RAM utilizada (MB)	300
Max. CPU utilizado (%)	10
Latencia (ms)	47

Tabla 4.3: Indicadores clave de rendimiento cuantitativos - Entorno 1 - Parte virtual

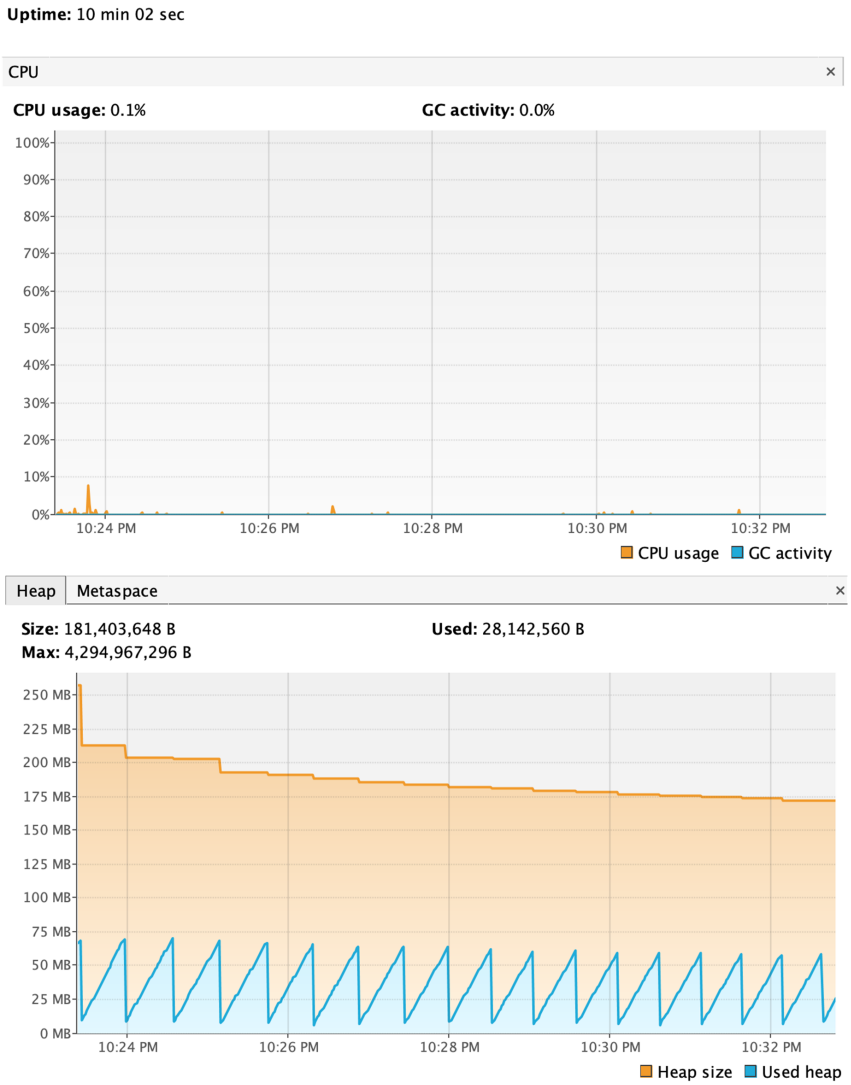

Figura 4.7: Indicadores clave de rendimiento cuantitativos - Entorno 1 - Parte física

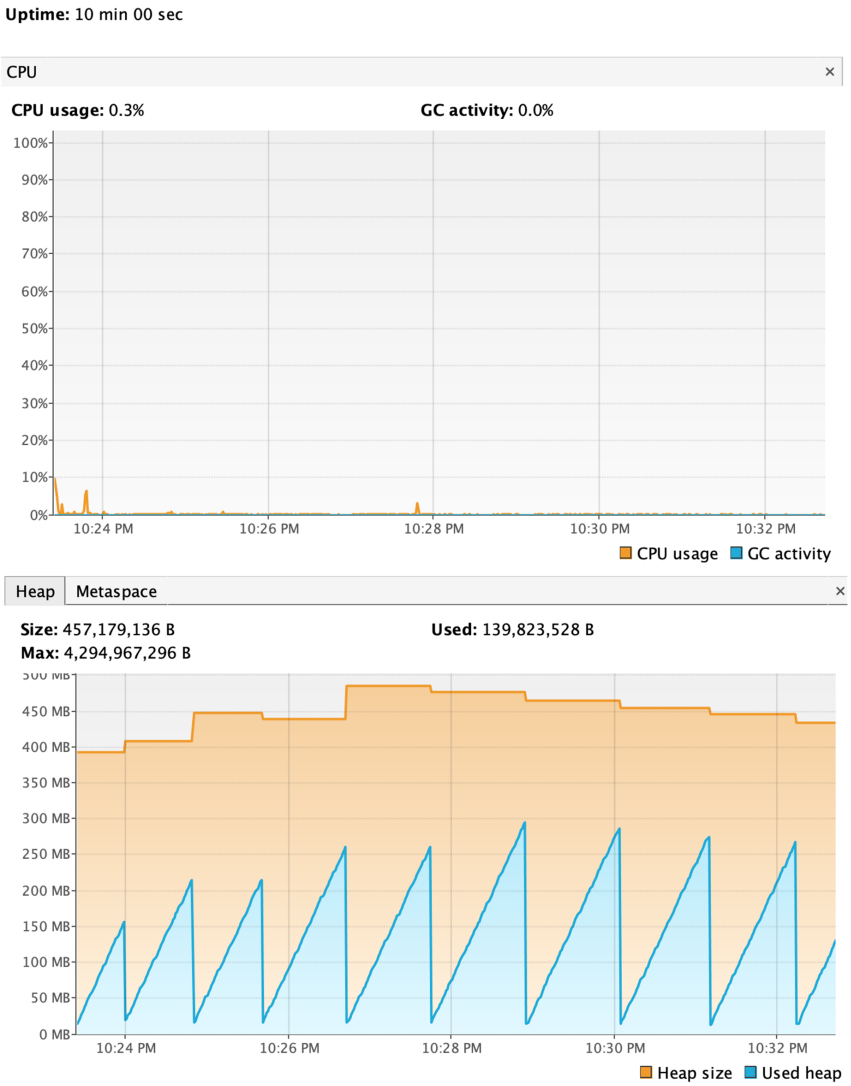

Figura 4.8: Indicadores clave de rendimiento cuantitativos - Entorno 1 - Parte virtual

Nombre	**Valor**
Max. Memoria RAM utilizada (MB)	78
Max. CPU utilizado (%)	11

Tabla 4.4: Indicadores clave de rendimiento cuantitativos - Entorno 2 - Parte física

Nombre	Valor
Max. Memoria RAM utilizada (MB)	250
Max. CPU utilizado (%)	12
Latencia (ms)	46

Tabla 4.5: Indicadores clave de rendimiento cuantitativos - Entorno 2 - Parte virtual

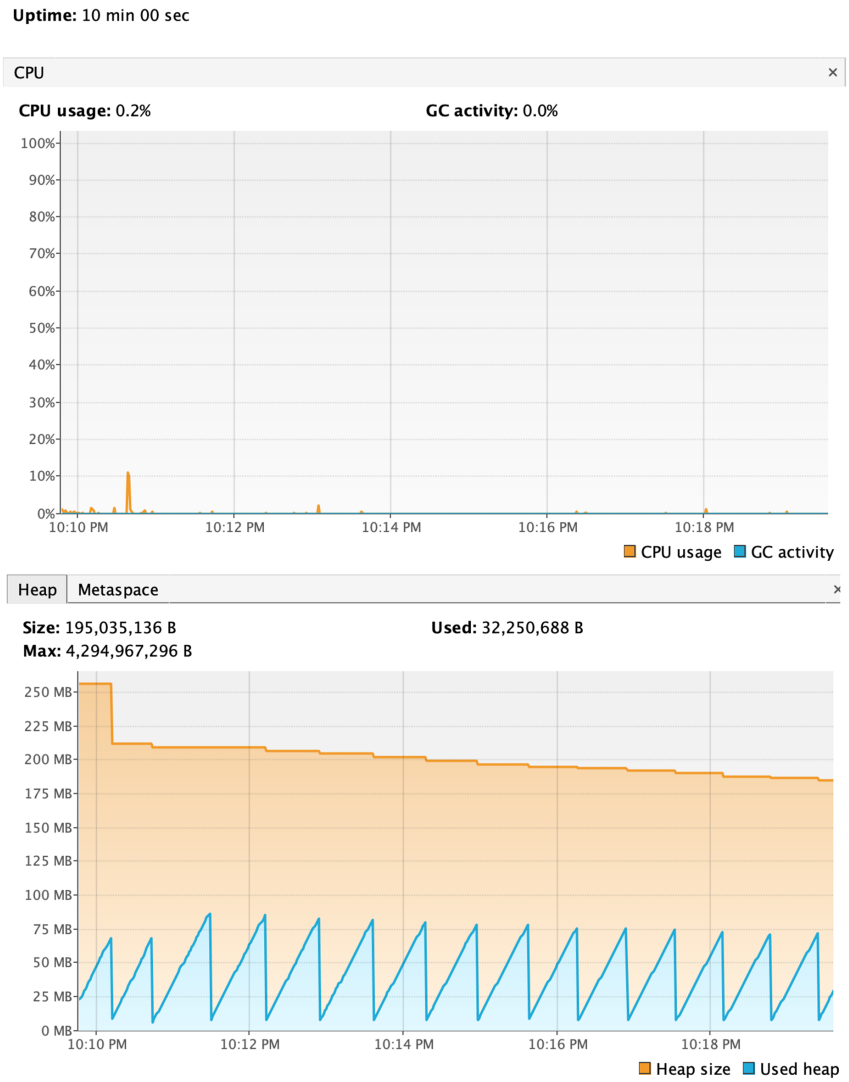

Figura 4.9: Indicadores clave de rendimiento cuantitativos - Entorno 2 - Parte física

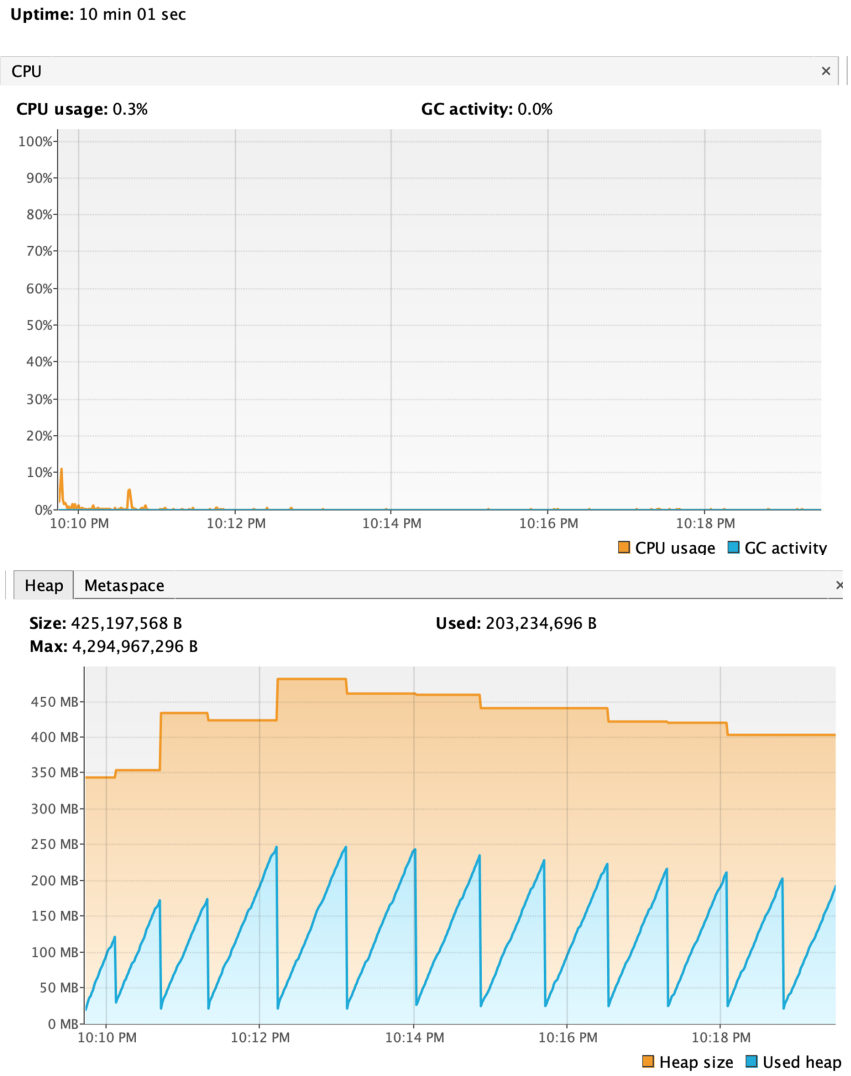

Figura 4.10: Indicadores clave de rendimiento cuantitativos - Entorno 2 - Parte virtual

Nombre	**Valor**
Max. Memoria RAM utilizada (MB)	74
Max. CPU utilizado (%)	19

Tabla 4.6: Indicadores clave de rendimiento cuantitativos - Entorno 3 - Parte física

Nombre	Valor
Max. Memoria RAM utilizada (MB)	340
Max. CPU utilizado (%)	10
Latencia (ms)	47

Tabla 4.7: Indicadores clave de rendimiento cuantitativos - Entorno 3 - Parte virtual

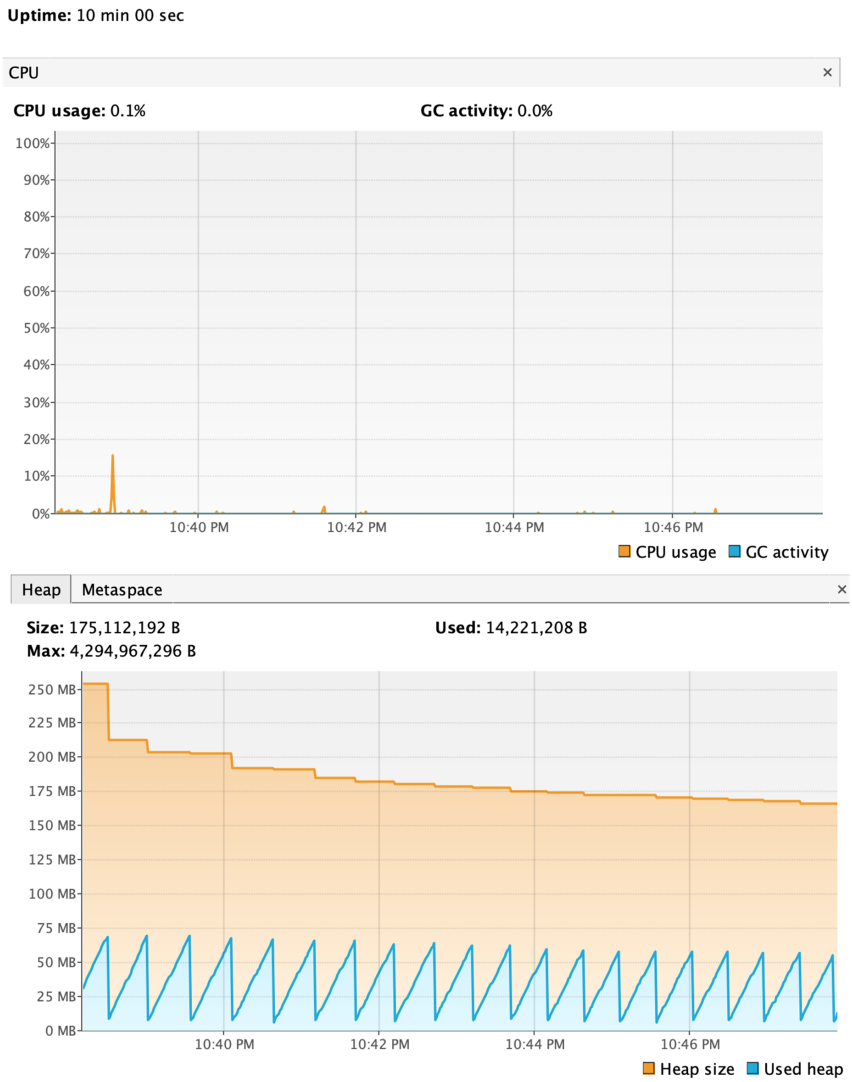

Figura 4.11: Indicadores clave de rendimiento cuantitativos - Entorno 3 - Parte física

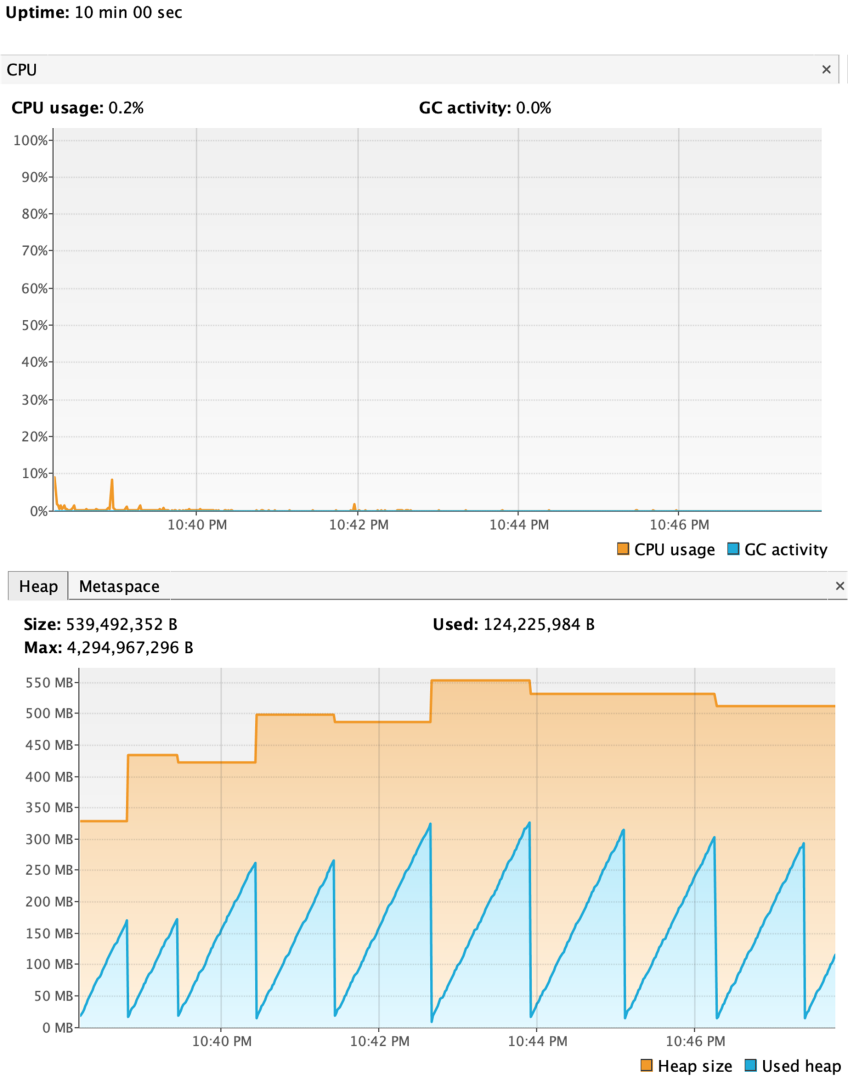

Figura 4.12: Indicadores clave de rendimiento cuantitativos - Entorno 3 - Parte virtual

Capítulo 5

Validación: INTER-IoT

El proyecto INTER-IoT es una acción de investigación e innovación dentro del Programa Marco de la Comunidad Europea Horizonte 2020. El proyecto tiene como objetivo el diseño, la implementación y la experimentación de un marco abierto, una metodología asociada y herramientas para permitir la interoperabilidad entre plataformas heterogéneas de Internet de las Cosas.

El proyecto permite el desarrollo eficaz y eficiente de aplicaciones y servicios de IoT inteligentes y adaptables, sobre diferentes plataformas heterogéneas de IoT, que abarcan dominios de aplicación únicos y/o múltiples. El proyecto se probará en dos dominios de aplicación: transporte y logística en un entorno portuario y salud móvil.

El enfoque de INTER-IoT es de propósito general y puede aplicarse a cualquier dominio de aplicación y entre dominios, en los que exista la necesidad de interconectar sistemas IoT ya desplegados o añadir otros nuevos.

INTER-IoT se basa en tres bloques principales:

- Métodos y herramientas para proporcionar interoperabilidad entre y a través de cada una de las capas de las plataformas (INTER-Layer)
- Marco global para programar y gestionar plataformas IoT interoperables (INTER-FW).
- Metodología de ingeniería (INTER-Meth) basada en la herramienta CASE para la integración/interconexión de plataformas IoT.

Estos tres bloques principales se representan en la figura 5.1.

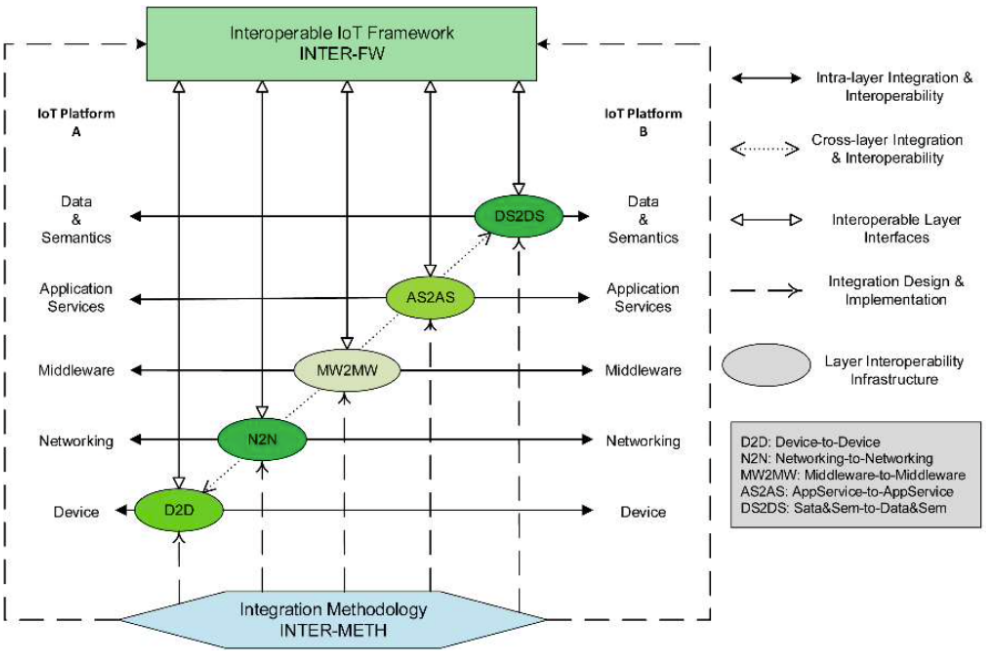

Figura 5.1: Concepto general de INTER-IoT

INTER-IoT proporciona un componente de mediación interoperable (INTER-Layer) para permitir el descubrimiento y el intercambio de dispositivos conectados a través de las plataformas IoT existentes y futuras para el rápido desarrollo de aplicaciones IoT multiplataforma. A su vez, permite una interoperabilidad flexible y voluntaria en diferentes capas. Este enfoque por capas puede lograrse introduciendo un despliegue incremental de la funcionalidad de INTER-IoT en el espacio de la plataforma, que en efecto influirá en el nivel de colaboración y cooperación de la plataforma con otras plataformas. INTER-IoT no pretende crear una nueva plataforma IoT, sino una estructura de interoperabilidad para interconectar diferentes plataformas IoT, dispositivos, aplicaciones y otros artefactos IoT.

La interoperabilidad sintáctica y semántica representan los mecanismos esenciales de interoperabilidad en el futuro ecosistema de INTER-IoT, mientras que la interoperabilidad organizativa/empresarial tiene diferentes estructuras/capas para permitir a los proveedores de plataformas elegir un modelo de interoperabilidad adecuado para sus necesidades empresariales. Se apoya en INTER-FW para permitir el desarrollo de nuevas aplicaciones y servicios sobre INTER-Layer e INTER-Meth, para proporcionar una metodología con

el fin de coordinar la interoperabilidad apoyada por la definición de diferentes patrones de interoperabilidad y una herramienta CASE.

INTER-Layer se compone de cinco capas, con el apoyo de componentes de capas cruzadas según sea necesario para la interacción de las diferentes capas:

- A nivel de dispositivos: para permitir la inclusión de nuevos dispositivos IoT y su interoperabilidad con los dispositivos heterogéneos ya existentes, permitiendo un rápido crecimiento de los ecosistemas de objetos inteligentes.
- A nivel de red: permitiendo el soporte para la movilidad de los objetos inteligentes ("roaming") y el enrutamiento de la información. Esto permitirá el diseño y la implementación de ecosistemas totalmente conectados.
- A nivel de "middleware": un sistema de descubrimiento y gestión de recursos sin fisuras para los objetos inteligentes y sus servicios básicos, que permita la explotación global de los objetos inteligentes en sistemas de IoT a gran escala.
- A nivel de aplicaciones y servicios: el descubrimiento, uso, importación, exportación y combinación de servicios heterogéneos entre diferentes plataformas de IoT.
- A nivel de datos y semántica: para lograr una interpretación común de los datos y la información de diferentes plataformas y fuentes de datos heterogéneas, proporcionando interoperabilidad semántica.

Además, INTER-FW, proporciona el entorno envolvente para la coordinación de componentes INTER-Layer y el desarrollo de nuevos servicios mediante una API común.

La interoperabilidad abierta cumple la promesa de permitir a los proveedores y desarrolladores interactuar e interoperar, sin interferir en la capacidad de cualquiera para competir ofreciendo un producto y una experiencia superiores. A falta de normas globales de IoT, el proyecto INTER-IoT apoya y facilita a cualquier empresa el diseño de dispositivos, objetos inteligentes o servicios de IoT y su rápida comercialización, y crea nuevos ecosistemas interoperables de IoT. INTER-IoT puede ofrecer una solución a cualquier problema potencial de interoperabilidad dentro del panorama del IoT. La Figura 5.2 representa el entorno potencial de uso de INTER-IoT.

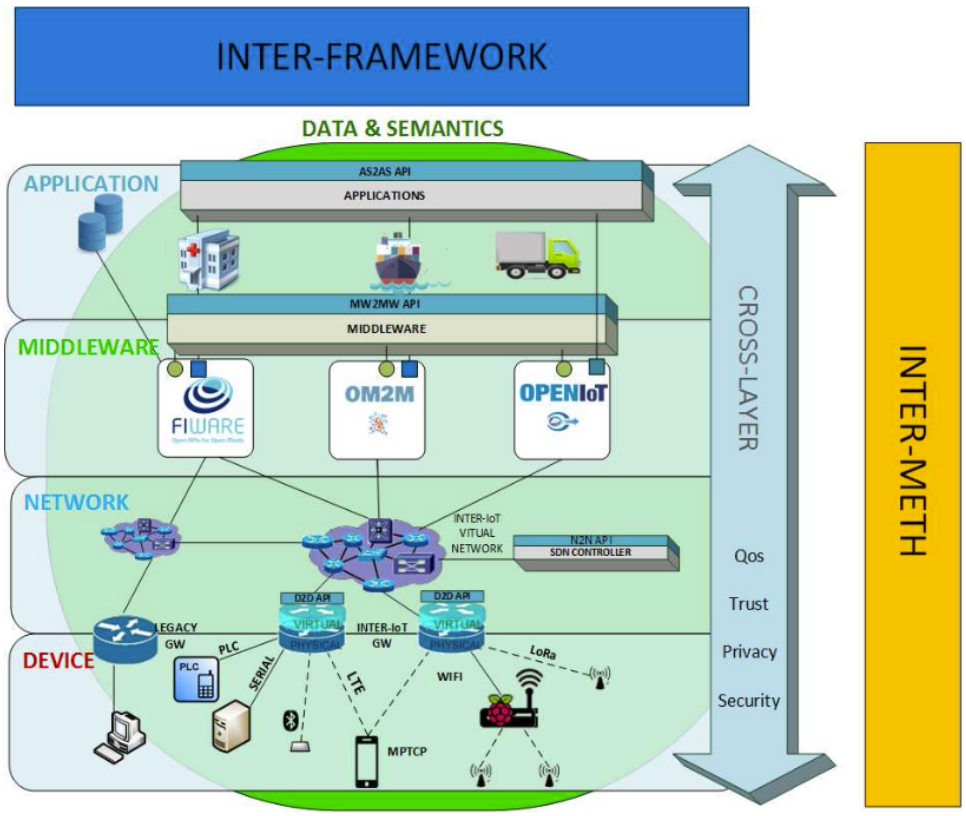

Figura 5.2: Enfoque por capas de INTER-IoT

El enfoque de INTER-IoT se basa en casos de uso, implementados y probados en tres pilotos realistas a gran escala:

- El Puerto de Valencia, un escenario complejo de transporte y logística que involucra plataformas heterogéneas con alrededor de 400 objetos inteligentes.
- Un centro nacional de salud italiano enfocado a salud móvil que involucra alrededor de 200 pacientes, equipados con redes de sensores corporales, sensores "vestibles" y dispositivos móviles inteligentes.
- Un piloto de dominio cruzado que involucra plataformas IoT de diferentes dominios de aplicación y ampliado por la colaboración de las soluciones asociadas a las diferentes capas y subcapas de los terceros que han asistido a una convocatoria abierta.

Los casos de uso son:

- **INTER-LogP:** El uso de plataformas IoT en los puertos del futuro permitirá localizar, supervisar y manejar diferentes equipos de transporte y carga y zonas de almacenamiento. Este caso de uso abordará la necesidad de manejar sin problemas la interoperabilidad de las plataformas IoT dentro de las instalaciones portuarias: terminal de contenedores, empresas de transporte, almacenes, transportistas, autoridades portuarias, aduanas y fuera del puerto.
- **INTER-Health:** El caso de uso de monitorización descentralizada y móvil del estilo de vida asistido, tiene como objetivo desarrollar un sistema de IoT integrado para monitorizar el estilo de vida de los seres humanos de forma móvil descentralizada para prevenir enfermedades crónicas. El proceso de monitorización mencionado puede descentralizarse desde el centro de salud hasta los hogares de los sujetos monitorizados, y apoyarse en la movilidad mediante el uso de monitores de actividad física en el cuerpo.
- **INTER-Domain:** Compuesto por plataformas IoT de los dos pilotos orientados al dominio de aplicación y las plataformas IoT y las soluciones orientadas a capas específicas de diferentes dominios de aplicación seleccionados en la convocatoria abierta. Se han seleccionado las plataformas SENSINACT [1] y OM2M [2] con orientación a ciudades inteligentes, y las contribuciones de las diferentes capas pueden complementar INTER-IoT.

El proyecto ha analizado los requisitos proporcionados por las partes interesadas del proyecto y la usabilidad de las soluciones proporcionadas desde la perspectiva de los creadores de la plataforma IoT, los propietarios de la plataforma IoT, los programadores de aplicaciones IoT y los usuarios que investigan las perspectivas de negocio y crean nuevos modelos de negocio. Estos resultados permiten la puesta en marcha el ecosistema INTER-IoT y los beneficios más importantes para terceros están relacionados con las nuevas características y componentes que han sido liberados por el consorcio: metodologías, herramientas, protocolos y API. Eso se ha publicado como elementos abiertos disponibles para desarrollar nuevas aplicaciones y servicios [3]. La variedad y la

[1] https://projects.eclipse.org/projects/technology.sensinact
[2] https://www.eclipse.org/om2m/
[3] https://github.com/orgs/INTER-IoT/repositories

disponibilidad cruzada de los resultados han sido utilizados para construir e integrar servicios y plataformas en diferentes capas según las necesidades de los interesados y los desarrolladores. En el futuro, la disponibilidad de más y nuevos datos estimulará la creación de nuevas oportunidades y productos.

5.1. Caso de uso: INTER-LogP

5.1.1. Introducción

En los últimos años, ha surgido la necesidad de compartir datos en tiempo real entre distintas empresas para ofrecer nuevos servicios a sus clientes. En el entorno portuario, hay muchas empresas diferentes, cada una con su propio sistema independiente. Hoy en día solo intercambian alguna documentación logística y no datos de sensores.

El objetivo del piloto INTER-LogP es demostrar la necesidad de un sistema que permita el intercambio de datos y mensajes entre los diferentes actores de la comunidad portuaria. En la figura 5.3 se ofrece una visión general. Hay tres actores principales: el puerto, la terminal y la empresa de transporte. INTER-IoT tiene que proporcionar interoperabilidad entre las plataformas IoT del puerto y la terminal, y dar acceso a otros dispositivos de otras empresas, como los camiones.

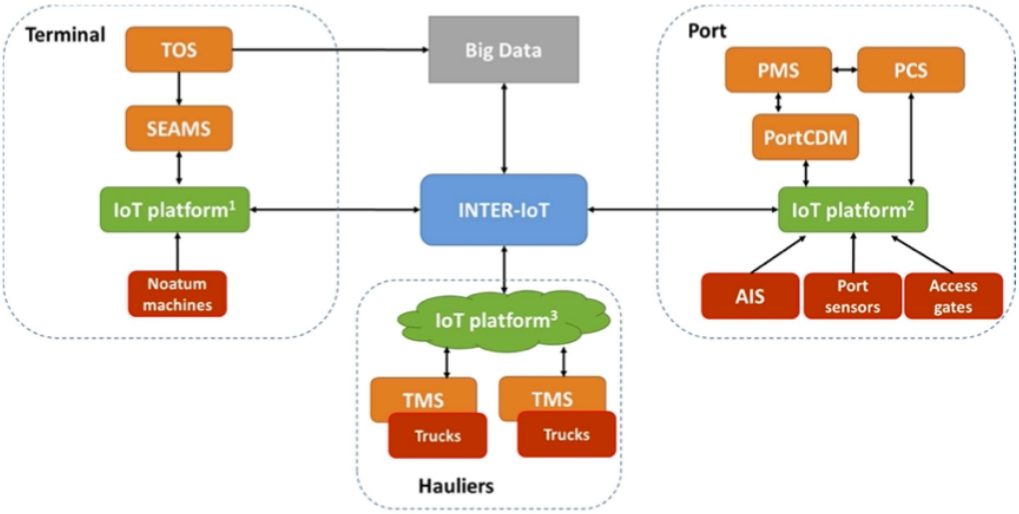

Figura 5.3: Arquitectura de alto nivel de INTER-LogP

Tanto el puerto como la terminal tienen un gran número de sensores y dispositivos que producen grandes cantidades de datos, que pueden ser interesantes para otras entidades. Además, necesitan datos de otras empresas para dar un mejor servicio a sus clientes.

Como veremos más adelante, la pasarela IoT se utiliza en los sistemas desplegados por uno de los tres actores principales en este piloto: el terminal de contenedores (Subsección 5.1.3).

Autoridad Portuaria

La autoridad portuaria dispone de varios sensores distribuidos por el puerto que proporcionan datos para la gestión y la explotación. La mayoría de esos datos son confidenciales, pero otros pueden ser compartidos, aportando valor a otras empresas.

La arquitectura para proporcionar interoperabilidad a partir de la infraestructura existente es la que puede verse en la Figura 5.4. En la actualidad, la autoridad portuaria dispone de una base de datos común en la que todos los datos procedentes de diferentes sistemas se almacenan (en rojo). Utiliza WSO2 para proporcionar una arquitectura IoT de dos maneras: datos en tiempo real a través del "Message Broker" y datos históricos a través del servidor de "Data Services" y el bus de "Enterprise service".

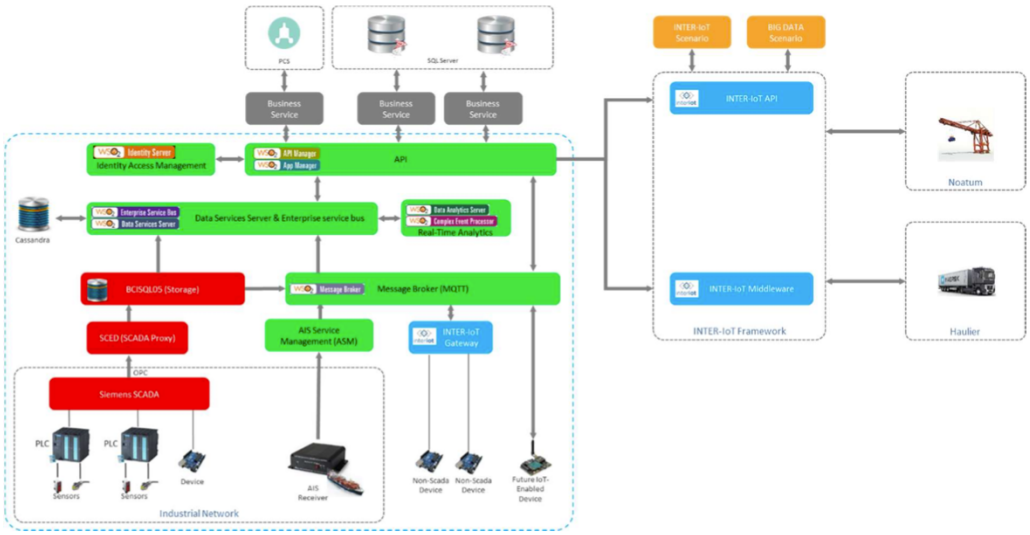

Figura 5.4: Integración de la plataforma IoT del puerto

Como el puerto tiene su propia plataforma, la integración con INTER-IoT se realiza a través de INTER-MW. Necesita un puente o "bridge" en la capa de middleware para poder interoperar con otras plataformas. Otra integración podría realizarse si se necesita desplegar nuevos dispositivos o sensores en un lugar sin conexión por cable. En ese caso, se puede utilizar la pasarela desarrollada en esta tesis dentro del marco del proyecto INTER-IoT para conectar con la plataforma IoT todos los sensores.

WSO2 es un middleware de arquitectura orientada a servicios (SOA) de código abierto. Está diseñado con componentes independientes, por lo que se puede adaptar para una solución orientada a las aplicaciones empresariales. Los productos WSO2 utilizan tecnología Java y están construidos sobre WSO2 Carbon, una plataforma de middleware SOA. Carbon hace uso de Apache Axis2 y encapsula la funcionalidad SOA, como los servicios de datos, la gestión de procesos de negocio, el enrutamiento/transformación ESB (Enterprise Service Bus), las reglas, la seguridad, el estrangulamiento, el almacenamiento en caché, el registro y la supervisión. No todos los componentes se utilizan como implementaciones independientes. Muchos de ellos se utilizan para complementar las capacidades o añadir funcionalidad a una implementación del ESB. Los principales componentes WSO2 desplegados en la plataforma IoT son:

- **Integración Enterprise Service Bus:** Permite a los desarrolladores conectar y gestionar sistemas y software de acuerdo con los principios de la gobernanza SOA. Servidor de servicios de datos: Proporciona una interfaz de servicios web para los almacenes de datos. Agente de mensajes: Traduce, valida y encamina los mensajes entre sistemas. Gestión de API Gestor de API: Plataforma de gestión de APIs para crear, desplegar y gestionar APIs para exponer datos y funcionalidades de los sistemas backend.

- **Gestión de identidades y seguridad:** Conecta y gestiona múltiples identidades a través de aplicaciones, APIs, la nube, el móvil y los dispositivos del Internet de las Cosas. Gestión y gobierno App Manager: Facilita el proceso de creación, despliegue y gestión de aplicaciones. Analítica Servidor de análisis de datos: Analítica en tiempo real, por lotes, interactiva y predictiva con datos de la empresa. Procesador de eventos complejos: Procesamiento y detección de eventos en tiempo real. Identifica patrones de múltiples fuentes de datos y analiza sus impactos. Utiliza WSO2 Siddhi y Apache Storm.

Terminal de contenedores

La correcta gestión de los recursos en una terminal de contenedores implica la monitorización de toda la maquinaria para poder gestionar adecuadamente los recursos. Por ello, en la terminal de Noatum cada una de las máquinas (vehículos, grúas, etc.) proporciona datos masivos de hasta 80 sensores por máquina y segundo. Hay alrededor de 300 dispositivos monitorizados entre las máquinas y la iluminación dinámica de los postes de luz. Los datos se envían desde la maquinaria a la plataforma IoT de dos maneras: Los sensores "legacy" se recogen una vez por segundo y se insertan en la Plataforma IoT, mientras que los nuevos dispositivos IoT se configuran para enviar directamente a través de interfaces MQTT o REST datos en tiempo real. Además, los datos se almacenan en una base de datos no relacional, lo que permite un acceso más rápido a la información. Como en el caso del puerto, la plataforma IoT del terminal se integrará con INTER-IoT a través de la capa de middleware y el API.

La terminal de contenedores tiene su propio servidor con su plataforma IoT. Es interesante principalmente conocer la hora estimada de llegada del camión a la terminal para poder gestionar sus recursos. Además, la terminal da acceso a otras empresas a algunos de sus propios datos, como la entrada y salida de camiones por su acceso.

Empresa de transporte

La empresa de transportes cuenta con una amplia flota de camiones que acceden diariamente al puerto. Cada uno de ellos tiene una aplicación móvil (MyDriving) instalada en un móvil o una tableta que actúa como puente entre el vehículo y la plataforma IoT de la empresa. Todos los dispositivos del camión y del conductor envían los datos a la plataforma IoT a través de la app móvil mediante Bluetooth. La empresa de transporte tiene una plataforma IoT en "Azure", donde sus camiones envían todos los datos del vehículo. Estos datos serán accesibles para otras empresas siempre que estén autorizadas y se cumplan ciertas condiciones, como estar dentro de la zona portuaria.

5.1.2. Pilotos IoT desplegados

Durante la ejecución del proyecto se desplegaron tres pilotos en los que se demostraron los productos desarrollados. Estos pilotos son:

Piloto IoT de control de acceso, tráfico y asistencia operativa

El objetivo principal en el piloto definido es un servicio para controlar el acceso, supervisar el tráfico y asistir las operaciones en el puerto. Varios sistemas podrán identificar a los camiones y a los conductores utilizando diferentes dispositivos. Esta información puede ser compartida bajo ciertas reglas predefinidas a través de la interoperabilidad entre las plataformas involucradas. Esta información puede utilizarse para que la plataforma de la Autoridad Portuaria controle el camión dentro del puerto (con fines de seguridad y protección) y para gestionar más eficazmente los recursos en la terminal. Esto también permitirá evitar colas en las puertas de acceso al puerto y a la terminal.

Los principales beneficios que podemos obtener de este escenario son la obtención de datos relativos a las colas, la congestión y la distribución temporal del tráfico, para gestionar eficazmente los recursos. Otro dato importante es la posición de los camiones mientras están dentro de las instalaciones portuarias, por seguridad y protección. Todos estos datos pueden ser compartidos entre la autoridad portuaria y las terminales portuarias para mejorar el funcionamiento.

Piloto de iluminación dinámica

En este piloto se desplegará y se evaluará la correcta ejecución de la pasarela desarrollada. El objetivo es sustituir las luminarias existentes por un sistema de iluminación inteligente, de forma que se iluminen las zonas cuando sean necesarias, ofreciendo mayor seguridad y a su vez ahorrando energía. En la Subsección 5.1.3 se explica en detalle este piloto y el papel de la pasarela en el sistema IoT desplegado.

Piloto Detección de ráfagas de viento

Actualmente, tanto la autoridad portuaria como cada una de las terminales de contenedores del puerto disponen de anemómetros para detectar las rachas de viento. En situaciones en las que la velocidad del viento supera un umbral, las operaciones deben detenerse por razones de seguridad. Sin embargo, cada terminal solo puede medir la información en sus premisas, por lo que no hay datos de las zonas circundantes, lo que hace imposible predecir cuándo se pueden esperar las rachas de viento más fuertes. Esto hace que la primera detección de viento fuerte sea una situación de riesgo para los operadores, ya

que el peligro solo se detecta cuando hay ya está activo. Si pudieran recibir esta información antes, detendrían la operación de forma más segura.

El principal beneficio que podemos obtener de este escenario es la mejora de la seguridad operativa en las terminales, permitiendo un sistema de concienciación temprana que podría acabar en menos accidentes por fenómenos ambientales.

5.1.3. Piloto de iluminación dinámica

El objetivo de este piloto es ampliar la iluminación inteligente (Iluminación Dinámica) en la zona de Noatum y la zona ferroviaria. En este caso, los postes de iluminación son de la autoridad portuaria de Valencia, pero la maquinaria es de Noatum, por lo que se necesita un intercambio de datos entre ambas empresas para iluminarla adecuadamente durante la operación. Actualmente la zona de vías está poco iluminada con los postes de alumbrado de la zona de contenedores. El objetivo es sustituir los postes de iluminación de la carretera por un sistema de iluminación dinámica, que recibe datos de la terminal para cambiar el grado de iluminación. El sistema de iluminación dinámica se basa en la posición GPS de los equipos portuarios de Noatum y en sensores PIR de largo alcance (sensores de presencia).

Como se puede observar en la Figura 5.5, la zona de vías (zona verde) está poco iluminada con los postes de alumbrado del patio de contenedores. El objetivo es sustituir los postes de iluminación de la carretera (zona azul) por un sistema de iluminación dinámica, que recibe datos de la terminal para cambiar el grado de iluminación. El sistema de iluminación dinámica se basa en la posición GPS de los equipos portuarios de Noatum y en sensores PIR de largo alcance (sensores de presencia).

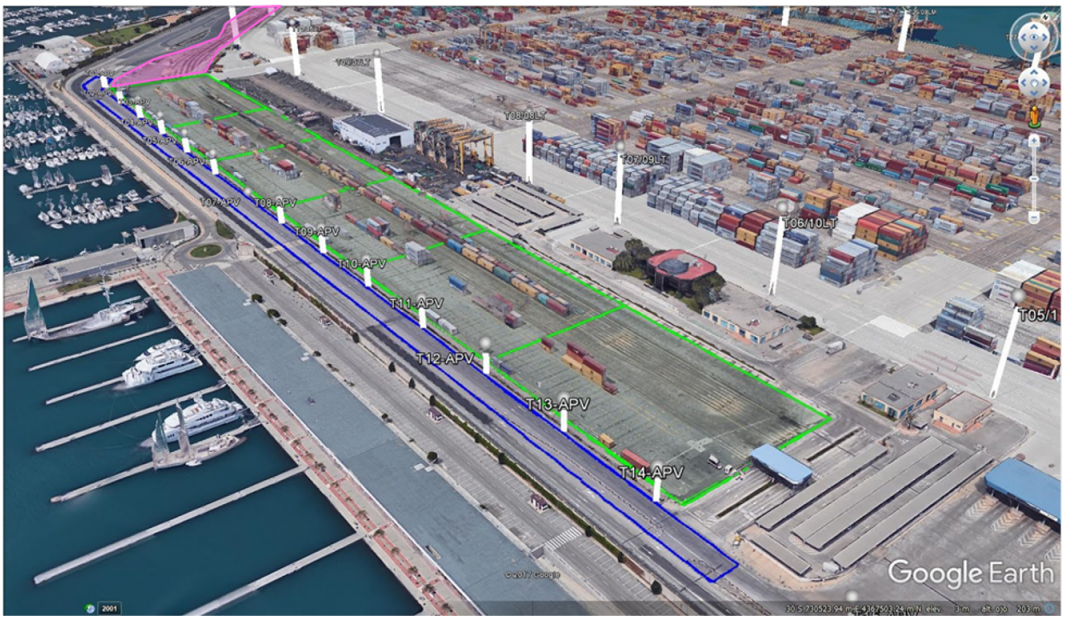

Figura 5.5: Piloto de iluminación: Postes de alumbrado y zonas del terminal de contenedores

Los principales beneficios que podemos obtener de este escenario es un ahorro de energía debido a la adaptación de la iluminación al tráfico y a la operación, y una mejora de la seguridad en la infraestructura ferroviaria debido a una mejor iluminación. Este piloto se desplegará con dos enfoques diferentes. En primer lugar, se desplegará un piloto solo con la participación de los socios de INTER-IoT. Luego, habrá una segunda versión en los pilotos de INTER-Domain, que integra la tecnología de una otra empresa (E3TCity) que participa en la convocatoria abierta promocionada por el proyecto, en la Figura 5.6 se puede ver un esquema del despliegue del piloto de iluminación.

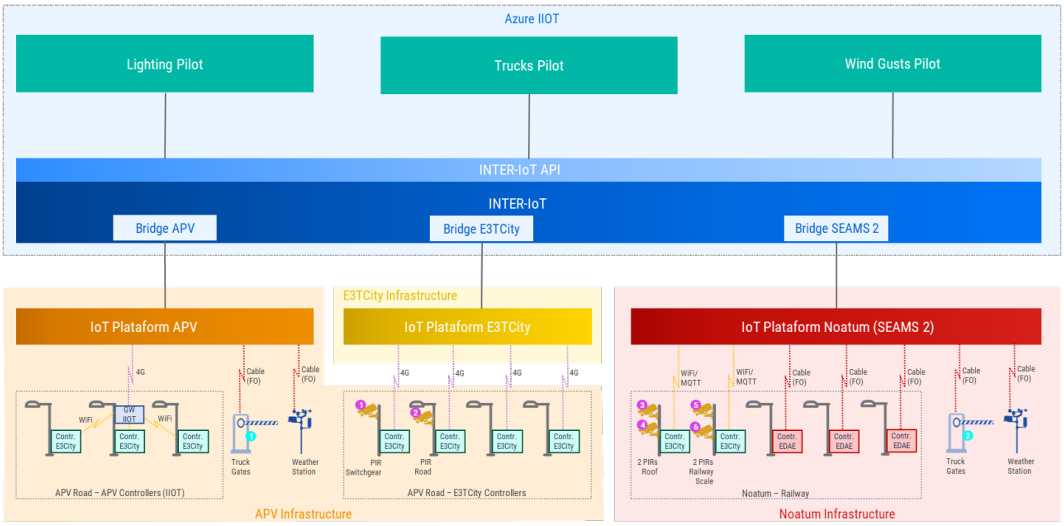

Figura 5.6: Esquema de despliegue del piloto de iluminación

En el piloto de iluminación dinámica, se evalúa la pasarela desplegándola en varios postes lumínicos. En concreto en las cajas de los postes **B08**, **B12** y **B15**. En el resto de postes se despliegan otro tipo de controladores de postes lumínicos que también forman parte del piloto de iluminación dinámica. En la Figura 5.7 se puede ver un esquema de la ubicación de los elementos que forman parte del piloto.

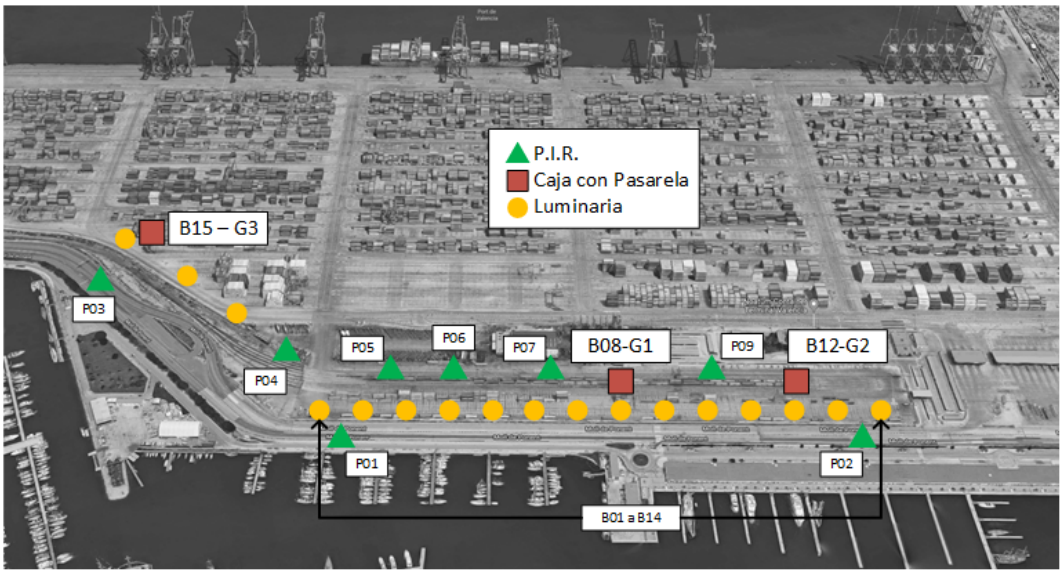

Figura 5.7: Elementos que forman parte del piloto de iluminación dinámica

Según la caja en la que está desplegada la pasarela, se lleva a cabo una instalación diferente dependiendo de la disponibilidad de red y los elementos cercanos en la caja. En el caso de las cajas **B08** y **B12** existe conectividad de red directa, por lo que las pasarelas **G1** y **G2** reciben directamente los mensajes MQTT del PIR (sensores) con los eventos recibidos, al igual que se mandan los mensajes MQTT a los controladores de las luminarias con las acciones a realizar (actuadores). En la caja **B15** no existe conectividad de red, por lo que la pasarela **G3** utiliza un módem USB 4G y se conecta a las luminarias directamente a través de MODBUS.

Los elementos utilizados en las cajas **B08** y **B12** son (Figura 5.8):

- *TELTONIKA RUT950*: para la conectividad de red.
- *SIMATIC IOT2000/2040*: el Hardware donde se ejecutará la pasarela física.

En la Figura 5.8 y la Figura 5.9 se pueden ver los esquemas de conexión de las diferentes cajas.

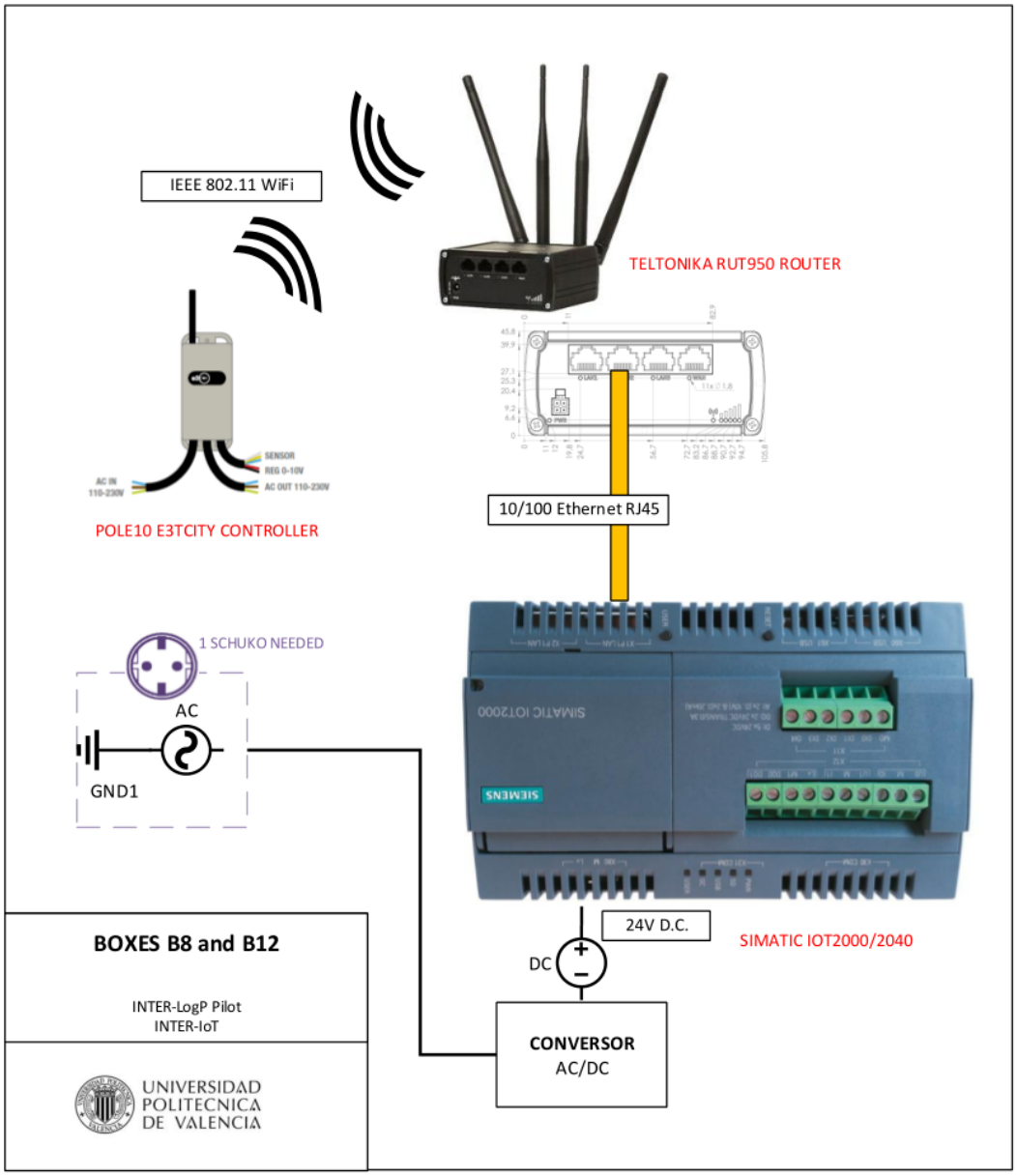

Figura 5.8: Esquema de conexión de las cajas B8 y B12

Los elementos utilizados en la caja **B15** son (Figura 5.9):

- *LB40 E3TCity*: controlador MODBUS de las luminarias.
- *Raspberry PI 3*: el Hardware donde se ejecutará la pasarela física.

- *Modem 4G USB*: para la conectividad de red.

- *Conversor RS485 a USB*: para la conversión de señalización en serie RS485 a RS232.

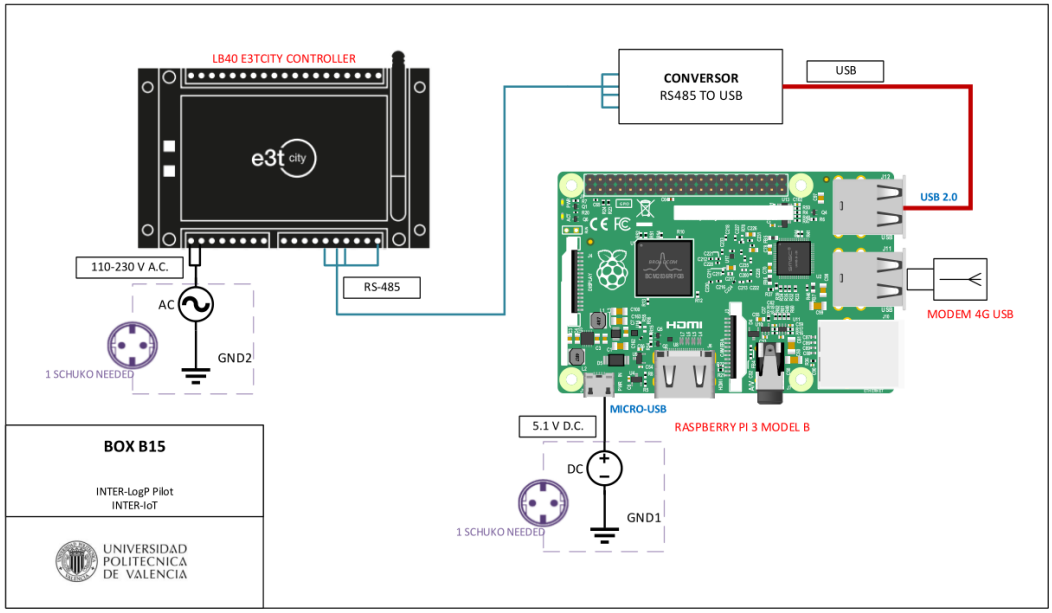

Figura 5.9: Esquema de conexión de la caja B15

En la Figura 5.10 y la Figura 5.11 se pueden ver las cajas de las luminarias con todos los elementos ya conectados.

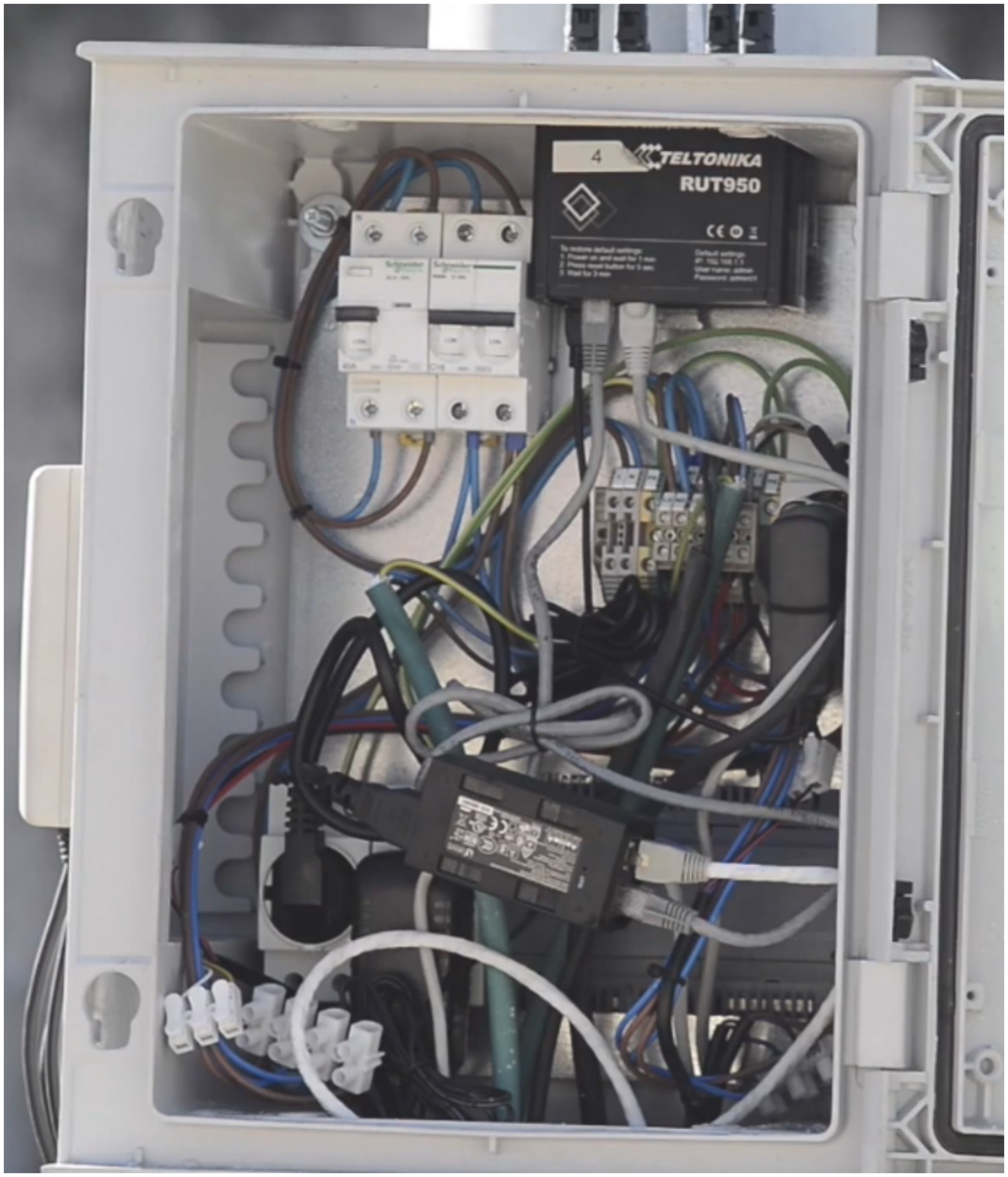

Figura 5.10: Caja B8/B12 con todos los elementos conectados

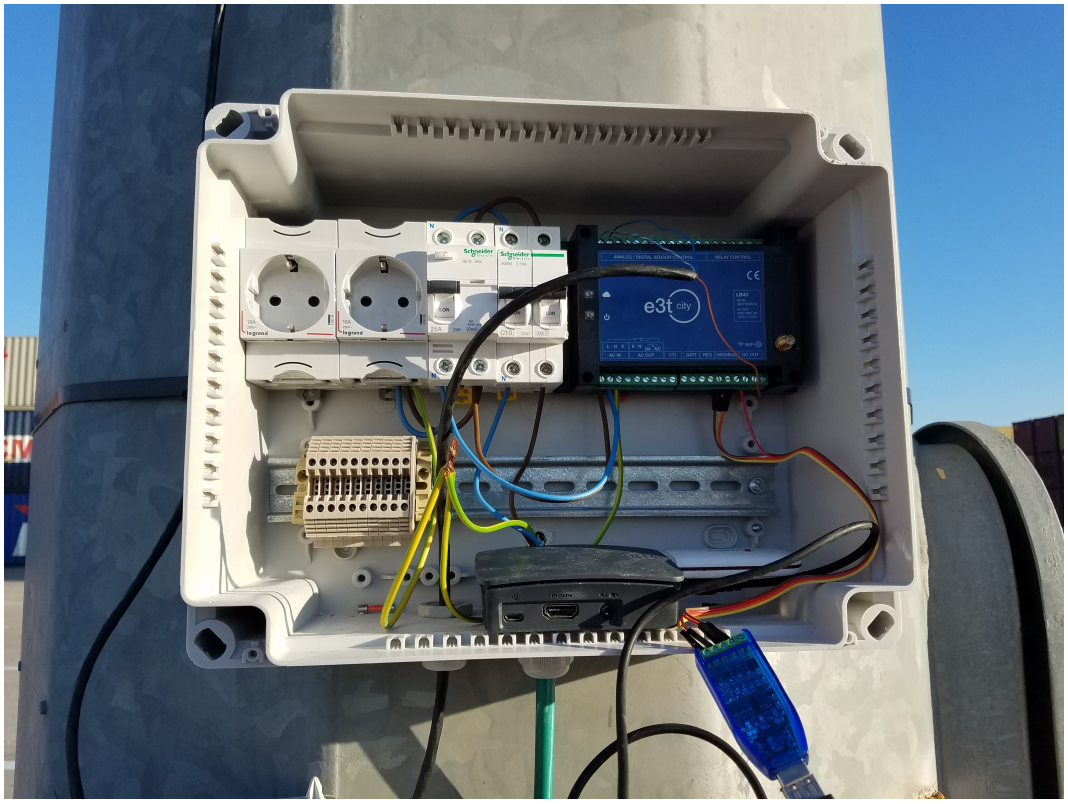

Figura 5.11: Caja B15 con todos los elementos conectados

Finalmente, las pasarelas físicas están conectadas con la pasarela virtual que está presente en las instalaciones de la Autoridad Portuaria y estas a su vez conectadas a la plataforma IoT (WSO2).

5.2. Caso de uso: INTER-Health

5.2.1. Introducción

Es un hecho conocido que el mundo envejece rápidamente. Vivir más tiempo no significa vivir mejor, lo que puede significar una reducción de la calidad de vida. Ello conduce a una población con mayor dependencia que hace que los sistemas sanitarios se vean desbordados y genera una necesidad de soluciones para aliviar esta carga. Los sistemas sanitarios necesitan mejores datos para comprender los riesgos sanitarios a los que se enfrenta la población para dirigir

los servicios de prevención e intervención adecuados. No se trata de proporcionar medicamentos para mitigar un problema de salud; se trata de proporcionar un servicio de salud para contribuir a tener una **buena calidad de vida a lo largo de sus vidas.**[103]

En la actualidad, la Medicina Personalizada es un nuevo campo en el que uno de sus objetivos es conseguir los mejores resultados para prevenir o gestionar la enfermedad de un paciente. La salud está determinada por las características intrínsecas del ser humano, combinadas con su estilo de vida y el entorno. La combinación de esta información socio-médica de la vida de los seres humanos puede ayudar a determinar el riesgo individual de desarrollar una enfermedad, la detección precoz de enfermedades, o incluso intervenciones más eficaces para mejorar la salud.

En esa línea, el Internet de las Cosas aporta al mercado un abanico de oportunidades, permitiendo la comunicación omnipresente entre el mundo físico y el mundo virtual [104]. El IoT tiene el potencial para contribuir a muchas aplicaciones de salud electrónica, como la monitorización, enfermedades crónicas, o cuidado de ancianos entre otras [105, 106]. El número de aplicaciones de salud electrónica en el mercado está aumentando rápidamente, lo que genera una enorme cantidad de datos, siendo los datos médicos la columna vertebral de los sistemas sanitarios [13, 25, 26].

Al mismo tiempo, el cambio cada vez mayor hacia la atención centrada en el paciente genera la necesidad de una plataforma sanitaria integrada para lograr la escalabilidad y el compromiso. No es común que las organizaciones sanitarias dispongan de una única historia clínica electrónica. Por lo general, pueden tener varias fuentes de datos para diferentes fines. Esta fragmentación lleva a poner en riesgo la integridad de los datos, a definir procesos que consumen mucho tiempo y a crear desafíos en la coordinación de la atención para el paciente, aumentando los costes de mantenimiento [107].

El objetivo de la sanidad conectada comienza con un sistema integrado a una asistencia sanitaria orientada a los datos. Sin embargo, no siempre es posible integrar todo en la misma plataforma.

Debido a la importancia de los datos médicos, los desafíos de las TIC para el manejo de datos médicos, se vuelven más importantes. La interoperabilidad es una cuestión fundamental para comunicar y manejar diferentes formatos de datos médicos. Al mismo tiempo, hay varias normas legales y técnicas para el manejo, el procesamiento y la comunicación de los datos médicos. La interoperabilidad y la integración en el sistema sanitario dependen de varios niveles de conectividad. Abarca un espectro técnico muy amplio y plantea enormes

desafíos para conectar diferentes piezas (plataformas sanitarias, soluciones de m-Health, dispositivos IoT o cualquier otro recurso que contribuya a una mejor vida de los pacientes) de forma regulada y estandarizada para los flujos de trabajo [108, 109, 110].

El marco de INTER-IoT aplicado al sector sanitario, INTER-Health, está diseñado y construido para adaptarse específicamente a las necesidades de comunicación y pacientes y profesionales de la salud. INTER-Health integra diferentes arquitecturas IoT, servicios de salud electrónica y sensores de salud. Es una prueba de concepto del el potencial de INTER-IoT en la provisión de interoperabilidad dentro de un entorno clínico. INTER-Health mejora el servicio sanitario ofrecido por el hospital proporcionando una atención continua.

Como parte del despliegue de INTER-Health se desarrolla un prototipo de sensorización del paciente totalmente integrado con la pasarela física denominado "Prime-IoT".

5.2.2. PRIME-IoT de Rinicare

"PRIME-IoT" es el nombre que tiene el primer producto comercial basado en la pasarela desarrollada en el contexto del proyecto INTER-IoT y expuesta en esta tesis doctoral. [4] El prototipo fue desarrollado por "Rinicom Ltd" [5] en el contexto del proyecto y el producto final es comercializado por "Rinicare Ltd" [6] tras haber obtenido el sello CE de la Unión Europea [7].

"PRIME-IoT" es un sistema inalámbrico de monitorización de pacientes, que ayuda tanto a los pacientes como a los médicos. El conjunto de sensores inalámbricos de PRIME IoT (Figura 5.12) incluye un oxímetro de pulso SPO2, un estetoscopio inalámbrico, un termómetro timpánico, un tensiómetro inalámbrico y un electrocardiograma de 12 derivaciones.

[4] https://rinicom.com/inter-iot-epi-event-in-athens-greece/
[5] https://rinicom.com/
[6] https://rinicare.com/
[7] https://rinicare.com/rinicares-prime-hub-achieves-ce-marking/

Figura 5.12: Conjuntos de sensores de "PRIME-IoT"

El "Hub" de "PRIME-IoT" recoge los datos capturados por el conjunto de sensores. Se trata de un módulo independiente que luego puede transmitir estos datos a cualquier dispositivo compatible (Figura 5.13). Con una batería de larga duración y un diseño compacto, en el interior contiene la pasarela física sobre el hardware (en las fases de desarrollo y prototipado) de una "Raspberry Pi 3" (procesador ARM Cortex-A53 1.2GHz) [8]. La carcasa estanca tiene unas dimensiones de 64.2x133.6mm y una batería recargable de 3.7V 5.2Ah. La conectividad con los sensores es a través de Bluetooth 4.1 BLE y la interfaz de comunicación con la pasarela virtual es sobre Wi-Fi (802.11b/g/n 2.4GHz).

[8] https://www.raspberrypi.com/products/raspberry-pi-3-model-b/

Figura 5.13: Prototipo final del “Hub” “PRIME-IoT”

Tras recoger los datos de los sensores, la pasarela física envía los datos en crudo a la pasarela virtual, que realiza un pre-procesado de los datos y permite la interconexión con cualquier plataforma IoT y a su vez expone los datos a través del módulo API REST de la pasarela virtual, utilizada por una APP móvil y una interfaz Web para la consulta de los datos obtenidos por los sensores en tiempo real (Figura 5.14).

Figura 5.14: Interfaz web de “PRIME-IoT”

Durante las fases de desarrollo de “PRIME-IoT” en el contexto del proyecto INTER-IoT, se realizó una primera integración con la plataforma IoT “Fiware - Orion” [9] a través del su módulo de conexión de la pasarela virtual. En esta primera integración, y a través de reglas simples en la plataforma IoT, se establecen una serie de alarmas para encender o apagar su correspondiente luz LED en base a umbrales establecidos. Estas luces LED están conectadas a través de un controlador “Arduino Uno” [10] que a su vez se conecta la plataforma IoT “Orion” mediante la pasarela física/virtual y sus correspondientes módulos de conexión. Un esquema de este despliegue se puede ver en la Figura 5.15.

[9] https://github.com/telefonicaid/fiware-orion
[10] https://store.arduino.cc/products/arduino-uno-rev3

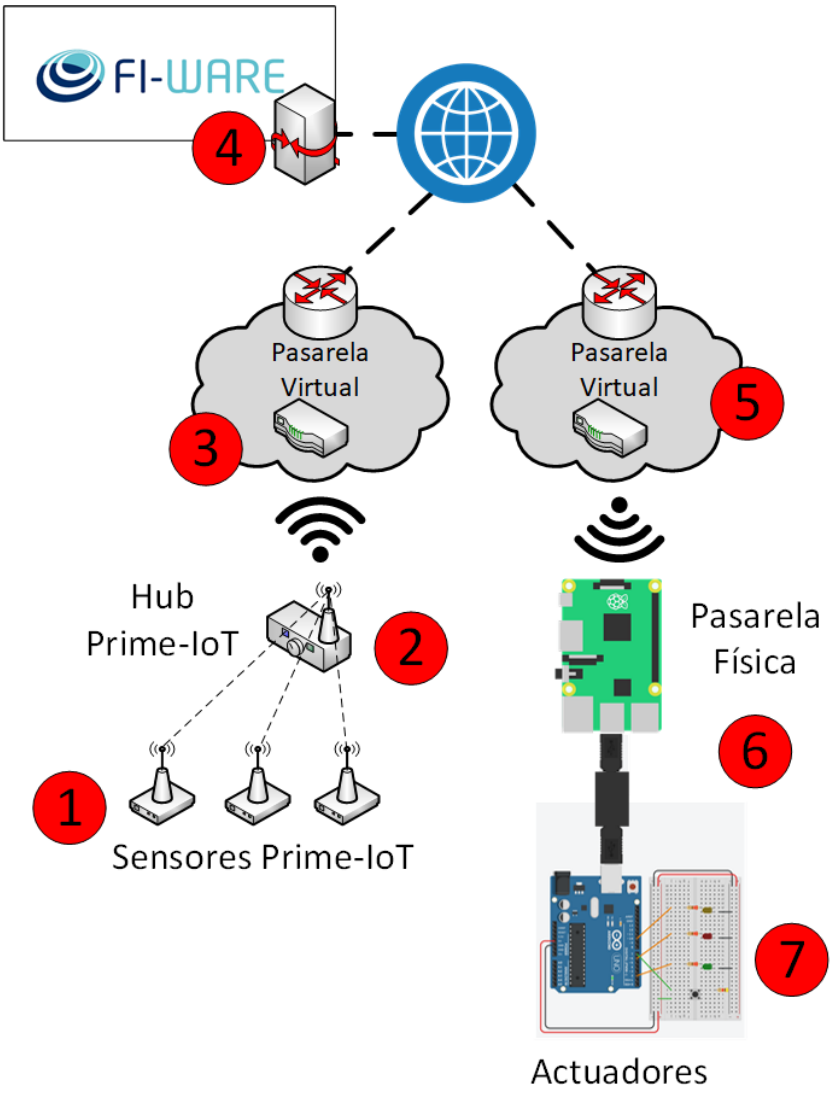

Figura 5.15: Esquema de la prueba de integración de "PRIME-IoT"

Los elementos del prototipo desplegado según aparecen en la Figura 5.15 son:

- **1.** *Sensores Prime-IoT*. Localizados en la WBAN. Capturan los datos del paciente. Los sensores son un termómetro timpánico y un tensiómetro, ambos inalámbricos.
- **2.** *Hub Prime-IoT*. Localizado en la LAN. Contiene una versión adaptada de la pasarela física con un módulo conector BLE para conectarse a los

sensores.

- **3.** *Pasarela Virtual*. Localizado en la MAN. Desplegados en el "Fog" o "Edge" de la red, es la representación virtual de la pasarela física. Tiene un módulo de plataforma IoT para conectarse a "Orion".

- **4.** *Plataforma IoT*. Localizado en la WAN, en este prototipo, desplegado en el "Cloud" de "Azure" [11]. Se establecen reglas sencillas para activar los actuadores en función de los valores de temperatura y tensión.

- **5.** *Pasarela Virtual*. Similar al desplegado en **3** pero siendo una representación virtual de la pasarela física **6**.

- **6.** *Pasarela Física*. En este caso, la pasarela física está desplegada sobre una "Raspberry Pi 3" con el módulo de conector serie de "Arduino Uno".

- **7.** *Actuadores*. Una serie de luces LED controladas a través de un dispositivo "Arduino Uno".

En la Figura 5.16 y la Figura 5.17 se puede ver una imagen del despliegue de este prototipo como parte de una demostración del proyecto INTER-IoT. Los sensores empleados se pueden ver en la Figura 5.16 y la luz verde en la Figura 5.17 indica unos valores de temperatura entre 36 y 37.2 grados Celsius.

[11] https://azure.microsoft.com/

Figura 5.16: Dispositivos de “PRIME-IoT” utilizados en la demostración

Figura 5.17: Ejemplo de funcionamiento de la integración de “PRIME-IoT”

Capítulo 6

Validación: 5GENESIS

La tecnología 5G ha entrado en la fase crucial de experimentación, y actualmente se enfrenta al reto de validar los KPI de la red 5G y verificar las tecnologías 5G con un enfoque integral.

Con este objetivo, un reto clave es integrar todos los resultados y tecnologías muy diversos de los proyectos de I+D de la Unión Europea, globales e internos (corporativos), para unificar la imagen de la 5G y desvelar el potencial de una plataforma 5G verdaderamente completa, de extremo a extremo, capaz de cumplir los objetivos de KPI definidos.

En este contexto, el principal objetivo de 5GENESIS será validar los KPI de 5G para varios casos de uso de 5G, tanto en montajes controlados como en eventos a gran escala. Esto se logrará reuniendo los resultados de un número considerable de proyectos de la Unión Europea, así como las actividades internas de I+D de los socios, con el fin de realizar una instalación 5G integrada de extremo a extremo.

La instalación 5GENESIS, en su conjunto, se encargará de:

- Implementar y verificar todas las evoluciones del estándar 5G, mediante un procedimiento iterativo de integración y pruebas.
- Incorporar una gran diversidad de tecnologías e innovaciones en cadena que abarcan todos los dominios, logrando una cobertura completa del panorama 5G.
- Unificar los elementos heterogéneos de la red física y virtual bajo un marco común de coordinación y apertura expuesto a los experimentadores de las industrias verticales y que permita la fragmentación de extremo a extremo y la automatización de los experimentos.

- Apoyar otros proyectos de experimentación, en particular los centrados en los mercados verticales.

Las cinco plataformas del dispositivo 5GENESIS, y sus principales características/orientación, son:

- **La plataforma de Atenas.** Una infraestructura de radio compartida habilitada para la computación de borde (gNBs y células pequeñas), con diferentes rangos y cobertura superpuesta que se apoyan en un núcleo habilitado para SDN/NFV, para mostrar la entrega segura de contenido y aplicaciones de baja latencia en grandes eventos públicos.
- **La Plataforma de Málaga.** Orquestación y gestión automatizada de diferentes segmentos de red en múltiples dominios, sobre la red central 5G NR y totalmente virtualizada para mostrar servicios de misión crítica en el laboratorio y en despliegues exteriores.
- **La plataforma de Limasol.** Interfaces de radio de diferentes características y capacidades, que combinan las comunicaciones terrestres y por satélite, integradas para mostrar la continuidad del servicio y el acceso ubicuo en zonas desatendidas.
- **La Plataforma de Surrey.** Múltiples tecnologías de acceso radioeléctrico que pueden soportar comunicaciones masivas de tipo máquina (mMTC), incluyendo 5G NR y NB-IoT, combinadas bajo una plataforma flexible de gestión de recursos radioeléctricos (RRM) y de compartición de espectro para mostrar servicios masivos de IoT.
- **La plataforma de Berlín.** Zonas ultradensas cubiertas por varios despliegues de red, que van desde nodos de interior hasta clústeres nómadas de exterior, coordinados a través de tecnologías avanzadas de "backhauling" para mostrar el suministro de servicios inmersivos.

6.1. Plataforma 5G de Limasol

6.1.1. Topología de la Plataforma 5G

La plataforma 5G de Limasol integra varias infraestructuras en la ciudad de Limasol, Chipre, para formar una instalación multi-radio interoperable, que combina las comunicaciones terrestres y por satélite con el objetivo final

de ampliar de forma eficiente la cobertura 5G a zonas desatendidas. Como se muestra en la Figura 6.1, las infraestructuras clave sobre las que se construye la plataforma son:

- **El banco de pruebas experimental de I+D de Primetel en Limasol.** Está situado en el edificio central de la empresa edificio central de la empresa, cerca del puerto de Limasol. El banco de pruebas actúa como nodo central de la plataforma: aloja, en su centro de datos privado, todos los componentes de gestión y servicios de la plataforma, y a su vez proporciona la interconexión con la pasarela satélite e Internet, así como a las demás plataformas de 5GENESIS.

- **La pasarela de satélites de Avanti en la estación terrestre de Makarios.** La estación terrestre de Avanti en Chipre se utiliza para proporcionar servicios "Satcom" gestionados a través de sus satélites "HYLAS 2" y "HYLAS 4" utilizando una plataforma de red de grado profesional que admite el transporte de tráfico celular, así como interfaces de gestión y APIs a través de su sistema de apoyo operativo (OSS) y plataforma de red (NMS).

- Una red remota, que constituye el "hotspot" móvil 5G. Se trata de una plataforma móvil/portátil, que se utiliza para conectarse al satélite (y/o a la red terrestre), alojar el equipo informático de computación de borde, así como los activos RAT para proporcionar una cobertura 5G localizada.

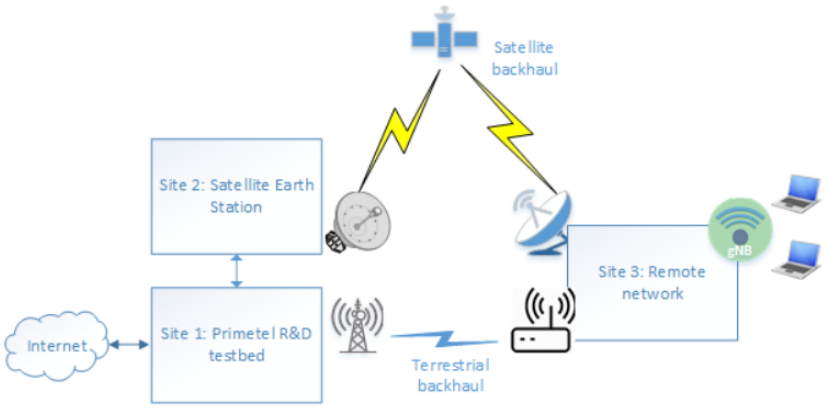

Figura 6.1: Topología del banco de pruebas de Limasol

6.1.2. Caso de uso: 5G bajo demanda e IoT en zonas rurales

Este caso de uso se centra en la provisión de conectividad en zonas desatendidas, como las rurales. Además, los servicios IoT se prestan en la parte superior de la infraestructura creada por la composición del enlace "Satcom" y el Backhaul terrestre.

Para este caso de uso, el objetivo principal es la integración de la red de acceso no- 3GPP en la infraestructura 5G. El enfoque principal adoptado para la implementación es que las pasarelas físicas y virtuales se conectarán directamente a través de la infraestructura 5G-NSA. Para integrar la conexión de la pasarela física en la infraestructura 5G el método seleccionado ha sido a través de la red de acceso 3GPP, utilizando la interfaz "S1", por lo que la pasarela debe soportar: Conectividad LTE y tener una pila IP".

El caso de uso se ha desarrollado en dos fases. En la primera fase, se integra la pasarela IoT Física-Virtual desarrollada en el contexto del proyecto INTER-IoT y expuesta en la presente tesis doctoral. Como ya sabemos, esta pasarela traduce la información proporcionada por los sensores a formatos de datos y protocolos comunes, por lo que durante la primera fase se pretende la demostración de un escenario sencillo de IoT en el que un sensor y un actuador estaban conectados a diferentes pasarelas físicas y se comunicaban a través de la infraestructura de Limasol.

En concreto, la solución estaba compuesta por varios componentes físicos (dispositivo compatible con LoRaWaN, dispositivo compatible con Arduino y pasarelas físicas) y virtuales (pasarela virtual y servicios IoT).

Ejemplos de los componentes utilizados para este caso de uso se pueden observar en la Figura 6.2, de izquierda a derecha: un dispositivo compatible con "Arduino" equipado con LEDs actuadores de diferentes colores utilizados para mostrar los cambios de temperatura, humedad, duración de la batería, etc. Una pasarela física con el módulo LoRa y la antena y un dispositivo LoRa personalizado con sensores de temperatura, presión y humedad.

Figura 6.2: Dispositivos empleados en el caso de uso de la plataforma de Limasol

Durante la primera fase, se pudieron desplegar el servicio IoT con dos pasarelas Físicas y dos pasarelas Virtuales, respectivamente conectados, junto con un dispositivo LoRa y un dispositivo "Arduino". El despliegue de la pasarela física se realizó correctamente, y la pasarela virtual se desplegó en dos ubicaciones (borde y núcleo). Sin embargo, como no había VIM instalado en el borde (todavía), el despliegue de las máquinas virtuales se hizo manualmente.

En la fase 2, no hubo modificaciones significativas en el hardware/software utilizado pero sí en la configuración y gestión del ciclo de vida de los componentes. Además, se incrementa el número de dispositivos, probando en el laboratorio diferentes tipos de dispositivos LoRa comerciales. También se integra el nodo MONROE para recoger información mejor y más precisa de los dispositivos IoT.

Para la segunda fase del caso de uso, se finaliza el soporte MANO extremo a extremo, se ha modificado y mejorado este despliegue lógico utilizando VNFs para implementar los servicios proporcionados por la pasarela virtual, permitiendo así su despliegue en tiempo real a través de la creación de un servicio de red con sus diferentes VNFs, siendo gestionado por el orquestador sobre la marcha.

Uno de los principales KPI que se medirá en el periodo de pruebas de la segunda fase será el tiempo de creación del servicio, es decir, el tiempo que transcurre hasta que se solicita el servicio y este se proporciona, incluyendo el despliegue del "slice", la creación del servicio de red y el despliegue, configuración y ejecución de la VNF. De este modo, para proporcionar servicios IoT bajo demanda, la pasarela IoT virtual ha sido encapsulada en una VNF para facilitar su manejo por los componentes de gestión y orquestación en la plataforma Limasol. Por lo tanto, la creación, el despliegue y las pruebas de un descriptor VNF para la pasarela IoT virtual y la creación de un descriptor

NS para desplegar el servicio por OSM son los principales logros de este caso de uso.

Capítulo 7

Validación: Otros casos de uso

7.1. INTER-HARE

El proyecto INTER-HARE pretende diseñar una nueva tecnología LPWAN lo suficientemente flexible como para abarcar de forma transparente tanto los dispositivos LPWAN como las denominadas redes de área local de baja potencia (LPLANs), garantizando al mismo tiempo la fiabilidad global del sistema. Se crea una red en forma de árbol de clústeres [111], en la que la LPWAN actúa no solo como colector de datos, sino también como red de retorno para varias LPLAN, como se muestra en la Figura 7.1.

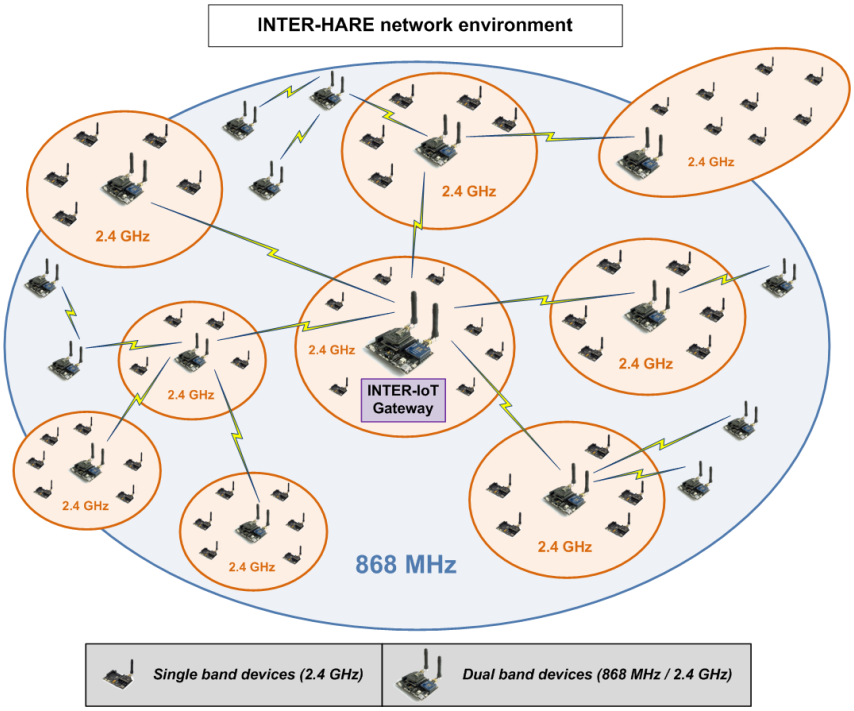

Figura 7.1: Red de INTER-HARE

La comunicación dentro de la LPWAN se basa en la pila de protocolos HARE [112], que garantiza la fiabilidad de la transmisión, el bajo consumo de energía mediante la adopción de la comunicación multisalto de enlace ascendente, la auto-organización y la resiliencia. La plataforma INTER-HARE se concibe como una evolución innovadora de la pila de protocolos HARE y puede considerarse como un multiprotocolo dinámico mediante la integración con la pasarela INTER-IoT. La arquitectura de la plataforma INTER-HARE se puede dividir en dos redes con diferentes propósitos: la red de transporte y la red de integración (como se puede ver en la Figura 7.2).

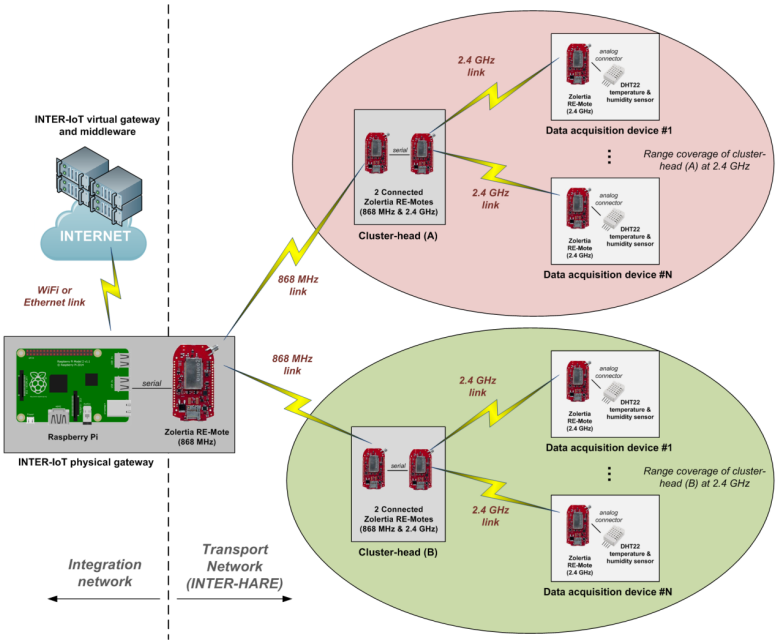

Figura 7.2: Arquitectura de INTER-HARE

La red de transporte incluye todas las infraestructuras internas responsables de recoger y transportar la información desde los dispositivos finales hasta la pasarela física. Esta infraestructura interna está formada por una única pasarela de protocolo HARE, varias cabezas de clúster (CH) y dispositivos de adquisición de datos (DAD). La red de integración está formada por la pasarela INTER-IoT, que permite el acceso a toda la pila IoT. La comunicación entre la Pasarela Física y la Pasarela de Protocolo HARE, se realiza con el protocolo de comunicación UART en serie. La pasarela INTER-IoT se considera, por tanto, el cerebro de la plataforma INTER-HARE y el único punto de contacto entre la red física y el resto del sistema INTER-IoT.

7.2. SENSHOOK

SensHook es un nodo IoT enfocado a la prevención y detección de mosquitos vectores de enfermedades. El nodo está compuesto por una trampa inteligente para mosquitos capaz de imitar el cuerpo humano (olor y respiración) y de contar automáticamente los mosquitos capturados, identificar el género y la especie. La información recogida por cada nodo se envía a un servidor. De este modo, SensHook pretende reducir los costes de inspección al tiempo que

mejora los programas de vigilancia, siendo la primera solución del mundo que combina la imitación humana con la información automática sobre plagas en su propuesta de valor. Esto permitirá a toda una nueva población de consumidores establecer programas de vigilancia que solo eran accesibles para aquellos con importantes recursos.

En este caso de uso, la integración se realiza a nivel de pasarela física. A pesar de que SensHook proporciona su propia plataforma para realizar comunicaciones y computación de bajo nivel, no se dispone de la capacidad de compartir la información de sus dispositivos con plataformas IoT. Por ello, con el objetivo de habilitarla, se realiza una conexión con la Pasarela Virtual, mediante el desarrollo de un conector específico integrado en la plataforma SensHook que entiende el protocolo de comunicación Físico-Virtual como se puede ver en la Figura 7.3.

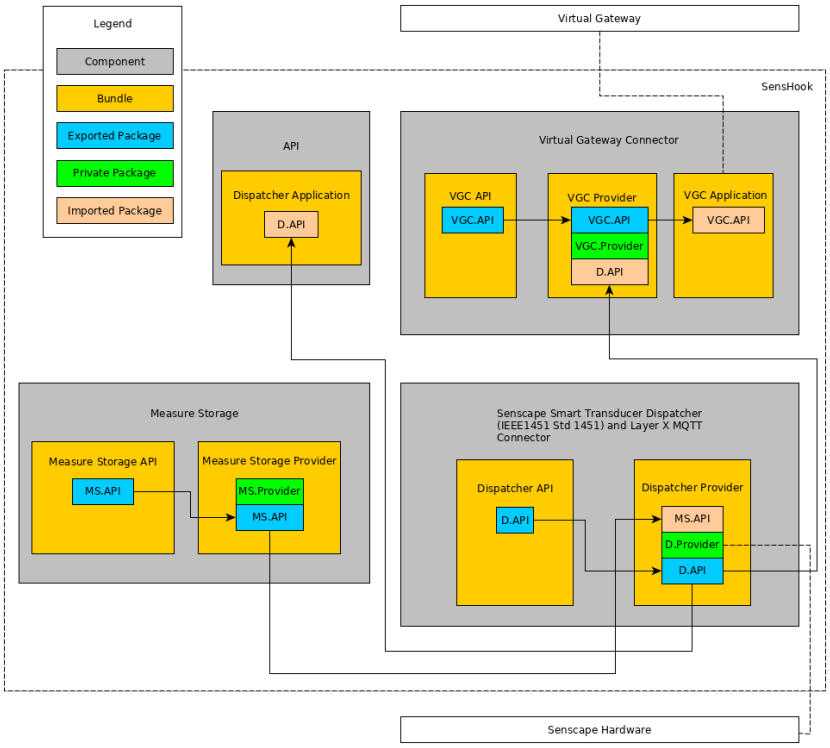

Figura 7.3: Arquitectura de SensHook

7.3. ACHILLES

ACHILLES es un proyecto que proporciona un control de acceso avanzado y una autenticación de punto final a los dispositivos conectados a la pasarela INTER-IoT. En general, estos dispositivos suelen estar limitados en cuanto a capacidad de almacenamiento, potencia, energía y capacidad de procesamiento, lo que presenta riesgos de seguridad en los despliegues de IoT. Dado que estos dispositivos no suelen ser capaces de realizar operaciones criptográficas complejas, la gestión de la seguridad se convierte en una tarea imposible desde la perspectiva del dispositivo. El proyecto ACHILLES supera estas limitaciones permitiendo la delegación de las operaciones de seguridad a un tercero que puede ser implementado por una entidad independiente de confianza, tal y como se representa en la figura 7.4.

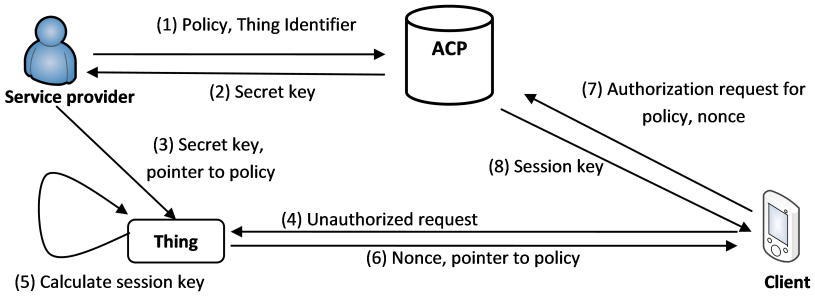

Figura 7.4: Arquitectura de Achilles

Capítulo 8

Conclusión y líneas de trabajo futuras

En esta tesis doctoral, se ha estudiado y analizado los retos que plantea el Internet de las Cosas y que siguen sin resolver, en concreto, en la capa de dispositivos. Se ha planteado una posible solución a la falta de interoperabilidad entre dispositivos y la gran cantidad de plataformas IoT heterogéneas existentes mediante la especificación de la arquitectura de una pasarela física/virtual. Esta arquitectura ha servido de base para una implementación de la pasarela modular basada en OSGI que hemos puesto a prueba en diferentes pilotos y casos de uso.

Durante el proceso de investigación y diseño, se han obtenido una serie de conclusiones que se exponen a continuación en la Sección 8.1. A continuación se detallará el alcance obtenido con los resultados de esta tesis doctoral en la Sección 8.2 y finalmente se detallan las líneas de trabajo futuras en la Sección 8.3.

8.1. Conclusiones finales

- Uno de los problemas más comunes a los que se enfrentan los despliegues de IoT es encontrar dispositivos (sensores, actuadores) capaces de realizar la(s) tarea(s) requerida(s) para los casos de uso que conducen al despliegue de una red IoT. En algunos casos, hay una gran variedad de sensores y en otros casos, hay pocos. La selección de los sensores apropiados para un caso de uso suele requerir que se trabaje con diferentes fabricantes y quizás con diferentes interfaces.

- Distintos dispositivos pueden tener diferentes mecanismos de configuración, como el uso de un formulario integrado en un servidor web, la modificación de un archivo de configuración almacenado en el sistema operativo, el uso de una API REST o el envío de comandos a través de un canal de comunicación. Esto representa una dificultad para las capas de dispositivo y "middleware", ya que este tipo de operaciones son difíciles de estandarizar, impidiendo que se incluyan estas características en las capas de interoperabilidad.

- La pasarela desarrollada contiene las características que se consideran lo suficientemente genéricas como para ser gestionadas en un único punto. Así, la configuración de los dispositivos se ha mantenido fuera del ámbito de la pasarela. Para realizar la configuración de los dispositivos se ha seguido la siguiente metodología:

  - Identificar el mecanismo de configuración de dispositivos específicos. Si la plataforma IoT lo hace automáticamente, el problema se resuelve automáticamente.
  - Si necesitan configuraciones específicas, comprobar si se pueden automatizar o no.
  - Si no se pueden automatizar, hay que realizar acciones específicas para configurarlos. Estas acciones deben ser realizadas por el integrador del sistema o el propietario del caso de uso (dependiendo del esquema de responsabilidad de la instalación de IoT).
  - Si se pueden automatizar, desarrollar los mecanismos e incluirlos en los scripts de inicialización.
  - Incluir los nuevos scripts en los contenedores de los módulos afectados según el enfoque de despliegue estándar.

  Este enfoque tiene la ventaja de que puede realizarse fácilmente con una pequeña complejidad en la mayoría de los casos. Además, normalmente solo hay que realizarlo una vez, ya que la mayoría de los sensores tienen una configuración persistente. La desventaja es que no se ha desarrollado una forma estandarizada de abordar el despliegue, por lo que se evita la automatización.

- Algunas plataformas de IoT pueden no seguir los estándares establecidos, o incluso no proporcionar ninguna API porque se tratan de soluciones cerradas. Se pueden definir a grandes rasgos la siguiente situación respecto a las APIs de las plataformas IoT:

  - La plataforma IoT no proporciona una API.
  - La plataforma IoT proporciona una API programática (como una interfaz "Java" o "C++").
  - La plataforma IoT proporciona un servicio web bien documentado y estandarizado (como REST o WSDL).
  - La plataforma IoT proporciona un servicio web personalizado (no estándar) sobre HTTP.
  - La plataforma IoT proporciona acceso a los datos a través de un "broker" de datos (como "RabbitMQ", "ApacheMQ", etc.) utilizando protocolos estándar (como por ejemplo AMQP, MQTT).
  - La plataforma IoT tiene la posibilidad de definir su propia interfaz para acceder a los datos (muchas veces utilizando tecnologías obsoletas).

- En los casos industriales, existen numerosas plataformas que se construyen inicialmente para resolver usos específicos. Algunas de ellas evolucionan y se convierten en una especie de plataforma IoT. Por ello, en la mayoría de estos casos, no siguen estándares, buenas prácticas o metodologías, lo que dificulta la adaptación de mecanismos de interoperabilidad como los desarrollados en INTER-IoT. INTER-IoT se basa con frecuencia en la idea de que para realizar tareas relacionadas con el IoT, los dispositivos y las plataformas deben realizar actividades similares que puedan generalizarse.

- En un sector industrial, como el portuario, en el que existe una enorme competencia entre las distintas empresas es difícil conseguir la interoperabilidad de los datos entre las empresas. Ahora mismo, solo comparten la documentación mínima exigida, por ejemplo, por un organismo público como las aduanas. Además, los sistemas no están preparados para compartir estos datos y exigirlo supone un esfuerzo económico y personal considerable, por lo que el beneficio debe ser mayor que los problemas ocasionados. Y en el caso de que exista un acuerdo para intercambiar algunos datos, las empresas quieren estar seguras de que los datos son accesibles para las personas autorizadas y se utilizan para el propósito definido.

- La complejidad del piloto portuario desarrollado en la Sección 5.1 no ha sido únicamente técnica. Existe un proceso burocrático complejo y un estudio minucioso de los requerimientos y el impacto generado:

    - Entrevista con los responsables de la empresa donde se explica el proyecto. En esta reunión tienes que presentar el proyecto y los objetivos. También puedes mostrar la arquitectura y los procesos de seguridad. Pero el tema principal debe ser los beneficios para la empresa. Tal vez sean necesarias otras reuniones con los técnicos de la empresa. Antes de comenzar cualquier integración es importante firmar un acuerdo de confidencialidad con la empresa en el que se describan los datos que se van a compartir, quién va a acceder a los datos y cómo se van a utilizar.
    - Como parte del punto anterior es necesario explicar los diferentes mecanismos de seguridad en los componentes desplegados para garantizar la privacidad de los datos descritos en el acuerdo de confidencialidad.
    - Por último, se puede iniciar la integración con los sistemas de la empresa. Es probable que la empresa no pueda destinar recursos a la integración, por lo que debe estar preparado para realizarla con el apoyo de los técnicos de la empresa.

- En el sector sanitario, la preservación de la privacidad es una de las principales preocupaciones de cualquier solución informática en este ámbito. Estas soluciones tratan con datos muy personales y sensibles y, en consecuencia, se trata de un entorno fuertemente regulado, desde el nuevo GDPR hasta las normativas locales. Estas imponen muchas restricciones a las soluciones tecnológicas que se utilizan, no solo técnicas, sino también de procedimiento y legales.

- Otro obstáculo en el entorno sanitario es que hasta ahora es difícil, al menos en algunos entornos sanitarios, encontrar soluciones informáticas integradas. Hay muchos subcampos (casi tantos como profesionales) en cualquier institución sanitaria. Puede haber soluciones informáticas para cada uno de ellos, e históricamente, tanto por la normativa mencionada como por otros muchos factores, estos sistemas no suelen ser, cuando menos, interoperables.

8.2. Alcance obtenido

A continuación se listan los resultados y el alcance que se ha obtenido durante el estudio de interoperabilidad entre dispositivos y el diseño e implementación de la pasarela IoT:

- Conclusiones y estudio teórico obtenido en cuanto a la interoperabilidad entre dispositivos. Los resultados se presentan en varias publicaciones listadas en la Sección 1.4.
- Especificación y diseño de una arquitectura modular para una pasarela dual física/virtual. Los resultados se presentan en el Capítulo 3.
- Implementación de una pasarela IoT que cumple con el diseño propuesto. Los resultados se presentan en el Capítulo 4. [1]
- Diseño e implementación de varias extensiones y módulos para la pasarela física. [2]
- Diseño e implementación de varias extensiones y módulos para la pasarela virtual. [3]
- Distintas empresas han mostrado interés para explotar los resultados obtenidos, y han creado diferentes módulos para sus dispositivos y plataformas, tal y como se ha mostrado en el piloto del puerto de Valencia en Sección 5.1, en el caso de "Inter-Hare" en la Sección 7.1 y en el caso de "Achilles" en la Sección 7.3.
- Otras entidades han utilizado la arquitectura y el diseño de esta pasarela modular como base para la creación de un producto. Como es el caso de "Prime-IoT" expuesto en la Subsección 5.2.2, o "Senshook" en la Sección 7.2.

8.3. Líneas de trabajo futuras

El trabajo realizado durante esta tesis doctoral, aunque ha sido extenso y se ha intentado abarcar muchos de los aspectos relacionados con la interoperabilidad entre dispositivos, se puede extender y completar en varias líneas de investigación diferentes. A continuación se describen algunas ideas que pueden ser la base para futuras investigaciones y posteriores desarrollos de la pasarela:

- Desarrollar más adaptadores de protocolos y redes de acceso. Aunque ya se han desarrollado algunos adaptadores para las redes de acceso y protocolos más comunes en el ámbito de IoT. Con el tiempo aparecerán nuevos

[1] https://github.com/enolgor/gateway
[2] https://github.com/enolgor/gateway-extensions-physical
[3] https://github.com/enolgor/gateway-extensions-virtual

protocolos de comunicación de corto y largo alcance, y de baja potencia, para los que sería interesante desarrollar el adaptador correspondiente.

- Desarrollar más adaptadores de plataformas IoT. Surgirán nuevas plataformas IoT con los cuales sería interesante conectar la pasarela virtual. En los últimos años, se están popularizando las soluciones de plataformas IoT en la nube bajo demanda, como las ofrecidas en "AWS" o "Azure". Sería interesante desarrollar módulos que se adapten a estas nuevas plataformas.

- Mejorar la usabilidad de la pasarela. Hay características que fueron planeadas, pero no se llegaron a implementar, puesto que eran requisitos que fueron descartados por su baja prioridad y mayor complejidad. Por ejemplo, la actualización automática y "Hot-Reload" o "Hot-Swap" de los módulos. Para conseguir un servicio de actualización completamente automatizado, se debería especificar en el esquema del módulo una "url" permanente y consultar de manera periódica nuevas versiones compatibles. Si existe una nueva versión, descargarla y reemplazarla automáticamente por el módulo desfasado sin interrumpir el servicio (es un problema con una complejidad muy alta).

- Mejorar las interfaces de interacción con la pasarela. Aunque existe el módulo de API REST, se pueden crear otros módulos que expongan otro tipo de APIs como "GraphQL", que ofrece una conexión a través de "WebSocket" para la lectura de datos en tiempo real y de manera asíncrona.

- Mejorar el descubrimiento de los dispositivos. Tal y como se ha expuesto en las lecciones aprendidas, no se ha desarrollado una forma estandarizada de abordar el despliegue de dispositivos, y la automatización es compleja. Se ha investigado el descubrimiento automatizado con el protocolo "UPnP", pero este protocolo no se utiliza en sensores y actuadores con bajas capacidades por lo que se podrían seguir nuevas líneas de investigación para resolver el problema de descubrimiento de sensores de bajas capacidades.

Referencias

[1] Giancarlo Fortino, Claudio Savaglio, Giandomenico Spezzano, and MengChu Zhou. Internet of things as system of systems: A review of methodologies, frameworks, platforms, and tools. *IEEE Transactions on Systems, Man and Cybernetics: Systems*, 51(1):223–236, 2021. URL: https://doi.org/10.1109/TSMC.2020.3042898, doi:10.1109/TSMC.2020.3042898.

[2] Ovidiu Vermesan and Peter Friess, editors. *Digitising the Industry Internet of Things Connecting the Physical, Digital and Virtual Worlds*. Riverpublishers, 2016. doi:https://doi.org/10.13052/rp-9788793379824.

[3] Michele Chincoli and Antonio Liotta. Transmission Power Control in WSNs: From Deterministic to Cognitive Methods. In Raffaele Gravina, Carlos E. Palau, Marco Manso, Antonio Liotta, and Giancarlo Fortino, editors, *Integration, Interconnection, and Interoperability of IoT Systems*, Internet of Things, pages 39–57. Springer International Publishing, Cham, 2018. URL: https://doi.org/10.1007/978-3-319-61300-0_3, doi:10.1007/978-3-319-61300-0_3.

[4] C. Savaglio, G. Fortino, and M. Zhou. Towards interoperable, cognitive and autonomic IoT systems: An agent-based approach. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pages 58–63, December 2016. doi:10.1109/WF-IoT.2016.7845459.

[5] Salvatore F. Pileggi., Carlos E. Palau., and Manuel Esteve. Building semantic sensor web: Knowledge and interoperability. In *Proceedings of the International Workshop on Semantic Sensor Web - Volume 1: SSW, (IC3K 2010)*, pages 15–22. INSTICC, SciTePress, 2010. doi:10.5220/0003112000150022.

[6] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys Tutorials*, 17(4):2347–2376, 2015. doi:10.1109/COMST.2015.2444095.

[7] Edward A. Lee. Cyber physical systems: Design challenges. In *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, pages 363–369, 2008. doi:10.1109/ISORC.2008.25.

[8] Siddharth Sridhar, Adam Hahn, and Manimaran Govindarasu. Cyber–physical system security for the electric power grid. *Proceedings of the IEEE*, 100(1):210–224, 2012. doi:10.1109/JPROC.2011.2165269.

[9] Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli. Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209, 2012. doi:10.1109/JPROC.2011.2161428.

[10] ITU-T Study Group 20. Requirements and functional architecture for the open ubiquitous sensor network service platform. Recommendation ITU-T Y.4402/F.747.4, International Telecommunication Union - Standardization Sector, Geneva, CH, 2013. URL: http://handle.itu.int/11.1002/1000/12051.

[11] ITU-T Study Group 20. Requirements for support of ubiquitous sensor network (usn) applications and services in the ngn environment. Recommendation ITU-T Y.4105/Y.2221, International Telecommunication Union - Standardization Sector, Geneva, CH, 2010. URL: http://handle.itu.int/11.1002/1000/10235.

[12] G. Fortino, C. Savaglio, C. E. Palau, J. Suarez, M. Ganzha, M. Paprzycki, M. Montesinos, A. Liotta, and M. Llop. Towards multi-layer interoperability of heterogeneous iot platforms: The inter-iot approach, 2016. doi:https://doi.org/10.13052/rp-9788793379824.

[13] Shancang Li, Li Da Xu, and Shanshan Zhao. The internet of things: a survey. *Information Systems Frontiers*, 17(2):243–259, 2015.

[14] ITU-T Study Group 20. Requirements and common characteristics of the iot identifier for the iot service. Recommendation ITU-T Y.4801/F.748.1, International Telecommunication Union - Standardization Sector, Geneva, CH, 2014. URL: http://handle.itu.int/11.1002/1000/12229.

[15] ITU-T Study Group 20. Terms and definitions for the internet of things. Recommendation ITU-T Y.4050/Y.2069, International Telecommunication Union - Standardization Sector, Geneva, CH, 2012. URL: http://handle.itu.int/11.1002/1000/11700.

[16] A. Broring, A. Zappa, O.Vermesan, K. Främling, A. Zaslavsky, R. Gonzalez-Usach, P. Szmeja, C. Palau, M. Jacoby, I. P. Zarko, S. Soursos, C. Schmitt, M. Plociennik, S. Krco, S. Georgoulas, I. Larizgoitia, N. Gligoric, R. García-Castro, F. Serena, V. Orav. *Advancing IoT Platform Interoperability*. River Publishers, The Nederlands, 2018.

[17] Ioannis Chatzigiannakis, Henning Hasemann, Marcel Karnstedt, Oliver Kleine, Alexander Kröller, Myriam Leggieri, Dennis Pfisterer, Kay Römer, and Cuong Truong. True self-configuration for the iot. In *2012 3rd IEEE International Conference on the Internet of Things*, pages 9–15, 2012. doi:10.1109/IOT.2012.6402298.

[18] Martin Bauer, Mathieu Boussard, Nicola Bui, Francois Carrez, Christine (SIEMENS, Jourik (ALUBE, Carsten (SAP, Stefan Meissner, Andreas IML, Alexis Olivereau, Matthias (SAP, Walewski Joachim, Julinda Stefa, and Alexander Salinas. Internet of things - architecture iot-a deliverable d1.3 – updated reference model for iot v1.5, 06 2012.

[19] DP World / The Economist Intelligence Unit. A turning point: The potential role of ict innovations in ports and logistics, 2015.

[20] R. Giffinger, C. Fertner, H. Kramar, R. Kalasek, N. Pichler-Milanovic, and E. Meijers. Smart cities - ranking of european medium-sized cities, 2007.

[21] R. Nicholson. Smart cities: Proving ground for the intelligent economy, 2010.

[22] Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi. Internet of things for smart cities. *IEEE Internet of Things Journal*, 1(1):22–32, 2014. doi:10.1109/JIOT.2014.2306328.

[23] et al. B. Celtinkaya, R.Cuthbertson. Sustainable supply chain management, practical ideas for moving towards best practice, 2011.

[24] S. M. Riazul Islam, Daehan Kwak, MD. Humaun Kabir, Mahmud Hossain, and Kyung-Sup Kwak. The internet of things for health care: A comprehensive survey. *IEEE Access*, 3:678–708, 2015. doi : 10.1109/ACCESS.2015.2437951.

[25] YIN Yuehong, Yan Zeng, Xing Chen, and Yuanjie Fan. The internet of things in healthcare: An overview. *Journal of Industrial Information Integration*, 1:3–13, 2016.

[26] Diana Yacchirema, David Sarabia-Jácome, Carlos E. Palau, and Manuel Esteve. System for monitoring and supporting the treatment of sleep apnea using iot and big data. *Pervasive and Mobile Computing*, 50:25–40, October 2018. URL: https://linkinghub.elsevier.com/retrieve/pii/S1574119217306259, doi:10.1016/j.pmcj.2018.07.007.

[27] *IEEE Standard for Low-Rate Wireless Networks*, 2020. doi:10.1109/IEEESTD.2020.9144691.

[28] *IEEE Standard for Medium Frequency (less than 12 MHz) Power Line Communications for Smart Grid Applications*, 2018. doi:10.1109/IEEESTD.2018.8360785.

[29] *IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments*, 2010. doi:10.1109/IEEESTD.2010.5514475.

[30] *IEEE Standard for Wireless Access in Vehicular Environments (WAVE)–Identifiers*, 2019. doi:10.1109/IEEESTD.2019.8877516.

[31] *IEEE Health informatics–Point-of-care medical device communication Part 10207: Domain Information and Service Model for Service-Oriented Point-of-Care Medical Device Communication*, 2018. doi:10.1109/IEEESTD.2018.8299598.

[32] *IEEE Standard for Smart Energy Profile Application Protocol*, 2018. doi:10.1109/IEEESTD.2018.8608044.

[33] *IEEE Standard for a Smart Transducer Interface for Sensors and Actuators - Network Capable Application Processor Information Model*, 2000. doi:10.1109/IEEESTD.2000.91313.

[34] *IEEE Standard for Sensor Performance Parameter Definitions*, 2018. doi:10.1109/IEEESTD.2018.8277147.

[35] Zach Shelby, Klaus Hartke, and Carsten Bormann. The Constrained Application Protocol (CoAP). RFC 7252, June 2014. URL: https://rfc-editor.org/rfc/rfc7252.txt, doi:10.17487/RFC7252.

[36] Gabriel Montenegro, Jonathan Huii, David Culler, and Nandakishore Kushalnagar. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944, September 2007. URL: https://rfc-editor.org/rfc/rfc4944.txt, doi:10.17487/RFC4944.

[37] Roger Alexander, Anders Brandt, JP Vasseur, Jonathan Huii, Kris Pister, Pascal Thubert, P Levis, Rene Struik, Richard Kelsey, and Tim Winter. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550, March 2012. URL: https://rfc-editor.org/rfc/rfc6550.txt, doi:10.17487/RFC6550.

[38] ISO Central Secretary. Internet of things (iot) — reference architecture. Standard ISO/IEC 30141:2018, International Organization for Standardization, Geneva, CH, 2018. URL: https://www.iso.org/standard/65695.html.

[39] ISO Central Secretary. Information technology — internet of things (iot) — vocabulary. Standard ISO/IEC 20924:2018, International Organization for Standardization, Geneva, CH, 2018. URL: https://www.iso.org/standard/69470.html.

[40] ISO Central Secretary. Internet of things (iot) — interoperability for iot systems — part 1: Framework. Standard ISO/IEC 21823-1:2019, International Organization for Standardization, Geneva, CH, 2019. URL: https://www.iso.org/standard/71885.html.

[41] ISO Central Secretary. Internet of things (iot) — interoperability for iot systems — part 2: Transport interoperability. Standard ISO/IEC 21823-2:2020, International Organization for Standardization, Geneva, CH, 2020. URL: https://www.iso.org/standard/80986.html.

[42] ISO Central Secretary. Internet of things (iot) - interoperability for iot systems - part 3: Semantic interoperability (pre release version). Standard ISO/IEC 21823-3:2021, International Organization for Standardization, Geneva, CH, 2021. URL: https://webstore.iec.ch/publication/69229.

[43] ISO Central Secretary. Information technology — sensor networks: Sensor network reference architecture (snra) — part 1: General overview and requirements. Standard ISO/IEC 29182-1:2013, International Organization for Standardization, Geneva, CH, 2013. URL: https://www.iso.org/standard/45261.html.

[44] ISO Central Secretary. Information technology — sensor networks: Sensor network reference architecture (snra) — part 2: Vocabulary and terminology. Standard ISO/IEC 29182-2:2013, International Organization for Standardization, Geneva, CH, 2013. URL: https://www.iso.org/standard/57091.html.

[45] ISO Central Secretary. Information technology — sensor networks: Sensor network reference architecture (snra) — part 3: Reference architecture views. Standard ISO/IEC 29182-3:2014, International Organization for Standardization, Geneva, CH, 2014. URL: https://www.iso.org/standard/57092.html.

[46] ISO Central Secretary. Information technology — sensor networks: Sensor network reference architecture (snra) — part 4: Entity models. Standard ISO/IEC 29182-4:2013, International Organization for Standardization, Geneva, CH, 2013. URL: https://www.iso.org/standard/57094.html.

[47] ISO Central Secretary. nformation technology — sensor networks: Sensor network reference architecture (snra) — part 5: Interface definitions. Standard ISO/IEC 29182-5:2013, International Organization for Standardization, Geneva, CH, 2013. URL: https://www.iso.org/standard/57095.html.

[48] ISO Central Secretary. Information technology — sensor networks: Sensor network reference architecture (snra) — part 6: Applications. Standard ISO/IEC 29182-6:2014, International Organization for Standardization, Geneva, CH, 2014. URL: https://www.iso.org/standard/57096.html.

[49] ISO Central Secretary. Information technology — sensor networks: Sensor network reference architecture (snra) — part 7: Interoperability guidelines. Standard ISO/IEC 29182-7:2015, International Organization for Standardization, Geneva, CH, 2015. URL: https://www.iso.org/standard/57097.html.

[50] ISO Central Secretary. Information technology — message queuing telemetry transport (mqtt) v3.1.1. Standard ISO/IEC 20922:2016, International Organization for Standardization, Geneva, CH, 2016. URL: https://www.iso.org/standard/69466.html.

[51] ISO Central Secretary. Information technology — security techniques — privacy framework. Standard ISO/IEC 29100:2011, International

Organization for Standardization, Geneva, CH, 2011. URL: https://www.iso.org/standard/45123.html.

[52] ISO Central Secretary. Information technology — security techniques — privacy architecture framework. Standard ISO/IEC 29101:2018, International Organization for Standardization, Geneva, CH, 2018. URL: https://www.iso.org/standard/75293.html.

[53] ISO Central Secretary. Information technology — security techniques — guidelines for privacy impact assessment. Standard ISO/IEC 29134:2017, International Organization for Standardization, Geneva, CH, 2017. URL: https://www.iso.org/standard/62289.html.

[54] ISO Central Secretary. Information technology — security techniques — code of practice for personally identifiable information protection. Standard ISO/IEC 29151:2017, International Organization for Standardization, Geneva, CH, 2017. URL: https://www.iso.org/standard/62726.html.

[55] ISO Central Secretary. Information technology — security techniques — code of practice for protection of personally identifiable information (pii) in public clouds acting as pii processors. Standard ISO/IEC 27018:2019, International Organization for Standardization, Geneva, CH, 2019. URL: https://www.iso.org/standard/76559.html.

[56] ITU-T Study Group 20. Overview of the internet of things. Recommendation ITU-T Y.4000/Y.2060, International Telecommunication Union - Standardization Sector, Geneva, CH, 2012. URL: http://handle.itu.int/11.1002/1000/11559.

[57] ITU-T Study Group 20. Common requirements of the internet of things. Recommendation ITU-T Y.4100/Y.2066, International Telecommunication Union - Standardization Sector, Geneva, CH, 2014. URL: http://handle.itu.int/11.1002/1000/12169.

[58] ITU-T Study Group 20. Common requirements for internet of things (iot) applications. Recommendation ITU-T Y.4103/F.748.0, International Telecommunication Union - Standardization Sector, Geneva, CH, 2014. URL: http://handle.itu.int/11.1002/1000/12228.

[59] ITU-T Study Group 20. Functional framework and capabilities of the internet of things. Recommendation ITU-T Y.4401/Y.2068, International Telecommunication Union - Standardization Sector, Geneva, CH, 2015. URL: http://handle.itu.int/11.1002/1000/12419.

[60] ITU-T Study Group 20. Functional requirements and architecture of the next generation network for support of ubiquitous sensor network applications and services. Recommendation ITU-T Y.4403/Y.2026, International Telecommunication Union - Standardization Sector, Geneva, CH, 2012. URL: http://handle.itu.int/11.1002/1000/11696.

[61] ITU-T Study Group 20. Service description and requirements for ubiquitous sensor network middleware. Recommendation ITU-T Y.4104/F.744, International Telecommunication Union - Standardization Sector, Geneva, CH, 2009. URL: http://handle.itu.int/11.1002/1000/10616.

[62] ITU-T Study Group 20. Sensor control networks and related applications in a next generation network environment. Recommendation ITU-T Y.4250/Y.2222, International Telecommunication Union - Standardization Sector, Geneva, CH, 2013. URL: http://handle.itu.int/11.1002/1000/11912.

[63] ITU-T Study Group 20. Snmp-based sensor network management framework. Recommendation ITU-T Y.4701/H.641, International Telecommunication Union - Standardization Sector, Geneva, CH, 2012. URL: http://handle.itu.int/11.1002/1000/11546.

[64] ITU-T Study Group 20. Framework of constrained device networking in the iot environments. Recommendation ITU-T Y.4451, International Telecommunication Union - Standardization Sector, Geneva, CH, 2016. URL: http://handle.itu.int/11.1002/1000/13026.

[65] ITU-T Study Group 20. Architectural reference models of devices for internet of things applications. Recommendation ITU-T Y.4460, International Telecommunication Union - Standardization Sector, Geneva, CH, 2019. URL: http://handle.itu.int/11.1002/1000/13921.

[66] ITU-T Study Group 20. Requirements and use cases for universal communication module of mobile iot devices. Recommendation ITU-T Y.4210, International Telecommunication Union - Standardization Sector, Geneva, CH, 2020. URL: http://handle.itu.int/11.1002/1000/14371.

[67] ITU-T Study Group 20. Lightweight intelligent software framework for internet of things devices. Recommendation ITU-T Y.4475, International Telecommunication Union - Standardization Sector, Geneva, CH, 2020. URL: http://handle.itu.int/11.1002/1000/14377.

[68] ITU-T Study Group 20. Common requirements and capabilities of device management in the internet of things. Recommendation ITU-T Y.4702, International Telecommunication Union - Standardization Sector, Geneva, CH, 2016. URL: http://handle.itu.int/11.1002/1000/12780.

[69] ITU-T Study Group 20. Requirements of the network for the internet of things. Recommendation ITU-T Y.4113, International Telecommunication Union - Standardization Sector, Geneva, CH, 2016. URL: http://handle.itu.int/11.1002/1000/13025.

[70] ITU-T Study Group 20. Common requirements and capabilities of a gateway for internet of things applications. Recommendation ITU-T Y.4101/Y.2067, International Telecommunication Union - Standardization Sector, Geneva, CH, 2017. URL: http://handle.itu.int/11.1002/1000/13384.

[71] ITU-T Study Group 20. Architecture of the internet of things based on next generation network evolution. Recommendation ITU-T Y.4416, International Telecommunication Union - Standardization Sector, Geneva, CH, 2018. URL: http://handle.itu.int/11.1002/1000/13638.

[72] ITU-T Study Group 20. Gateway functional architecture for internet of things applications. Recommendation ITU-T Y.4418, International Telecommunication Union - Standardization Sector, Geneva, CH, 2018. URL: http://handle.itu.int/11.1002/1000/13640.

[73] ITU-T Study Group 20. Security capabilities supporting safety of the internet of things. Recommendation ITU-T Y.4806, International Telecommunication Union - Standardization Sector, Geneva, CH, 2017. URL: http://handle.itu.int/11.1002/1000/13391.

[74] ITU-T Study Group 20. Accessibility requirements for the internet of things applications and services. Recommendation ITU-T Y.4204, International Telecommunication Union - Standardization Sector, Geneva, CH, 2019. URL: http://handle.itu.int/11.1002/1000/13858.

[75] ITU-T Study Group 20. Framework of delegation service for internet of things devices. Recommendation ITU-T Y.4463, International Telecommunication Union - Standardization Sector, Geneva, CH, 2020. URL: http://handle.itu.int/11.1002/1000/14166.

[76] ITU-T Study Group 20. Requirements of the plug and play capability of the internet of things. Recommendation ITU-T Y.4112/Y.2077, In-

ternational Telecommunication Union - Standardization Sector, Geneva, CH, 2016. URL: http://handle.itu.int/11.1002/1000/12706.

[77] ITU-T Study Group 20. Internet of things requirements for support of edge computing. Recommendation ITU-T Y.4208, International Telecommunication Union - Standardization Sector, Geneva, CH, 2020. URL: http://handle.itu.int/11.1002/1000/14162.

[78] John Soldatos, Nikos Kefalakis, Manfred Hauswirth, Martin Serrano, Jean-Paul Calbimonte, Mehdi Riahi, Karl Aberer, Prem Prakash Jayaraman, Arkady Zaslavsky, Ivana Podnar Žarko, Lea Skorin-Kapov, and Reinhard Herzog. Openiot: Open source internet-of-things in the cloud. In Ivana Podnar Žarko, Krešimir Pripužić, and Martin Serrano, editors, *Interoperability and Open-Source Solutions for the Internet of Things*, pages 13–25, Cham, 2015. Springer International Publishing.

[79] G. Fortino, C. Savaglio, C.E. Palau, J.S. de Puga, M. Ghanza, M. Paprzycki, M. Montesinos, A. Liotta, and M. Llop. Towards multilayer interoperability of heterogeneous iot platforms: The inter-iot approach. *Internet of Things*, 0(9783319612997):199–232, 2018. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85027051038&doi=10.1007%2f978-3-319-61300-0_10&partnerID=40&md5=94c2df7b8c2c571253637931831a4f01, doi:10.1007/978-3-319-61300-0_10.

[80] D4.2 - Final Reference IoT Platform Meta-Architecture and Meta Data Model. INTER-IoT H2020 project, 2017. URL: https://inter-iot.eu/deliverables.

[81] D3.1 - Methods for Interoperability and Integration v.1. INTER-IoT H2020 project, 2016. URL: https://inter-iot.eu/deliverables.

[82] Martin Bauer, Mathieu Boussard, Nicola Bui, Francois Carrez, Christine (SIEMENS, Jourik (ALUBE, Carsten (SAP, Stefan Meissner, Andreas IML, Alexis Olivereau, Matthias (SAP, Walewski Joachim, Julinda Stefa, and Alexander Salinas. Internet of things – architecture iot-a deliverable d1.5 – final architectural reference model for the iot v3.0, 07 2013.

[83] Martin Bauer, Nicola Bui, Christine Jardak, and Andreas Nettsträter. *The IoT ARM Reference Manual*, pages 213–236. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013. URL: https://doi.org/10.1007/978-3-642-40403-0_9, doi:10.1007/978-3-642-40403-0_9.

[84] D. C. Yacchirema, M. Esteve, and C. E. Palau. Design and implementation of a Gateway for Pervasive Smart Environments. In *2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pages 4454–4459, October 2016. doi:10.1109/SMC.2016.7844933.

[85] Gianluca Aloi, Giancarlo Fortino, Raffaele Gravina, Pasquale Pace, and Giuseppe Caliciuri. Edge computing-enabled body area networks. In *2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pages 349–353, Krakow, May 2018. IEEE. URL: https://ieeexplore.ieee.org/document/8418095/, doi:10.1109/WAINA.2018.00110.

[86] Decebal Constantin Mocanu. On the synergy of network science and artificial intelligence. In *Proceedings of the Twenty-Fifth International Joint Conference on Artificial Intelligence*, IJCAI'16, pages 4020–4021, New York, New York, USA, July 2016. AAAI Press.

[87] Matija Cankar, Eneko Olivares Gorriti, Matevž Markovič, and Flavio Fuart. Fog and Cloud in the Transportation, Marine and eHealth Domains. In Dora B. Heras, Luc Bougé, Gabriele Mencagli, Emmanuel Jeannot, Rizos Sakellariou, Rosa M. Badia, Jorge G. Barbosa, Laura Ricci, Stephen L. Scott, Stefan Lankes, and Josef Weidendorfer, editors, *Euro-Par 2017: Parallel Processing Workshops*, volume 10659, pages 292–303. Springer International Publishing, Cham, 2018. Series Title: Lecture Notes in Computer Science. URL: http://link.springer.com/10.1007/978-3-319-75178-8_24, doi:10.1007/978-3-319-75178-8_24.

[88] Andreu Belsa, David Sarabia-Jacome, Carlos E. Palau, and Manuel Esteve. Flow-based programming interoperability solution for iot platform applications. In *2018 IEEE International Conference on Cloud Engineering (IC2E)*, pages 304–309, Orlando, FL, April 2018. IEEE. URL: https://ieeexplore.ieee.org/document/8360346/, doi:10.1109/IC2E.2018.00059.

[89] M. Ganzha, M. Paprzycki, W. Pawlowski, P. Szmeja, and K. Wasielewska. Semantic technologies for the iot - an inter-iot perspective. In *2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pages 271–276, April 2016. doi:10.1109/IoTDI.2015.22.

[90] Maria Ganzha, Marcin Paprzycki, Wiesław Pawłowski, Paweł Szmeja, and Katarzyna Wasielewska. Semantic interoperability in the Internet

of Things: An overview from the INTER-IoT perspective. *Journal of Network and Computer Applications*, 81:111–124, March 2017. URL: https://linkinghub.elsevier.com/retrieve/pii/S1084804516301618, doi:10.1016/j.jnca.2016.08.007.

[91] James Robertson and Suzanne Robertson. Volere requirements specification template. 01 2000.

[92] Eduardo Miranda. Time boxing planning: buffered moscow rules. *ACM SIGSOFT Software Engineering Notes*, 36(6):1–5, November 2011. URL: https://dl.acm.org/doi/10.1145/2047414.2047428, doi:10.1145/2047414.2047428.

[93] K. S. Ahmad, N. Ahmad, H. Tahir, and S. Khan. Fuzzy moscow: A fuzzy based moscow method for the prioritization of software requirements. In *2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, pages 433–437, 2017. doi:10.1109/ICICICT1.2017.8342602.

[94] D2.3 - INTER-IoT Requirements and Business Analysis. INTER-IoT H2020 project, 2017. URL: https://inter-iot.eu/deliverables.

[95] D6.3 - Use case oriented pilots final version. INTER-IoT H2020 project, 2018. URL: https://inter-iot.eu/deliverables.

[96] D2.1 - Requirements of the Facility. 5Genesis H2020 project, 2018. URL: https://5genesis.eu/deliverables/.

[97] D4.8 - The Limassol Platform. 5Genesis H2020 project, 2020. URL: https://5genesis.eu/deliverables/.

[98] G. Fortino, C. Palau, A. Guerrieri, N. Cuppens, F. Cuppens, H. Chaouchi, and A.Gabillon, editors. *Interoperability, Safety and Security in IoT - Third International Conference, InterIoT 2017, and Fourth International Conference, SaSeIot 2017, Proceedings*, volume 242 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Springer, 2018. URL: https://doi.org/10.1007/978-3-319-93797-7, doi:10.1007/978-3-319-93797-7.

[99] D3.3 - Methods for Interoperability and Integration Final Version. INTER-IoT H2020 project, 2018. URL: https://inter-iot.eu/deliverables.

[100] D7.1 - Evaluation plan. INTER-IoT H2020 project, 2018. URL: https://inter-iot.eu/deliverables.

[101] D7.2 - Technical Evaluation and Assessment report. INTER-IoT H2020 project, 2018. URL: https://inter-iot.eu/deliverables.

[102] D7.3 - Final evaluation report. INTER-IoT H2020 project, 2018. URL: https://inter-iot.eu/deliverables.

[103] Richard Suzman, John R Beard, Ties Boerma, and Somnath Chatterji. Health in an ageing world—what do we know? *The Lancet*, 385(9967):484–486, 2015.

[104] Giancarlo Fortino and Paolo Trunfio, editors. *Internet of Things Based on Smart Objects, Technology, Middleware and Applications*. Springer, 2014. URL: https://doi.org/10.1007/978-3-319-00491-4, doi:10.1007/978-3-319-00491-4.

[105] G. Fortino, R. Gravina, and S. Galzarano. *Wearable computing: From modeling to implementation of Wearable systems and body sensor networks*. 2018. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85050645987&doi=10.1002%2f9781119078807&partnerID=40&md5=f52b34e82ab2095887e8ec2b87bf18d4, doi:10.1002/9781119078807.

[106] R. Gravina and G. Fortino. Wearable body sensor networks: state-of-the-art and research directions. *IEEE Sensors Journal*, 2020. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85098772315&doi=10.1109%2fJSEN.2020.3044447&partnerID=40&md5=8b533a237ae94de1eda2b332c91fd778, doi:10.1109/JSEN.2020.3044447.

[107] Randall D Cebul, James B Rebitzer, Lowell J Taylor, and Mark E Votruba. Organizational fragmentation and care quality in the us healthcare system. *Journal of Economic Perspectives*, 22(4):93–113, 2008.

[108] Olaronke Iroju, Abimbola Soriyan, Ishaya Gambo, and Janet Olaleke. Interoperability in healthcare: benefits, challenges and resolutions. *International Journal of Innovation and Applied Studies*, 3(1):262–270, 2013.

[109] D. Yacchirema, R. Gonzalez-Usach, M. Esteve, and C. E. Palau. Interoperability of iot platforms applied to the transport and logistics domain. In *Transport Arena Research Conference 2018*, Austria, 2018. TRA.

[110] P. Giménez, B. Molína, C. E. Palau, and M. Esteve. Swe simulation and testing for the iot. In *2013 IEEE International Conference on Systems, Man, and Cybernetics*, pages 356–361, 2013. doi:10.1109/SMC.2013.67.

[111] Liviu Octavian Varga. *Réseaux de capteurs sans fils multi-sauts à récupération d'énergie : routage et couche liaison de bas rapport cyclique*. Theses, Université Grenoble Alpes, December 2015. URL: https://tel.archives-ouvertes.fr/tel-01348307.

[112] Toni Adame Vázquez, Sergio Barrachina-Muñoz, Boris Bellalta, and Albert Bel. HARE: Supporting Efficient Uplink Multi-Hop Communications in Self-Organizing LPWANs. *Sensors*, 18(2):115, jan 2018. URL: http://www.mdpi.com/1424-8220/18/1/115, doi:10.3390/s18010115.

Anexos

Anexo A

Protocolo de comunicación interno de la pasarela

A.1. Descripción de la pasarela

```
{
  "type": "gateway-info",
  "payload": {
    "UUID": "fca50b99-d8f2-4a1b-b335-9a68ddd122b2",
    "extensions": [
      "eu.interiot.gateway.extension.physical.device-controller.simulator",
      "eu.interiot.gateway.extension.common.console",
      "eu.interiot.gateway.extension.physical.device-controller.panstamp",
      "eu.interiot.gateway.extension.physical.device-controller.arduino-uno"
    ],
    "version": "0.4.2",
    "specVersion": "0.4.2",
    "build": "20181029160000",
    "type": "PHYSICAL",
    "vendor": "inter-iot",
    "specVendor": "inter-iot"
  },
  "timestamp": "2019-01-08T09:31:21.894Z",
  "uuid": "fd222fe6-b03b-42f1-9c96-d8550a71caad",
  "awaitResponse": true
}
```

A.2. Registro de dispositivo

```
{
   "type":"register-device",
   "payload":{
      "device":{
         "id":"ABCDE2",
         "type":"arduino",
         "description":"light, temperature and humidity sensor
             bme280",
         "deviceIOs":{
            "light":{
               "type":"ACTUATOR",
               "attribute":{
                  "name":"light",
                  "type":"BOOLEAN"
               },
               "config":{

               }
            },
            "temperature":{
               "type":"SENSOR",
               "attribute":{
                  "name":"temperature",
                  "type":"FLOAT"
               },
               "config":{

               }
            },
            "humidity":{
               "type":"SENSOR",
               "attribute":{
                  "name":"humidity",
                  "type":"INTEGER"
               },
               "config":{

               }
            }
         },
         "controller":"arduino",
```

```
        "config":{
           "rate":"60",
           "rateUnit":"SECONDS"
        }
     }
  },
  "timestamp":"2019-01-08T09:31:21.950Z",
  "uuid":"1d834f3a-1a56-4114-9815-bb02cb32434e",
  "awaitResponse":false
}
```

A.3. Medida de un sensor

```
{
  "type":"measurement",
  "payload":{
     "deviceId":"ABCDE2",
     "measurement":{
        "timestamp":1546939895682,
        "data":[
           {
              "attribute":{
                 "name":"temperature",
                 "type":"FLOAT"
              },
              "value":31.885914134795684,
              "timestamp":1546939895682
           },
           {
              "attribute":{
                 "name":"humidity",
                 "type":"INTEGER"
              },
              "value":85,
              "timestamp":1546939895682
           }
        ]
     }
  },
  "timestamp":"2019-01-08T09:31:35.682Z",
```

```
   "uuid":"54171c59-9728-4238-a103-6157f48a25d0",
   "awaitResponse":false
}
```

A.4. Acción a un actuador

```
{
   "type":"action",
   "payload":{
      "deviceId":"ABCDE3",
      "action":{
         "timestamp":0,
         "data":[
            {
               "attribute":{
                  "name":"light",
                  "type":"BOOLEAN"
               },
               "value":"true"
            }
         ]
      }
   },
   "timestamp":"2019-01-08T09:31:22.357Z",
   "uuid":"db883d04-775d-44c9-9bfc-7567b73925bb",
   "awaitResponse":false
}
```

Anexo B

Archivos de configuración

B.1. Configuración de la pasarela física

```
eu.interiot.gateway.core.common.cache.path: ./cache
eu.interiot.gateway.core.physical.commons-physical.autodeploy: true
eu.interiot.gateway.core.physical.commons-physical.autodeploy.folder:
    ./devices
eu.interiot.gateway.core.physical.commons-physical.reconnect.delay:
    2000
eu.interiot.gateway.core.physical.commons-physical.reconnect.maxdelay:
    60000
eu.interiot.gateway.core.common.connector.host: localhost
eu.interiot.gateway.core.common.connector.port: 8829
eu.interiot.gateway.core.common.connector.log: true
eu.interiot.gateway.core.common.connector.ssl: true
eu.interiot.gateway.core.common.connector.ssl.trustedCertDir: ./certs
```

B.2. Configuración de un dispositivo

```
 {
  "type": "panstamp",
  "controller": "panstamp",
  "description": "PanStamp device",
  "config": {
     "serialPort": "/dev/ttyUSB0",
```

```
      "serialBaudRate": "38400",
      "manufacturer": 1,
      "product": 1,
      "address": 1
   },
   "device_io": [
      {
         "type":"sensor",
         "attr_name":"temperature",
         "attr_type":"float"
      },
      {
         "type": "sensor",
         "attr_name": "humidity",
         "attr_type": "float"
      },
      {
         "type": "sensor",
         "attr_name": "voltage",
         "attr_type": "float"
      }
   ]
}
```

B.3. Configuración de la pasarela virtual

```
eu.interiot.gateway.core.common.cache.path: ./cache
eu.interiot.gateway.core.common.connector.host: 0.0.0.0
eu.interiot.gateway.core.common.connector.port: 8829
eu.interiot.gateway.core.common.connector.log: true
eu.interiot.gateway.core.common.connector.ssl: true
eu.interiot.gateway.core.common.connector.ssl.pemCertFile:
    ./certs/default-cert.pem
eu.interiot.gateway.core.common.connector.ssl.pemKeyFile:
    ./certs/default-key.pem

extension.eu.interiot.gateway.extension.virtual.api-engine.enabled:
    true
eu.interiot.gateway.extension.virtual.api-engine.ssl: false
eu.interiot.gateway.extension.virtual.api-engine.port: 8080
```

```
eu.interiot.gateway.extension.virtual.api-engine.host: 0.0.0.0
```

B.4. Configuración de una regla

```
{
  "statement": {
    "name": "st01",
    "description": "Statement 01",
    "statement": "select * from Measurement where
        data.attribute.name = 'temperature' and cast(data.value,
        double) >= 0"
  },
  "execution": {
    "name": "ex01",
    "description": "Execution 01",
    "execution": "var action = new Action(); action.addData(new
        ActionData('red-led', AttributeType.BOOLEAN, true));
        context.sendAction('ar001', action);"
  }
}
```

Anexo C

Extensiones de la pasarela

C.1. Esquema de descripción de una extensión

```
<?xml version="1.0"?>
<xs:schema attributeFormDefault="unqualified"
   elementFormDefault="qualified"
       targetNamespace="https://docs.inter-iot.eu/schemas/gateway/0.3.0"
   xmlns="https://docs.inter-iot.eu/schemas/gateway/0.3.0"
       xmlns:xs="http://www.w3.org/2001/XMLSchema">
   <xs:element name="extension">
      <xs:complexType>
        <xs:all minOccurs="1" maxOccurs="1">
          <xs:element type="xs:string" name="name" />
          <xs:element type="xs:string" name="version" />
          <xs:element type="xs:string" name="vendor" />
          <xs:element type="xs:string" name="specVersion" />
          <xs:element name="category">
            <xs:simpleType>
              <xs:restriction base="xs:string">
                <xs:enumeration value="controller" />
                <xs:enumeration value="physical" />
                <xs:enumeration value="virtual" />
                <xs:enumeration value="generic" />
              </xs:restriction>
            </xs:simpleType>
          </xs:element>
          <xs:element type="xs:anyURI" name="url" />
          <xs:element type="xs:string" name="description" />
```

```
        </xs:all>
      </xs:complexType>
   </xs:element>
</xs:schema>
```

C.2. Ejemplo de extensión de un controlador

```
<?xml version="1.0"?>
<extension>
  <name>arduino-uno</name>
  <version>0.4.1</version>
  <vendor>INTER-IoT</vendor>
  <specVersion>0.4.1</specVersion>
  <category>controller</category>
  <url>
    http://nexus.inter-iot.eu/repository/maven-snapshots/eu/interiot/gateway
    /extension/physical/device-controller.arduino-uno/0.4.1-SNAPSHOT
    /device-controller.arduino-uno-0.4.1-20180528.144630-2-dist.zip
  </url>
  <description>Controller for Arduino Uno devices</description>
</extension>
```

Anexo D

Otros

D.1. "Dockerfile" de la pasarela virtual

```
FROM docker.inter-iot.eu/alpine-jdk8:162b12
MAINTAINER Eneko Olivares <enolgor@teleco.upv.es>
COPY / /vgateway/
WORKDIR "/vgateway"
RUN chmod +x bin/run
ENTRYPOINT ["bin/run"]
EXPOSE 8080 8829
```

D.2. Comandos de generación de certificados

Generación de clave y petición de firma:

```
openssl req -new -newkey rsa:4096 -keyout default-key.pem -out
    default-cert.csr \
-subj '/CN=localhost' -nodes
```

Firma del certificado con un certificado raíz de confianza:

```
openssl x509 -req -in default-cert.csr -CA default-ca-cert.pem
    -CAkey default-ca-key.pem \
-CAcreateserial -out default-cert.pem -days 365
```