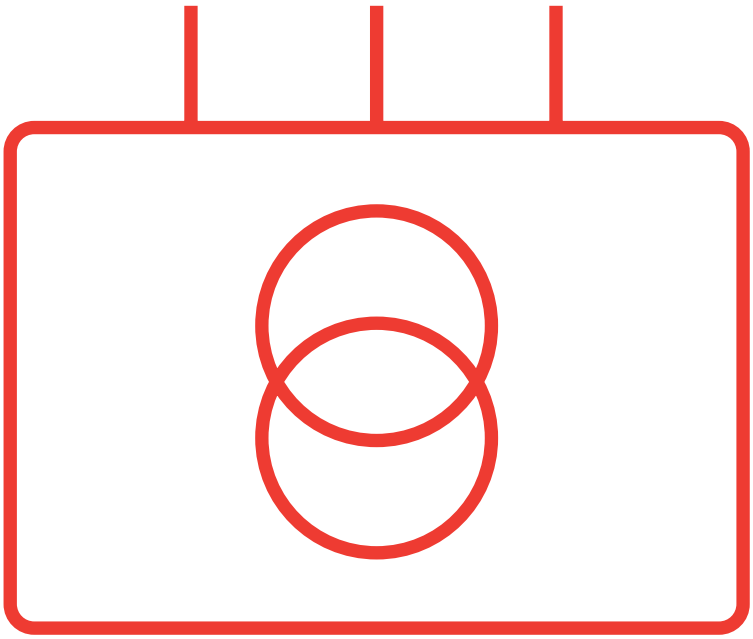
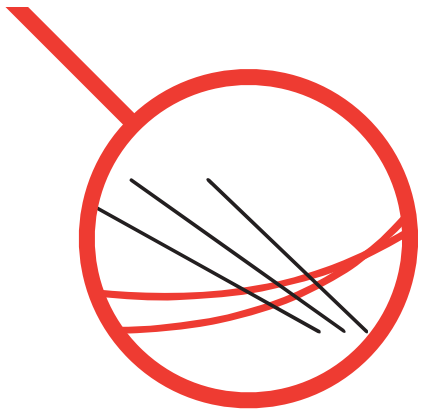


CENTRO DE TRANSFORMACIÓN INTELIGENTE:
FUNDAMENTOS PARA DISTRIBUCIÓN DE FUNCIONALIDADES



GRUPO DE TRABAJO
DE CENTRO DE
TRANSFORMACION
INTELIGENTE

30/06/2021

FutuRed

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN
AGENCIA ESTATAL DE INVESTIGACIÓN

Contenido

1. GLOSARIO ACRÓNIMOS 8

2. ALCANCE Y OBJETIVOS 10

2.1. Objetivos 10

2.2. Resultados a obtener 11

2.3. Guía del documento 11

3. ORGANIZACIÓN 12

3.1. Grupo Redacción 12

3.2. Grupo Edición 13

3.3. Grupo Revisión 14

4. ESTADO DEL ARTE Y TECNOLOGÍAS DEL SASCTI 15

4.1. Panorama general de Smart Grid en los centros de transformación 15

4.2. Características generales de un CT 16

4.3. Arquitectura de la Smart Grid y normas aplicables 17

4.4. Centro de transformación actual 17

4.4.1. Celdas de media tensión 18

4.4.2. Protecciones 18

4.4.3. Grados de automatización 19

4.4.4. Transformador de distribución 21

4.4.5. Cuadro de distribución 22

4.4.6. Interconexiones 22

4.4.7. Conexión del circuito de puesta a tierra 23

4.4.8. Retos a futuro para el CT 23

4.5. Tecnología de las plataformas de procesamiento distribuido. 24

4.5.1. Plataformas de procesamiento distribuído: Capas /Componentes. 25

4.5.2. El encapsulamiento y la gestión de las funciones distribuidas. 26

4.5.3. La distribución de la inteligencia. Edge, Core y Cloud. 34

4.5.4. Gestión y orquestación. 36

4.5.5. Comparativa plataformas. 39

4.6. Telecomunicaciones 54

4.6.1. Comunicaciones entre el SASCTI y Sistemas Centrales 54

4.6.2. Comunicaciones del SASCTI 55

4.6.3. Comunicaciones entre CTIs del mismo anillo de MT 60

4.7. Ciberseguridad 60

4.7.1. Normativas Ciberseguridad 62

4.7.2. Ciberseguridad en entornos distribuidos Edge-Cloud 64

4.8. Normativa y estándares de referencia aplicables ... 65
4.8.1. IEC TC57: "Power system management and associated information exchange" 68
4.8.2. CIM ... 69
4.8.3. El paradigma IEC 61850 ... 70
4.8.4. Protocolos de comunicaciones en entornos IoT. ... 72
5. REQUISITOS BASE: SASCTI ... 74
5.1. Arquitectura SASCTI. ... 74
5.2. Requerimientos arquitectura SW SASCTI ... 78
5.2.1. Servicios core de gestión/administración Edge. ... 79
5.2.2. Virtualización y Encapsulamiento de funciones ... 80
5.2.3. Gestión y Administración. ... 87
5.2.4. Ciberseguridad ... 90
5.2.5. Sistema Operativo. ... 93
6. METODOLOGÍA DE DEFINICION DE CASOS DE USO E INTEGRACIÓN ... 95
6.1. El proceso ... 95
6.2. Arquitectura de Referencia (AR). ... 99
6.2.1. Nuestro Sistema: SASCTI ... 99
6.2.2. Elementos y relaciones desde un punto de vista Funcional ... 101
6.2.3. Caso de Uso Base (CUB) ... 104
6.3. Casos de uso funcionales (CUFs) sobre el sistema SASCTI ... 105
6.4. Mapeo en el Modelo SGAM ... 108
7. FUNCIONALIDADES ... 114
7.1. Introducción ... 114
7.1.1. Metodología de desarrollo de casos de uso. ... 115
7.2. Concentrador de datos ... 116
7.3. Supervisión Avanzada de Baja Tensión ... 117
7.4. Predicción de red eléctrica ... 118
7.4.1. Simulación flujos de carga y estimación de estados ... 119
7.4.2. Balances de pérdidas técnicas y no técnicas. ... 119
7.4.3. Saturación del transformador ... 120
7.4.4. Análisis de capacidad de red ... 120
7.4.5. Mapa de tensiones ... 120
7.4.6. Equilibrado de fases en una línea de BT ... 120
7.5. Gestión de activos ... 121
7.5.1. Inventariado y estimación de vida útil ... 121
7.5.2. Autodiagnóstico ... 121
7.5.3. Reinício remoto equipos ... 122

7.6. Supervisión de Red 123
7.6.1. Detección anomalías BT 123
7.6.2. Listados de SPV sospechosos (anomalías de tensiones o conectividad) 127
7.6.3. Listados de CNs sospechosos (anomalías de tensiones) 128
7.6.4. Detección fallos de aislamiento 128
7.6.5. Detección anomalías MT 128
7.7. Analítica de Red 129
7.7.1. Topología-Conectividad Contadores 129
7.7.2. Detección y prevención de fraude 131
7.7.3. Detección ruidos PRIME BT 134
7.8. Control de Red 135
7.8.1. Regulación en carga transformador MT/BT 135
7.8.2. CBT Automatizado 137
7.9. Gestión de la energía – flexibilidad 138
7.9.1. Gestión local de la demanda 139
7.9.2. Potencia de generación flexible 140
7.9.3. Flexibilidad distribuida 140
7.9.4. Integración sistemas de almacenamiento 140
7.10. Movilidad, operación y mantenimiento de Red 140
7.10.1. Acceso a datos inventario de manera local 140
7.10.2. Realidad aumentada 141
7.11. Ciberseguridad 141
7.12. Seguridad y sostenibilidad 141
7.12.1. Control de acceso inteligente 142
7.12.2. Detección anomalías CT 142
7.12.3. Tratamiento de imagen 142
8. PROYECTOS PILOTOS EN CURSO Y POC 143
8.1. Introducción proyectos pilotos y PoC incorporados 143
8.2. Descripción proyectos pilotos y PoC incorporados 145
8.2.1. Pilotos E4S Alliance - SSP 145
8.2.2. Proyecto MiDE4S (Minsait-iDE) 147
8.2.3. CT4.0 UFD 154
8.2.4. Grupo Cuerva 156
8.2.5. DISCOVERER (2018) - Ormazabal 158
8.2.6. HOLISTICA (2019) - Ormazabal 162
8.2.7. POC100 E-distribución 164

8.3. Comparativa tecnologías entre proyectos 167
8.4. Conclusiones – ámbitos de colaboración 167
9. REFERENCIAS 168
ANEXOS 170
ANEXO I - Plantilla para desarrollo de Casos de Uso (DISCERN) 170
Description of the use case 170
Diagrams of use case 171
Technical details 171
Information Exchanged 173
Requirements (optional) 173
Common terms and definitions 173
Custom information (optional) 173
ANEXO II – Marco de referencia para la implementación de interoperabilidad entre aplicaciones en el Edge 174
A,II.1 WOT 174
A.II.2 MQTT 177
A.II.3 RESTful API 178

PRÓLOGO

El sector energético está viviendo una profunda y extensa transformación por dos causas principales. La primera, resumida en la conocida Transición Energética que tiene su origen en la lucha contra el cambio climático y que contribuye a la necesaria sostenibilidad de la vida en nuestro planeta. La segunda, en una transformación digital que afecta a todas las áreas y sectores de la Economía y de la Sociedad.

La Transición Energética cuenta con muchos factores y acciones orientadas fundamentalmente a la descarbonización, tanto desde el lado de la producción como desde el lado del consumo de energía y cuyo resultado se dirige a una intensa y masiva electrificación en el conjunto energético que permita un uso máximo de fuentes renovables, para el que es imprescindible el concepto de recursos energéticos distribuidos. Precisamente en esa distribución de recursos energéticos, incluyendo producción, almacenamiento, gestión de la demanda y movilidad eléctrica, adquieren especial relevancia las redes eléctricas de distribución.

Por otra parte, la transformación digital es un fenómeno tecnológico y social. Tecnológico, porque aprovecha los extraordinarios avances en las tecnologías de información y telecomunicaciones en general, obtenidos en las últimas décadas y que, además, se caracterizan por una enorme y rapidísima evolución. Y es social porque es la Sociedad quien se ha convertido en su conjunto en un actor principal de su adopción y demanda.

La combinación de ambas causas, la transición energética y la digitalización, resultan en una necesaria transformación del sector de la energía, en el que el eléctrico adquiere un papel primordial, adquiriendo las redes de distribución un protagonismo renovado configurándose como el activo principal de la descentralización para la descarbonización. La conexión de los recursos energéticos distribuidos y su operación eficiente va a exigir, y de hecho ya lo está haciendo, un grado de digitalización de las redes de distribución, convirtiéndolas en redes inteligentes, que permitirá, por un lado, la necesaria interacción operativa con dichos recursos, pero también extender esa supervisión y actuación en tiempo real que no necesitaban cuando se desarrollaron.

Dentro de este desafío, es necesario plantear la evolución del marco de control y monitorización actualmente basado en un Centro de Control Central hacia una arquitectura de administración, basada en dispositivos inteligentes distribuidos, capaces de ejecutar algoritmos de control dirigidos a una amplia gama de actuaciones, como la operación ante eventos complejos o el cumplimiento de reglas técnicas y comerciales. Con ello, se podrán ofrecer nuevos servicios a los usuarios finales, optimizando el uso de los recursos energéticos y obteniendo un conocimiento significativo sobre las tendencias de generación y demanda en estos entornos más dinámicos y volátiles.

En este contexto, el Centro de Transformación eléctrico se constituye en un punto estratégico de la red eléctrica de distribución, de manera que su digitalización lo convierta en el Centro de Transformación inteligente que permita conseguir todos esos objetivos. Confirmando su extraordinaria utilidad eléctrica, bien contrastada a lo largo de los más de cien años de su empleo y evolución, y aprovechando la economía de escala que ofrece la topología europea (número de clientes alimentados desde dicho centro), resulta necesario y muy oportuno en este momento definir la inteligencia a incorporar mediante un sistema informático y de telecomunicaciones que pueda aprovechar la multiplicación de capacidad de procesamiento que brinda ese concepto de control distribuido. El número y dispersión de Centros de Transformación en un sistema eléctrico como el español obliga a imponer desde el inicio de la etapa de diseño de ese sistema dos requisitos imprescindibles: la interoperabilidad entre dispositivos, que asegure el uso de diferentes suministradores de soluciones, evitando así el empleo de soluciones propietarias y, por supuesto, la ciberseguridad que debe proteger adecuadamente al conjunto del sistema ante los ataques que previsiblemente se producirán.

Admitiendo la necesidad de emplear los activos ya en operación y permitiendo la necesaria coexistencia entre sistemas de procesamiento centralizados y descentralizados, este sistema de información distribuida ayudará a procesar, resolver y entregar la gran cantidad de datos necesarios para administrar y controlar de manera efectiva el sistema de energía eléctrica. Además, podrá respaldar la toma de decisiones inmediata, casi en tiempo real, basada en la información disponible localmente y también brindará tendencias apropiadas y otra información procesable a otros sistemas de información. Por último, deberá aprovechar el grado de digitalización ya iniciado con la instalación de la medida inteligente, éste ya masivo y completado en España, complementada con diverso contenido y extensión, de actuaciones como la supervisión avanzada, automatización, etc.

El presente documento tiene por objeto constituirse como la referencia básica para la posterior elaboración de la especificación técnica con la que cada empresa distribuidora planteará sus licitaciones de equipos y servicios necesarios para dotar de inteligencia a sus centros de transformación. La participación en su redacción de todas las empresas distribuidoras y numerosos suministradores españoles, en el marco de FUTURED, dentro del grupo de trabajo creado a tal efecto, asegura el empleo de una terminología común de arquitectura, dispositivos y subsistemas así como un entendimiento común de las funciones exigidas a esa inteligencia. Todo ello contribuirá a un desarrollo e implantación ordenado y eficiente de este elemento imprescindible en nuestro futuro como lo es el Centro de Transformación inteligente, apoyando sin duda a la industria española, que ya ha conseguido una posición muy relevante en el campo internacional, en su innovación y negocio.

Enrique García García
Director Red Digital.
i-DE (Grupo Iberdrola)

Miguel Ángel Sánchez Fornié
Investigador afiliado del IIT
Director del Master en Smart Grids ICAI
Universidad Pontificia Comillas

1. GLOSARIO ACRÓNIMOS

ADM	Active Demand Management (Gestión activa de la demanda)
AMI	Advanced Metering Infrastructure
ANM	Active Network Management
API	Application Programming Interface (Interfaz de programación de aplicaciones)
AR	Arquitectura de Referencia
BT	Baja Tensión
CBT	Cuadro de Baja Tensión
CD	Concentrador de Datos
CEN	Comité Europeo de Normalización
CENELEC	Comité Europeo de Normalización Electrotécnica
CGP	Caja general de protección
CIM	Common Information Model
CN	Contador Inteligente de Telegestión
COSEM	COmpanion Specification for Energy Metering
CT	Centro de Transformación
CTi	Centro de Transformación Inteligente
CU	Caso de Uso
CUB	Caso de Uso Base
CUF	Caso de Uso Funcional
DER	Distributed Energy Resource
DERMS	Distributed Energy Resource Management System
DLMS	Device Language Message Specification
DMS	Distribution Management System
DPF	Detector de Paso de Falta
DSO	Distribution System Operator
EE	Estimación de Estado
ETSI	European Telecommunications Standards Institute
FO	Fibra Óptica
FC	Flujo de Cargas
HDLC	High Level Data Link Control
HW	Hardware
IA	Interruptor Automático
ICM	Modelo de Comunicación Interna
IaaS	Infrastructure as a Service
IEC	International Electrotechnical Commission
IoT	Internet of Things
IP	Internet Protocol
IT (TI)	Information Technology

JSON	JavaScript Object Notation
LBT	Línea de Baja Tensión
M2M	Machine TO Machine
MAC	Media Access Control
MDM	Meter Data Management
MQTT	Message Queuing Telemetry Transport
NEC	Nodo Edge Computing
OT (TO)	Operation Technology
OLTC	On Load Tap Changer
PaaS	Platform as a Service
PLC	Power Line Communication
PRIME	PoweRline Intelligent Metering Evolution
RAT	Reglamento de instalaciones eléctricas de Alta Tensión
RESTful	Web Services that conform to Representational State Transfer
RMU	Ring Main Unit
RTU	Remote Terminal Unit
SaaS	Software as a Service
SABT	Supervisión Avanzada de BT
SAI	Sistema de Alimentación Ininterrumpida
SASCTI	Sistema Avanzado de Supervisión y Control del CT Inteligente
SASCTI-M	SASCTI Manager
SASCTI-E	SASCTI Edge
SCADA	Supervisory Control and Data Acquisition
SF6	Hexafluoruro de azufre
SGAM	Smart Grid Architecture Model
SGCG	Smart Grid Coordination Group
SIEM	Gestión de sucesos e información de seguridad
SOAP	Simple Object Access Protocol
STG-DC	Sistema de Telegestión (Central system). También conocido como AMM en inglés.
SW	Software
TI	Transformador de Intensidad
TSO	Transmission System Operador (Operador del sistema de Transporte)
UCMR	Use Case Management Repository
VE	Vehiculo Eléctrico
WS	Web Services
WAN	Wide Area Network
WOT-A	Web of Things Architecture
W3C	World Wide Web Consortium
XML	eXtensible Markup Language

2. ALCANCE Y OBJETIVOS

Actualmente, según se va estableciendo en la normativa del Sector Eléctrico, las Empresas Distribuidoras deberán afrontar los nuevos escenarios que se irán desencadenando en la transición energética, donde el consumidor pasa a jugar un papel fundamental en la red, por lo que el siguiente paso será aplicar soluciones tecnológicas que permitan a las empresas afrontar estos nuevos escenarios funcionales a los que se pretende llegar.

Este documento tiene como objeto, servir de referencia básica para la elaboración de las especificaciones necesarias en su caso, de un centro de transformación inteligente (CTi) estándar, mediante la definición de una arquitectura de referencia y las funcionalidades asociadas a los casos de uso. En concreto, la inteligencia necesaria en el CT para convertirlo en CTi se obtendrá a través de unos nuevos dispositivos que integren los sistemas de medición y los elementos encargados de recoger lecturas e información de los elementos conectados a la red de BT/MT, empaquetando los datos y enviando la información necesaria a los sistemas seleccionados por las empresas eléctricas para monitorizar y operar la red.

El centro de transformación es el nexo de unión de los sistemas centrales con los contadores inteligentes y el punto más cercano de interacción con el cliente.

Su función ya va más allá de la gestión de contadores: monitoriza la red de media y baja tensión.

El incremento de la electrificación de la transición energética (más renovables, VE, ...) imponen nuevas dinámicas en la red de media y baja tensión (mecanismos de flexibilidad). El sistema de control del CT está en primera línea de esta gestión.

El CT, junto con sus sistemas de control y gestión, debe evolucionar para dar respuesta al nuevo escenario: variación dinámica de tensiones, regulación en carga de transformadores, uso de baterías/almacenamiento, etc).

Actualmente la gestión del CT se basa en tecnologías y arquitecturas centralizadas de monitorización y control, si bien, la distribución de inteligencia con el uso de las oportunidades que brinda el Edge Computing, ofrece unas ventajas a tener muy en cuenta a la hora de recomendar la arquitectura a adoptar.

Por otra parte, en el ámbito de las redes eléctricas, cada vez es mayor la sensorización y monitorización de todos los niveles de la red, lo que eleva la cantidad de información disponible en varios órdenes de magnitud. Además, la disponibilidad de mayor información del sistema y de mayores capacidades de computación, permiten la realización de algoritmos de control más avanzados, que en el ámbito eléctrico deben ejecutarse en algunos casos en cuestión de microsegundos para asegurar la integridad de la red. Dichas necesidades hacen muy discutible el seguir funcionando con el modelo centralizado, siendo muy beneficioso en este entorno la disposición de equipos de procesamiento en los sistemas periféricos para la ejecución de dichos algoritmos y preprocesamiento de los datos in situ para cumplir los límites de funcionamiento adecuados.

2.1. Objetivos

Como resultado de este trabajo se busca unificar criterios y método para especificar la arquitectura y funcionalidad del nuevo Centro de Transformación Inteligente, que permitirá abordar los retos indicados anteriormente.

Este Centro de Transformación Inteligente tendrá como objetivo transformar la gestión de la red de distribución en cuatro dimensiones fundamentales:

- **Simplificar y flexibilizar la gestión de la red,** a la vez que permite multiplicar por varios ordenes de magnitud el número de activos y puntos gestionados en tiempo real por el operador (DSO), habilitando la respuesta en tiempo real con una tecnología más flexible al cambio.
- **Optimizar la explotación y mantenimiento de toda la infraestructura desplegada en el SASCTI** (dispositivos, actuadores, equipos de comunicación, aplicaciones ...) maximizando las posibilidades de gestión remota y minimizando el coste global de operación y mantenimiento,
- **Minimizar los tiempos de reacción habilitando una respuesta más autónoma y dinámica de la red.** La gestión centralizada

actual de la información requiere como mínimo tiempos del orden de un minuto para recibir la información y otro minuto para actuar. La gestión distribuida permite dar respuesta a casos de uso que requieren tiempos de análisis y respuesta muchos más cortos, como pueda ser el control de la tensión en el SASCTI, la identificación y protección de la infraestructura y/o los clientes ante fallos inminentes o la coordinación de recursos energéticos distribuidos para evitar superar la capacidad máxima de la red.

- **Dotar de la seguridad necesaria**, tanto de la ciberseguridad como de la seguridad física, protegiendo al SASCTI y toda la red eléctrica y de telecontrol de nuevas amenazas.

2.2. Resultados a obtener

Como resultado se tendrá una propuesta consensuada de metodología para elaborar la especificación técnica del Centro de Transformación Inteligente la cual incluya:

1. Situación actual:

- Revisión del estado de los actuales CT Inteligentes y de los Sistemas Avanzados de Supervisión y Control del CT Inteligente (SASCTI). Estado del arte nacional e internacional.

2. Funciones de soporte: identificación y descripción de especificaciones funcionales

- Revisión del escenario a futuro para las especificaciones de los Sistemas Avanzado de Supervisión y Control del CT Inteligente (SASCTI).

3. Definición de arquitectura del CT

- Arquitectura HW /SW, protocolos de comunicación y telecomunicaciones
- Especificaciones

4. Identificación de pilotos en marcha

- Pilotos en DSO España
- Proyectos en DSO europeos
- Pilotos en otras DSO de interés

2.3. Guía del documento

El documento de acuerdo con la metodología de casos de uso (capítulo 6), identifica las especificaciones técnicas que el futuro SASCTI deberá cumplir para desarrollar las posibles funcionalidades distribuidas y locales del SASCTI definidas en el capítulo 7, todo dentro de un marco de referencia arquitectónico y tecnológico analizado en el capítulo 4 y desarrollado en forma de requerimientos básicos en el capítulo 5, que finalmente soportan la definición de la arquitectura en el capítulo 6.

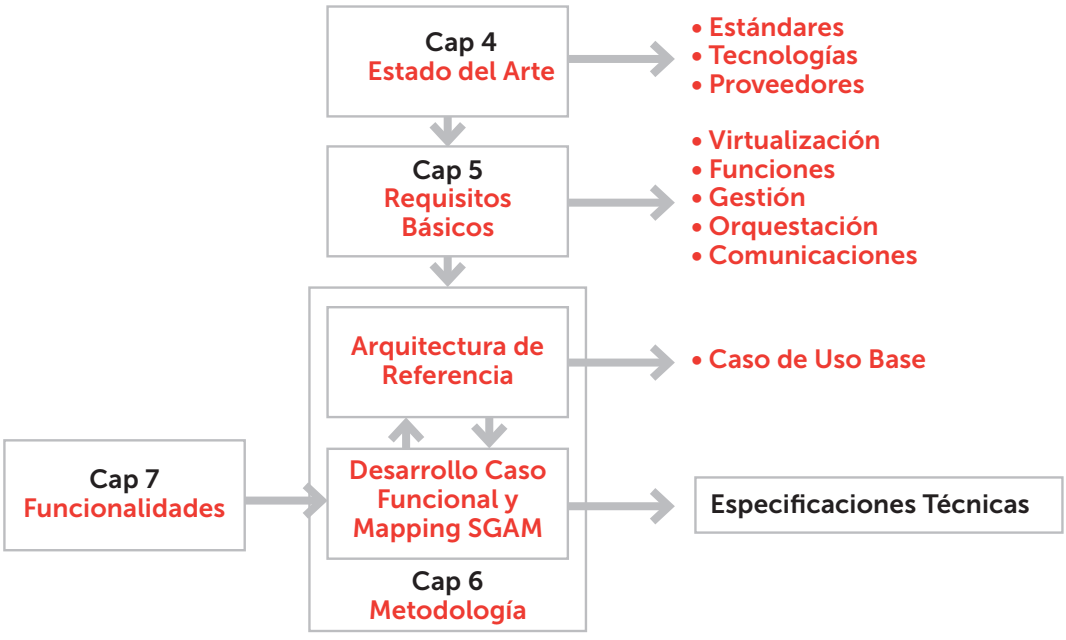


Figura 1: Esquema guía del documento

3. ORGANIZACIÓN

	Coordinador	Grupo
SASCTI Steering Committee	Enrique Garcia (i-DE)	Miguel Ángel Sánchez Fornié (Comillas)
Coordinador de Proyecto	Aurelio Sánchez (i-DE)	
Coordinación y Of Técnica	Anabel Soria (ITE)	
	Juan Gilabert (ITE)	
Comité Técnico	Aurelio Sánchez (i-DE)	Francisco Javier Leiva (e-Ditribución)
	José Luis Vallejo (UFD)	Alberto Villafañe (e-Distribucion)
	Juan Prieto (Indra)	Alejandro García (E-REDES)
	Luís del Rio (Ormazabal)	Luis Draspa (Sercide)
	Aitor Amezua (ZIV)	Alberto Sánchez (Cuerva)
	Antonio Higuera (Ikusi)	Marcos Álvarez (VIESGO)

3.1. Grupo Redacción

REDACCIÓN

Participante	Organización/Empresa
Aurelio Sánchez	I-DE Redes Eléctricas Inteligentes
Enrique Garcia	I-DE Redes Eléctricas Inteligentes
Jose Luis Navarro	Unión Fenosa Distribución
Juan Prieto	Indra Sistemas Tecnologías de la Información, S.L.U
Antonio Higuera Trujillo	ORMAZABAL
Mikel Zaldumbide	ORMAZABAL
Aitor Amezua	ZIV
Juan Gilabert	Instituto Tecnológico de la Energía
Miguel Ángel Sánchez Fornié	Comillas
Íñigo Lartategui	PRONUTEC
Alberto Sánchez	Grupo Cuerva
Juan María García	Ingeteam Power Technology, S.A.
Jonatan González	Merytronic
Haritz Zubia Urrutia	Ariadna Grid
Eutimio Sánchez	Fundación TECNALIA R&I
José Luis Martínez Ramos	AICIA
Marcos Álvarez Lavín	Viesgo Distribución Eléctrica S.L.
Carlos Martínez de Guereñu	ZIGOR Research and Development A.I.E.
Santiago Cascante	e-Distribución
Eduardo Carlos Borntein	EVERIS

José Julio Andrés Suárez	APYDE (ASOCIACION PRODUCT. Y DISTRIBUIDORES ENERGIA DE GALICIA)
Mario López Medina	E-redes distribución
David Cervero	Fundación CIRCE

3.2. Grupo Edición

Participante	Organización/Empresa
Aurelio Sánchez	I-DE Redes Eléctricas Inteligentes
Jose Luis Navarro	Unión Fenosa Distribución
José Luis Vallejo	Unión Fenosa Distribución
Juan Manuel Galán	Unión Fenosa Distribución
Juan Prieto	Indra Sistemas Tecnologías de la Información, S.L.U
Antonio Higuera Trujillo	Ormazabal
Luís del Rio	Ormazabal
Mikel Zaldunbide	Ormazabal
Aitor Amezua	ZIV
Haritz Zubia	Ariadna
Iñigo Lartategui	Pronutec
Alberto Villafañe	e-Distribución
Naiara Amilia	Ormazabal
Nestor Rodriguez	Comillas
Carlos Dolado	UFD
Javier Hernández	I-DE Redes Eléctricas Inteligentes
David Cervero	CIRCE
Marcos Álvarez	Viesgo
Jose Antonio Saez	Viesgo
Juan Gilabert	Instinto Tecnológico de la Energía
Eutimio Sánchez	Tecnalia
Rafael Ballesteros	Ingeteam Power Technology, S.A
Iñigo Lartategui	Pronutec
Francisco Javier Leiva	e-Distribución
Ibon Arechalde	Tecnalia
Alberto Sanchez	Grupo Cuerva
Pablo López	Grupo Cuerva
Mario López	E-redes
Antonio Luis Núñez	Sercide
Jose Antonio Saéz	Viesgo

Alejandro García	E-REDES
Jose Ramon Santiago	ZIV
Ignacio Gomez Osuna	UFD
EMILIO Miranda	e-Distribución
Carlos Gaytan	e-Distribución
Julia Leon	e-Distribución
Jonatan González	Merytronic
Imanol Garcia	Ingeteam Power Technology, S.A.

3.3. Grupo Revisión

Participante	**Organización/Empresa**
Miguel Outmuro Fernández	Arkossa Smart Solutions, SL
Adrián Devesa Mouzo	Deloitte
Isidro Díaz Caballero	Ingelectus S.L.
Jose Luis Domínguez García	Institut de Recerca en Energia de Catalunya (IREC)
Alfonso Santiago González	ISASTUR
Jon Martínez Rico	Tekniker
Alberto González	Telecontrol STM S.L.
Pedro Rodríguez	LOYOLA.TECH
Miroslav Vasić	Universidad Politécnica de Madrid, Centro de Electrónica Industrial
Luis Hernández Callejo	Universidad de Valladolid

4. ESTADO DEL ARTE Y TECNOLOGÍAS DEL SASCTI

4.1. Panorama general de Smart Grid en los centros de transformación

La diversidad de las tipologías de los centros de transformación se debe al resultado de la combinación de condiciones geográficas, económicas e históricas de cada región del mundo.

Figura 2: Diversidad Centros de Transformación en el mundo

En general todos los CCTT se pueden dividir en dos grandes grupos, principalmente relacionados con la tipología de líneas distribución: CT interior y CT exterior. Las características y los elementos que los componen se describen más adelante.

El nivel de desarrollo y la forma de operar la red de media y baja tensión define distintos niveles de inteligencia, en un nivel más básico el CT se puede operar de forma desatendida (sin visibilidad ni comunicación para el Operador). En los países más desarrollados la tónica general es disponer de equipamiento de comunicaciones utilizado como interfaz entre el proceso primario (p.ej. medida y aparamenta) y un sistema central (comúnmente un sistema de control SCADA/DMS). El nivel de inteligencia más avanzado es lo que se conoce como la Smart Grid.

La situación actual de las soluciones Smart grids en los centros de transformación de las Utilities europeas varía mucho, dependiendo fundamentalmente de si han llevado a cabo despliegues de contadores inteligentes y/o automatización de Media Tensión, y de qué tipo:

- Contadores inteligentes
- No realizado por recurso ante la Unión Europea u otras razones.
- Realizado con tecnología PLC BT.
- Realizado con tecnologías radio.
- Automatización de la MT.
- No realizado.
- Equipos autónomos.
- Equipos controlados remotamente.

Aquellas Utilities que hayan instalado en los CT equipamiento con acceso remoto, habrán tenido que instalar también equipos de comunicaciones, lo que supone una inversión que servirá para comunicar futuros servicios en el caso de que se le haya dotado de capacidad suficiente, haciendo más fácil su despliegue. Este es el caso de países como España, Portugal, Italia y Francia, que han aprovechado la oportunidad que el marco regulatorio para la instalación y medida de contadores inteligentes ofrece, para instalar una infraestructura de telecomunicación que permita adaptarse a nuevos requerimientos, basándose fundamentalmente en tecnología PLC.

No obstante, incluso en países con despliegue de PLC BT para contadores, en muchos CT urbanos los concentradores de datos de contadores instalados incluyen un modem 3G, que no se puede compartir con otros servicios, por lo que sería necesario utilizar un router adicional para las comunicaciones de estos.

En cuanto a plataformas y protocolos, existen por un lado las plataformas de telegestion de contadores basadas en DLMS y, por otro, los SCADA universalmente extendidos para el telecontrol de remotas de subestaciones de alta tensión, que se aprovechan para telecontrolar los equipos de automatización en MT en centros de transformación. Los SCADA utilizan IEC 61870-5-104 mayoritariamente, aunque también existen algunos países que utilizan DNP3.0. Los web services no son utilizados de forma importante más que en España y Portugal y algún otro país que haya podido realizar algún despliegue con contadores PLC BT PRIME .

Por otro lado, algunas utilities europeas ahora comienzan a plantearse especificar una red local para unir servicios del CT, aunque hay muchos casos en los que estas redes se están proponiendo con modbus sobre RS485.

En general, puede considerarse que España se encuentra muy avanzada en todo lo relacionado con Smart Grids en centros de transformación respecto a la mayoría de países de Europa, siendo el principal punto en común la utilización del SCADA y sus protocolos de telecontrol, y el DLMS para la medida.

4.2. Características generales de un CT

Por definición entendemos que el centro de transformación es una instalación que comprende uno o varios transformadores, aparamenta de media y baja tensión, conexiones y elementos auxiliares, para suministrar energía en baja tensión a partir de una red de alta/media tensión.

Generalmente, se alimentan en anillo por los cables de media tensión. Cada centro de transformación incorpora un conjunto de celdas de media tensión (RMU: Ring Main Unit) que gestiona la entrada y salida de la línea, y la alimentación y protección al transformador de distribución de media tensión a baja tensión.

En el marco de la gestión inteligente de la red eléctrica, los centros de transformación pueden incorporar:

- Sistemas de telecontrol y supervisión de media tensión (remota de telecontrol (RTU), detector de paso de falta (DPF), cambiador de tomas en carga del transformador, protección de MT del transformador, protección de líneas de MT y módem PLC de banda ancha en MT (MV B-PLC)).
- Telegestión y supervisión en la baja tensión para la gestión de la información de consumos de clientes (concentrador de datos de medida, supervisor básico de BT, supervisor avanzado de BT y automatización del cuadro de BT).
- Dispositivos auxiliares y comunicaciones que no pueden asociarse directamente a ninguno de ellos o bien a ambos (fuente de alimentación/cargador de baterías, sistemas de vigilancia, router celular/xDSL/inalámbrico/FO y estación meteorológica).

Los componentes mencionados se pueden encontrar en diferentes combinaciones y arquitecturas físicas. Es decir,

1. Se hallan presentes en la medida que se precisa su existencia en cada instalación concreta.

2. Se encuentran en diferentes formas. Dependiendo de la arquitectura física, se presentan agrupadas en un mismo equipo o en equipos discretos con funciones diferenciadas.

En la actualidad, existen instalaciones en las que cada una de las funciones se implementa en dispositivos discretos o diferenciados. Las plataformas de hardware que se utilizan son de propósito específico y, en gran medida, plataformas cerradas en las que las modificaciones que impliquen más de un cambio de configuración deben ser llevadas a cabo por el fabricante original.

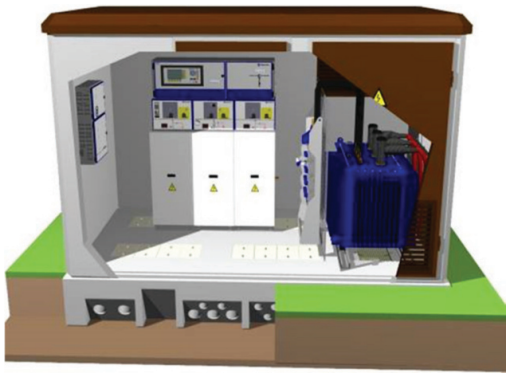


Figura 3: Esquema centro transformación

4.3. Arquitectura de la Smart Grid y normas aplicables

El Smart Grid Co-ordination Group desarrolló entre 2011 y 2014 el esquema básico de arquitectura de Smart Grids de Europa. Desde 2011 hasta la fecha de hoy se siguen revisando el conjunto de normas aplicables en las redes eléctricas inteligentes, detectando brechas normativas y priorizando su desarrollo en las tres asociaciones encargadas de la normalización en elementos del sistema eléctrico y de telecomunicaciones, CEN, CENELEC y ETSI.

El CT se enclava en el Dominio de Distribución y abarca Zonas que cubren desde el Proceso hasta la Operación. En la Capas de Interoperabilidad un CT necesita tener definidas las Capas de Componente, Comunicación, Información y Funcionalidad. El Smart Grid Coordination Group definió entre 2012 y 2014 los ámbitos de interoperabilidad, generándose en 2014 la SGCG_Interoperability_IOPtool (ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_Interoperability_IOPtool.xlsx) , un Excel que recoge todas las normas aplicables, clasificadas por Dominios, Zonas y Capas.

Por otro lado, IEC identifica tres bloques en su modelo de arquitectura de SmartGrids que afectan en mayor o menor medida a los CTs:

1. Automatización de distribución: se consideran en este caso los sistemas de automatización de centros de transformación, centros de seccionamiento y centros de reparto. Aparte estarían los dispositivos de automatización de líneas aéreas o los de los parques de MT de las subestaciones.

2. AMI infraestructura avanzada de medida: en el caso de utilización tecnologías basadas en la adquisición de datos de contadores mediante concentradores de datos, lo habitual es que éste se instale en el CT.

3. Energía distribuida, o autoproductores conectados en redes de distribución de MT o BT, en aquellos casos en los que la interconexión se realiza en centros de transformación, centros de seccionamiento o centros de reparto.

4.4. Centro de transformación actual

Existen múltiples criterios para la clasificación de los centros de transformación, según la alimentación (en punta o en paso), la propiedad (de empresa o de abonado), el emplazamiento de la maniobra (intemperie o interior), la acometida (aérea o subterránea), etc. Otra clasificación común para los de interior, es según la obra, distinguiendo entre:

- CT lonja / fachada / obra civil, donde se engloban todos los ubicados en el interior de un recinto específico construido de ladrillo, piedra y hormigón (no es habitual en la actualidad aunque se pueden encontrar entre las instalaciones existentes) y aquellos donde la aparamenta eléctrica se instala en

un edificio que es destinado a otros usos. El centro de transformación será considerado como parte del edificio y previo al montaje eléctrico tendrá que certificar el cumplimiento de los requisitos reglamentarios.

- CTs prefabricados, es un suministro llave en mano, íntegramente montado en fabrica y sometido a ensayos de tipo que garantizan la calidad del conjunto y aseguran la protección de las personas según las condiciones de servicio especificadas. Pueden distinguirse entre envolventes de hormigón, donde encontramos centros subterráneos, de maniobra interior y bajo poste, tanto monobloque como modular y envolventes metálicas que dan soporte a centros de maniobra interior, exterior y bajo poste. Aquí existen varios tipos desde los subterráneos hasta los de superficie.

Los elementos que componen un centro de transformación son descritos en las siguientes secciones.

Figura 4: Fotos ejemplo tipos de CTs

4.4.1. Celdas de media tensión

Se entiende por celda el conjunto de aparamenta eléctrica alojada bajo una envolvente metálica que constituye un único compartimento. Dentro de las celdas se ubican equipos de maniobra (interruptores, seccionadores...), medida (transformadores de corriente y de tensión), y, cuando se solicite, equipos de protección y control que cumplen la función de recibir y distribuir la energía eléctrica. Dependiendo de las características (tensión nominal, corriente de cortocircuito...) y del tipo de celda (función de línea, interruptor automático, medida...) seleccionada es posible tener diferentes aplicaciones pudiendo llevar a cabo todos los esquemas utilizados en la distribución secundaria de media tensión

1. Cuba SF6
2. Compartimento de mecanismos de maniobra
3. Base
   a. Compartimento de cables
   b. Compartimento de salida de gases
4 Armario de automatización de media tensión

4.4.2. Protecciones

Las celdas de protección, conocidas como celda de fusibles e interruptor automático, tienen como objetivo principal proteger al transformador, así como a la instalación general, de una sobrecarga en el caso del IA.

En funcionamiento normal por la instalación, circulan corrientes de servicio, incluidas eventuales sobrecargas, admisibles hasta cierto valor y/o duración. Cuando se produce un defecto de aislamiento, y dependiendo de la configuración del neutro, circula una corriente de cortocircuito que puede llegar a ser muy superior a la de servicio normal, las celdas de protección actuarán.

La celda de fusibles, que aloja en su interior tres fusibles uno por cada fase, puede ser de:

- Fusibles combinados: Al detectar un cortocircuito en cualquiera de las fases el fusible de esa fase se funde y las otras dos fases continúan alimentando al transformador.
- Fusibles asociados: Al detectar un cortocircuito en cualquiera de las fases el fusible de esa fase se funde abriendo el seccionador e interrumpiendo la alimentación del transformador.

El interruptor automático está formado por tres polos con dos contactos, uno fijo y otro móvil, y está garantizada la seguridad del operario a la hora de acceder al compartimento de cables. La maniobra de apertura del interruptor automático puede ser manual, por botonera o por señal del relé.

Mayores prestaciones se pueden lograr si se opta por un interruptor automático con mecanismo de maniobra con reenganche. En este caso, al detectarse una sobrecarga el interruptor automático abre el circuito y transcurrido un tiempo de X segundos, lo cierra en espera de que haya desaparecido la anomalía. Si ésta persiste, vuelve a abrir el circuito esperando un intervalo mayor para ver si la causa ha desaparecido. Finalmente, podría volver a abrir el circuito si la causa de la falta sigue existiendo, quedando en espera de nuevas órdenes. Esta secuencia de operaciones está siempre gobernada por el relé de protección general, quien da las señales de cierre o apertura en función de los valores que observa en la red y su programación previa.

4.4.3. Grados de automatización

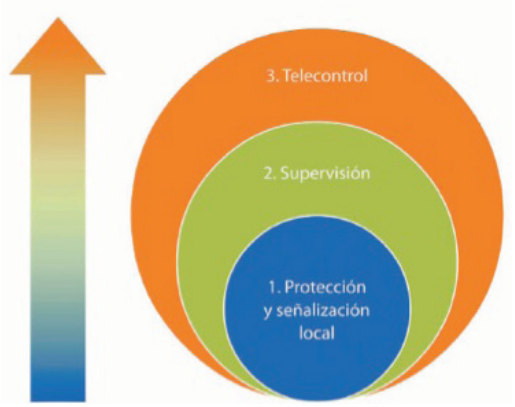
4.4.3.1. Protección y señalización local

Dota al centro de transformación convencional, con equipos de protección e indicación local de paso falta que permitan:

- Una rápida localización de faltas cuando ocurre un cortocircuito en la red, aislando la falta y reduciendo así los tiempos de cortes del suministro eléctrico.
- Detección de presencia/ausencia de tensión, aumentando la seguridad de la instalación.

4.4.3.2. Supervisión

Un paso más hacia la automatización de la red eléctrica de distribución consiste en introducir la supervisión en los centros de transformación. Para ello, partiendo tanto de un centro existente o nuevo, como de un centro con protección y señalización local, se instalan relés de protección multifuncional y control, relés de paso de falta con control y medidas, transformadores de intensidad en pasatapas, medida de tensión sin necesidad de usar transformadores convencionales (haciendo uso de la sensórica), comunicaciones, etc. Todo ello integrado en celdas de media tensión de maniobra manual.



	Grado de automatización	Solución
1	Protección y señalización local	• Indicador paso de falta en celdas de línea • Protección local autoalimentada en celda de protección • Detección de presencia de tensión • Alimentación auxiliar segura en BT • Señalización e indicación local
2	Supervisión	• Estado de celdas • Captación de medidas • Comunicaciones serie / IP • Webserver integrado • Alimentación auxiliar
3	Telecontrol	• Telemando/control de celdas • Infraestructura de comunicaciones y protocolos (automatismos locales) • Interconectividad entre centros de transformación (automatismos distribuidos)

Figura 5: Grados de automatización

Desde hace años se trabaja en desarrollar y potenciar productos, aplicaciones y servicios relacionados con la protección y automatización de la red de distribución, aportando innovación y alto valor añadido a la instalación. Por ello este campo está en constante evolución pasando de una automatización convencional, sin comunicaciones, a la más completa que incluye telecontrol. Podemos encontrar tres etapas diferenciadas en:

4.4.3.3. Telecontrol y Telegestión

Una red se puede automatizar partiendo de cero, o desde cualquiera de los casos anteriores, hasta la máxima extensión posible. Para ello, es necesario un centro de transformación con celdas de media tensión con maniobra motorizada, así como con características de telecontrol, comunicaciones, supervisión y medida. De esa manera mejora notablemente la calidad de servicio ya que se tiene un mayor control de la red obteniendo medidas e indicaciones precisas en tiempo real, lo que permite actuar

sobre las protecciones de manera inmediata en remoto.

Desde el armario de automatización se recogen y envían indicaciones a distancia mediante un enlace de transmisión para controlar un sistema o sistemas remotos que no están directamente conectados al lugar desde donde se envía el telecontrol. Suele estar situado en la parte superior de la aparamenta de media tensión o ser tipo mural y puede incorporar funciones de:

- Telecontrol: dota a la parte de media tensión del centro de transformación de tecnología que permita el envío de indicaciones a distancia.
- Telegestión: dota a la parte de baja tensión del centro de transformación de tecnología que permite el envío de indicaciones a distancia en tiempo real pudiendo analizar, actuar y supervisar, prestando nuevos servicios, mejorando la calidad del suministro y la satisfacción de los clientes.

El telecontrol está ligado a la parte de media tensión, por lo tanto, todos sus equipos irán referenciados a la puesta a tierra del centro de transformación (media tensión). Los equipos de telegestión en cambio, tomarán como referencia de tierras la asociada al neutro proveniente del cuadro de baja tensión. Si las señales de ambas áreas se agrupan sobre un mismo elemento de comunicaciones existirá una diferencia de potencial. Para solventar esta desigualdad de potenciales bastará con aislar las señales de una de las partes (la de baja tensión suele ser lo más habitual) a 10 kV tal y como indica el reglamento.

Hasta hace poco, las infraestructuras de comunicaciones eran requeridas en un número pequeño de subestaciones y como objetivo tenían que dar soporte a necesidades muy concretas (control remoto del seccionador, detección de faltas,...) para lo que bastaban unos protocolos de comunicación simples que se podían transmitir con dispositivos de radio; sin embargo en estos momentos ya se está desarrollando el sistema de medidas inteligentes, lo que hace que en cada subestación/centro de trasformación, se necesiten concentradores y por tanto, infraestructura de comunicación en cada una de ellas.

Para poder comunicar un gran número de centros de transformación entre sí, requiere combinar infraestructuras de comunicaciones privadas con los servicios públicos de las operadoras públicas. Para ello se deben tener en cuenta todos los requerimientos técnicos (seguridad para evitar ataques cibernéticos, incremento del ancho de banda para transmitir la información generada, alta disponibilidad y fiabilidad de disposición de las comunicaciones, flexibilidad y escalabilidad para dar soporte a necesidades actuales y futuras y baja latencia para aplicaciones de automatización y protección). En el apartado 4.6 de este documento se describen los diferentes medios de comunicaciones.

4.4.3.4. Telecomunicaciones

Lo primero que se tiene que conocer a la hora de identificar una comunicación, es la naturaleza de la señal a transmitir, pudiendo ser estas:

Analógicas, puede tener infinitos valores a lo largo del tiempo.

Digitales, solamente puede tener un rango definido de valores.

Otro concepto, a tener en cuenta a la hora de transmitir información, es el medio por el que se hace, pudiendo ser:

Medios guiados: la señal tiene un camino confinado por el que se transmite (cable coaxial, cable de pares, fibra óptica...). Si hablamos del tipo de cable, el coaxial es el más utilizado para la transmisión de las señales de medida entre los sensores de tensión y los relés. La fibra óptica es otro método muy utilizado ya que proporciona un gran ancho de banda, inmunidad frente a interferencias, gran seguridad de los datos y una alta resistencia a la corrosión y altas temperaturas.

Un caso particular de medio de comunicación guiados sería el denominado PLC, que utiliza la propia red eléctrica para transmitir información. Entre sus aplicaciones se encuentran conectar subestaciones de media tensión por la propia red eléctrica y la gestión remota de contadores.

Medios no guiados: la señal se propaga por un entorno abierto (aire, espacio, agua...). En este caso nos encontramos con las comunicaciones

de radiofrecuencia, satélite, telecomunicaciones móviles y wimax.

El tipo de comunicación más utilizado actualmente es la comunicación IP, donde todos los equipos tienen una dirección IP para poder ser identificados dentro de la red. Existen dos equipos que resultan básicos para gestionar las comunicaciones este tipo de redes:

- **Switch**, trabaja con direccionamiento físico, es decir, es capaz de comunicarse con equipos conectados a él a través de su dirección MAC.
- **Router**, trabaja con direccionamiento lógico, se comunica con equipos a través de direcciones IP. Este equipo se utiliza cuando se quieren interconectar dos redes diferentes, por ejemplo, la red local de una oficina con internet.

4.4.3.5. Sistema de alimentación ininterrumpida (SAI) y Baterías

Este sistema está formado por un dispositivo que, gracias a sus baterías u otros elementos almacenadores de energía, durante una interrupción de suministro eléctrico, puede proporcionar energía eléctrica por un tiempo limitado a todos los dispositivos que tenga conectados.

4.4.3.6. Sensórica

Los sensores permiten extender la visibilidad de la red eléctrica de media tensión, ofreciendo la precisión y confiabilidad que necesitan protecciones y medidores para desplegar funcionalidades avanzadas de automatización de la distribución. Los sensores posibilitan la operación automatizada e incrementan la eficiencia operativa de la red.

4.4.3.7. Nuevas necesidades de automatización

Existe actualmente un cambio lento pero irreversible de paradigma en las redes BT, pasando la gestión de estar centrada en los activos a poner el foco en el cliente. Por tanto, los mayores niveles de calidad, junto a la introducción de generación y almacenamiento en baja tensión, están favoreciendo la progresiva comercialización de nuevas funcionalidades en la operación de redes BT que conllevan nuevos desarrollos de automatización y el nuevo rol del centro de transformación como una unidad de recogida y transmisión de medidas e indicadores de la red BT:

- Incremento de la observabilidad en los consumos aguas abajo del transformador MT/BT con diversos fines: detección de fraude, reducción de pérdidas, reducción del desequilibrio, detección de sobretensiones y saturaciones.
- Control centralizado (desde el propio CT), descentralizado (desde el CT hacia agregadores intermedios) o local de las fuentes de generación distribuidas (incluido almacenamiento).
- Detección y localización de fallos en BT con objeto de reducir el tiempo de reparación.
- Reconfiguración de la explotación de la red de BT mediante la introducción de puntos de maniobra telecontrolados.

En el ámbito de la MT, el despliegue de comunicaciones entre CCTT permitirá una mayor efectividad en la detección, localización y aislamiento de fallos, la aparición de herramientas de diagnóstico on-line en cables y la gestión de fenómenos asociados a la generación distribuida como el funcionamiento en isla.

4.4.4. Transformador de distribución

Los transformadores de distribución disponen de un amplio abanico de potencias de 25 hasta 5000kVA con tensiones de alimentación MT de 24/36kV y con tensiones de salida BT en 420V. La refrigeración de los transformadores de distribución, salvo casos concretos, suele basarse en convección natural, para lo que los centros de transformación están dotados de rejillas de ventilación con ubicación y dimensiones adecuadas para este propósito.

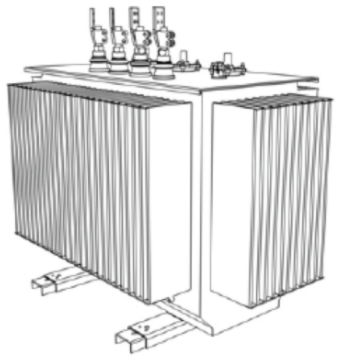


Figura 6: Esquema transformador de distribución

En una explotación radial y pasiva de la red de distribución en MT sin presencia de generación distribuida, los perfiles de tensión a lo largo de los alimentadores suelen ser decrecientes. Como consecuencia, aquellos centros de transformación situados cerca de la subestación primaria AT/MT tendrían tensiones BT mayores que otros en localizaciones más lejanas. Para evitar este inconveniente, los transformadores de distribución están dotados de cambiadores de tomas en vacío en los devanados MT que permiten ajustar la relación de transformación. Así, es posible tener una tensión adecuada en BT independientemente de la posición relativa del centro de transformación con respecto a la subestación primaria. Las tomas habituales de los transformadores de distribución, además de la toma central, suelen ser del $\pm$2.5%, $\pm$5% y $\pm$10%.

Hay que tener en cuenta que este ajuste debe efectuarse cuando el transformador está desconectado de la red por lo que, prácticamente, la posición de la toma se fija cuando el transformador es instalado y rara vez vuelve a cambiarse en su vida útil.

Sin embargo, las redes MT y BT, a medida en que crece la penetración de la generación distribuida, dejan de poderse considerar como pasivas. En esta nueva situación, será de vital importancia contar con mecanismos de control de tensión en la red efectivos, que permitan operar la red con una flexibilidad adicional.

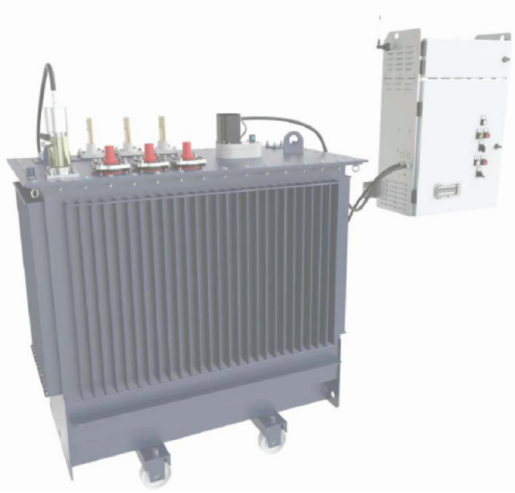


Figura 7: Transformador de distribución con cambiador de tomas

4.4.5. Cuadro de distribución

El cuadro de baja tensión es el encargado de proteger cada uno de los distintos circuitos en los que se divide la red de baja tensión. De él, parten las líneas de baja tensión y su función es recibir el circuito principal de baja tensión procedente del transformador MT/BT y distribuirlo en un número determinado de circuitos. Entre sus elementos principales cuenta con un embarrado de acometida, unas bases portafusibles, un seccionador, un compartimento de control y un bastidor.

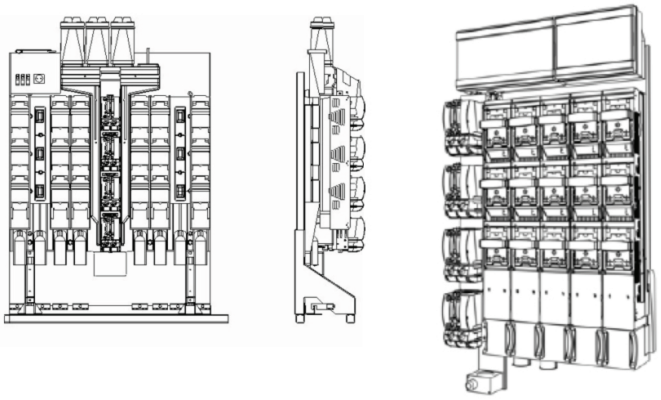


Figura 8: Esquemas cuadros de baja tensión

Debido al aumento de supervisión en la parte de baja tensión los cuadros de distribución están en constante evolución. Por ello, es cada vez más común encontrarnos con cuadros de distribución de baja tensión con embarrado aislado y supervisión avanzada de baja tensión.

4.4.6. Interconexiones

1. Interconexión celdas – transformador.

   La conexión eléctrica entre la celda y el transformador suele realizarse con cable unipolar seco de aluminio/cobre.

2. Interconexión transformador – cuadro de baja tensión.

El cuadro de baja tensión se deberá instalar lo más cerca posible del transformador siendo la interconexión entre transformador y cuadro lo más corta posible.

La conexión eléctrica entre el transformador y el cuadro de se realiza con cable unipolar seco de aluminio/cobre y su sección dependerá de la potencia del transformador.

4.4.7. Conexión del circuito de puesta a tierra

El centro de transformación está provisto de dos circuitos de puesta a tierra para facilitar la conexión de los diferentes elementos a la ejecución de la red de puesta a tierra exterior al Centro de Transformación.

1. Red de tierra de protección

   La línea de puesta a tierra de protección (herrajes) recoge la puesta a tierra de los diferentes elementos que componen el equipo eléctrico (celdas de media tensión, transformador de distribución y cuadro de baja tensión). Dicha pletina se une a la pletina colectora general de la propia envolvente, desde la cual se da tierra a todos los elementos metálicos de la envolvente que son accesibles desde el exterior.

   El circuito de puesta a tierra de protección se conecta a la caja de seccionamiento de protección del centro de transformación.

2. Puesta a tierra de servicio (neutro)

   La línea de puesta a tierra de servicio (neutro) une el embarrado de neutro del transformador de distribución con la caja de seccionamiento dispuesta en la envolvente del centro de transformación.

   La pletina de neutro del cuadro de baja tensión no está unida a la pletina de conexión de las tierras de protección (herrajes).

3. Red de tierra exterior

   El proyecto de la instalación debe incluir el apartado correspondiente a la ejecución de la instalación de puesta a tierra (consultar proyecto tipo de la compañía eléctrica), así como la justificación de su dimensionado. En el apartado de Instalaciones de puesta a tierra del RAT (ITC-RAT 13) se establecen los requisitos que deben reunir este tipo de instalaciones.

4.4.8. Retos a futuro para el CT

Tras ver todos los elementos que componen un CT actual es importante resaltar que los requerimientos e incluso los retos a resolver para su evolución hacia el SASCTI, varían sustancialmente en función de su tipología.

Retos **tecnológicos/digitalización**. Existe gran número de centros de transformación con aparamenta (MT) convencional que dificulta la implantación de los casos de uso relacionados con la MT. En aquellos donde sean imprescindibles estos casos de uso, la solución deberá ser la sustitución/renovación de aparamenta.

Retos relacionados con la **comunicación y la alimentación segura**. Habrá que discriminar entre aquellos casos de uso que requieran del tiempo real con falta de alimentación y aquellos casos de uso que son funcionales en explotación normal para dotar convenientemente a dichos centros de infraestructura adecuada de alimentación segura y comunicaciones (en función del sistema de comunicaciones que se utilice).

Aunque la filosofía del Edge reduce el tráfico de datos frente a una toma de decisiones centralizada, la digitalización del centro aumentará dicho tráfico. Acertar con el **canal de comunicaciones** adecuado para cada caso, por necesitar un mayor ancho de banda que el actualmente usado, será un reto para cada ubicación y cada distribuidora.

Retos relacionados con la **ciberseguridad**. Dado que se hipersensibilizará la red para una mayor adquisición de datos y por tanto un mayor riesgo de ciberataque y de exposición de la red a los ataques externos, será importante la segmentación, pero sin abandonar las funcionalidades de socorro que necesitan de la intercomunicación de centros entre sí.

Retos en **seguridad** y el aislamiento en equipos con orígenes en BT y orígenes en MT que se entremezclarán para una eficiente adquisición de datos

Retos **dimensionales**, dado que existe un gran número de centros de transformación compactos en envolventes ajustadas en tamaño que requerirán de un espacio mayor para instalar captadores que digitalicen las instalaciones en tiempo real, los de maniobra exterior, semienterrados, empotrados en fachada (Lonja), son casos en los que introducir nuevos equipos para digitalizar será un reto de espacio.

4.5. Tecnología de las plataformas de procesamiento distribuido

Las tecnologías y arquitecturas centralizadas que se usan actualmente para monitorizar y controlar las redes eléctricas y los mercados, no fueron diseñadas para operar bajo circunstancias tan exigentes como las que empiezan a vislumbrarse en las redes de BT.

El abaratamiento de los equipos de computación de uso industrial y el despliegue sobre los mismos de una **nueva arquitectura de gestión distribuida Edge**, permiten de forma única dar respuesta a estos retos a la vez que habilita nuevos modelos de intercambio de servicios entre los clientes conectados y la red. El cambio de paradigma que se contempla en la actualidad en las arquitecturas de comunicaciones de toda la industria, es el paso del cloud computing al edge computing[1].

El edge computing es el nuevo modelo de arquitectura de procesamiento distribuido, que en contraposición al fuertemente consolidado cloud computing, acerca el procesamiento de la información a los bordes de la red, reduciendo en el proceso la latencia y aumentando la velocidad de respuesta del sistema. Este modelo responde a las necesidades de un mercado en el cual cada vez la cantidad de información de los sistemas finales es mayor. En el ámbito de las redes eléctricas, cada vez es mayor la sensorización y monitorización de todos los niveles de la red, lo que eleva la cantidad de información disponible en varios órdenes de magnitud. Además, la disponibilidad de mayor información del sistema y de mayores capacidades de computación, permiten la realización de algoritmos de control más avanzados, que en el ámbito eléctrico deben ejecutarse en algunos casos en cuestión de microsegundos para asegurar la integridad de la red. Dichas necesidades hacen inviable seguir funcionando con el modelo centralizado en la cloud, siendo muy beneficioso en este entorno la disposición de equipos de procesamiento en los sistemas periféricos para la ejecución de dichos algoritmos y preprocesamiento de los datos in situ para cumplir los límites de funcionamiento adecuados.

Las arquitecturas de procesamiento distribuido son resultado de la convergencia de 3 grupos de tecnologías:

1. **IoT** (Internet of Things). Habilita la gestión de millones de dispositivos y sus flujos de información de forma escalable y a bajo costo.
2. **De Operación en tiempo real** (OT). Proporcionando capacidades de integración y control directo de equipos eléctricos y dispositivos de gestión de energía en tiempo real y de forma segura y robusta.

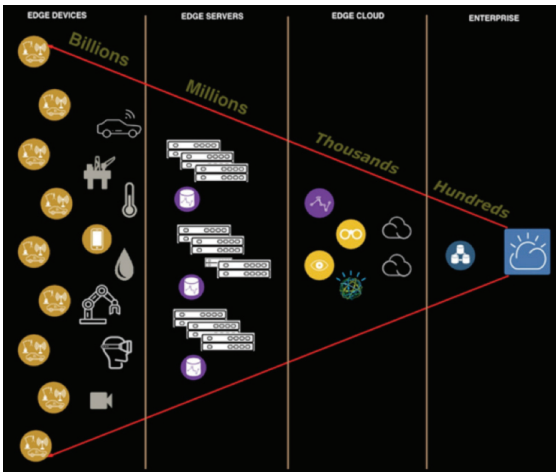


Figura 9: Volumen de información a gestionar desde los dispositivos en el borde al cloud

3. **De virtualización y gestión CaaS** (Container as a Service), permitiendo:

- El **encapsulamiento** eficiente de funciones de gestión y control eléctrico, habilitando ecosistemas abiertos y seguros con los que crecer sin inversión adicional en la funcionalidad del CT.
- La **gestión, mantenimiento y despliegue centralizado** (y eficiente) de cientos de miles o millones de Centros de Distribución Digitales.

Las arquitecturas de procesamiento distribuido frente a arquitecturas de procesamiento centralizado como puedan ser las arquitecturas SCADA o las arquitecturas IoT en nube presentan distintas ventajas para la gestión de

[1] https://www.apriorit.com/dev-blog/531-cloud-edge-computing

infraestructuras distribuidas como es el caso de las redes de distribución:

- **Minimiza los tiempos de reacción.** La gestión centralizada de la información requiere como mínimo tiempos del orden de un minuto para recibir la información y otro minuto para actuar. La gestión distribuida permite dar respuesta a casos de uso que requieren tiempos de análisis y respuesta muchos más cortos, como pueda ser el control de la tensión en el SASCTI o la identificación y protección de la infraestructura y/o los clientes ante fallos inminentes.
- **Simplifica la gestión global de la red** a la vez que permite multiplicar por varios órdenes de magnitud el número de activos y puntos gestionados en tiempo real por el operador. La distribución de la capacidad de procesamiento, análisis y reacción, maximiza el valor de la información recibida, a la vez que minimiza el volumen de información sobre la que el operador puede y debe reaccionar.
- **Optimiza el uso de la infraestructura existente** (comunicaciones, bases de datos y procesamiento) y minimiza el coste global de operación y mantenimiento:

Todos los beneficios anteriores deben de ponderarse con el potencial extra coste relacionado con el despliegue en un alto número de puntos de nuevos equipos de procesamiento y computación y su mantenimiento, protección y operación.

El aumento de dispositivos inteligentes implica un aumento de puntos potencialmente inseguros en la red, convirtiendo todavía más, si cabe la ciberseguridad un aspecto crítico de estos sistemas. También modifica los requerimientos hardware de los dispositivos de campo para poder realizar los procesos necesarios en local, y reduce la visibilidad de la información desde los servicios centrales, lo que dificulta la definición de estrategias y protocolos basados en el comportamiento del usuario final.

Para evitar estos inconvenientes cualquier plataforma de procesamiento distribuido debe de dar respuesta a 10 retos fundamentales como se recoge en la siguiente figura:

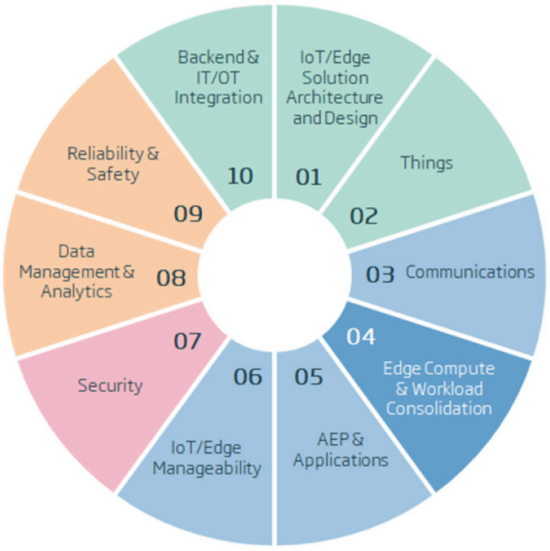


Figura 10: Retos a abordar por una plataforma de procesamiento distribuido.

4.5.1. Plataformas de procesamiento distribuído: Capas /Componentes

Cualquier arquitectura distribuida tiene al menos tres niveles diferenciados:

- **Dispositivo**.

  El primer nivel lo componen los dispositivos que se gobiernan. Son los que adquieren la información necesaria del entorno y aquellos que en última instancia llevan a cabo las acciones que el sistema comanda en función de cada caso de uso. Se trata principalmente de actuadores, captadores, sensores...

  También se encuadran en este nivel los dispositivos que proporcionan la conectividad necesaria al sistema.

- **Edge**.

  Este nivel se puede subdividir en varios niveles según los casos de uso y capacidades de comunicación.

  2.1. Edge Devices, con capacidad limitada e interactuando directamente con los dispositivos.

  2.2. Edge Server. Coordinando nubes de Edge devices.

- **Cloud**.

Es el nivel superior de esta arquitectura de tres niveles. En él residen las interfaces con

el usuario y las aplicaciones y procesos que interactúan con el Edge y otros procesos de negocio.

El siguiente esquema identifica los principales componentes que cualquier plataforma distribuida debe de contener en cada uno de los niveles.

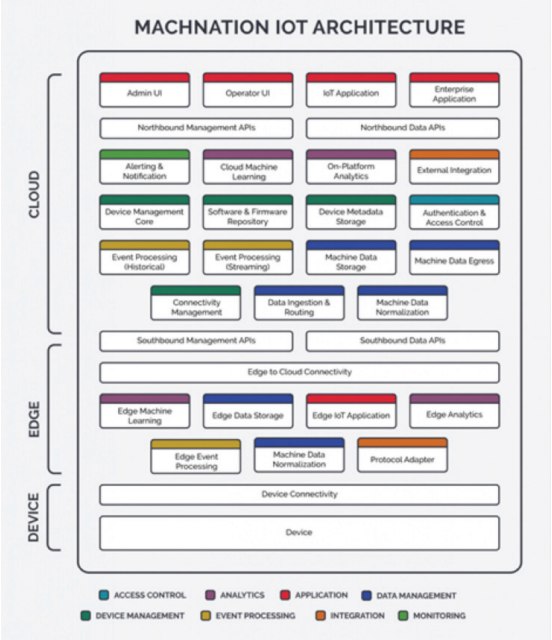


Figura 11: Componentes de una plataforma de procesamiento distribuido por capas.

4.5.1.1. Dispositivos y otros componentes hardware

Tal como se detalla en el apartado 4.3.1 los componentes hardware SmartGrids de un CT pueden clasificarse en función del nivel de tensión en el que actúan. Adicionalmente hay otros dispositivos auxiliares no directamente asociables al nivel de tensión, tal como se recoge en la siguiente tabla que no pretende ser exhaustiva.

4.5.2. El encapsulamiento y la gestión de las funciones distribuidas

Uno de los aspectos fundamentales a los que, una arquitectura Edge debe de dar respuesta es al encapsulamiento, gestión y distribución de la funcionalidad de negocio en cientos o miles de dispositivos Edge.

La virtualización (VM y Contenedores) y el despliegue de runtimes de ejecución (para servidores o agentes) son las tendencias para proporcionar una forma coordinada, adaptable y manejable holísticamente, de distribuir la capacidad de cómputo y la entrega rápida de servicios.

La virtualización se ha completado en los últimos años con el auge del uso de contenedores o virtualización ligera. La virtualización ligera ha permitido el uso de infraestructura definida por software de forma exponencial. Cada contenedor es un runtime aislado donde ejecutar una aplicación completa (o un servi-

MT	Remota de telecontrol (RTU)
	Detector de paso de falta (DPF)
	Cambiador de tomas en carga del transformador
	Protección de MT del transformador
	Protección de líneas de MT
	Módem PLC de banda ancha en MT (MV B-PLC)
BT	Concentrador de datos de medida
	Supervisor básico de BT
	Supervisor avanzado de BT
	Automatización del cuadro de BT
Auxiliares y comunicaciones	Fuente de alimentación/cargador de baterías
	Sistemas de vigilancia
	Router celular/xDSL/inalámbrico/FO
	Modem PLC BT
	Estación meteorológica.
	Sensores varios de humedad, presencia, temperatura interior etc.

Tabla 1. Detalle de componentes HW por subsistema en el ámbito de un CT.

cio). Los contenedores se definen como recursos empleando archivos de configuración YAML o JSON. La tecnología de contenedores más popular hoy en día es Docker.

Una tercera vía explotada por Amazon en su arquitectura en nube es el encapsulamiento en funciones lambda en la que únicamente se encapsula el código de la función.

Las mismas técnicas utilizadas en la virtualización de la infraestructura en nube se están comenzando a aplicar al mundo del Edge Computing para la distribución de cargas de trabajo y la ejecución cercana.

4.5.2.1. Aproximaciones para el encapsulamiento SW

Hoy en día, a la hora de desarrollar aplicaciones software, existen varias aproximaciones a considerar.

A continuación, se describen las principales corrientes existentes en la actualidad, que se podrían emplear a la hora de desarrollar una plataforma de procesamiento distribuido.

4.5.2.1.1. Aplicaciones Monolíticas

Son las aplicaciones desarrolladas tradicionalmente, que pueden considerarse como un "todo en uno". Estas aplicaciones se basan en la combinación de varios componentes que implementan diferentes funcionalidades en un único programa que se ejecutará sobre una plataforma HW/SW determinada.

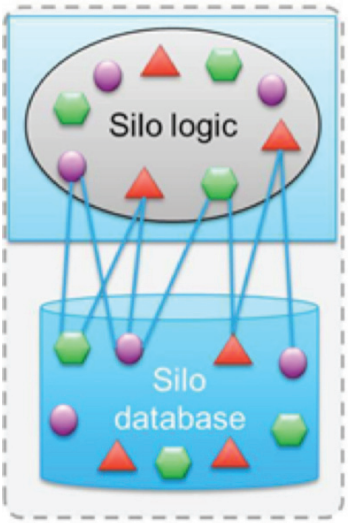


Figura 12: Ejemplo de una aplicación monolítica.

Todos los bloques que conforman la aplicación están intrínsecamente ligados y el fallo en una parte del código puede comprometer el funcionamiento del resto de bloques.

Por otro lado, la ejecución de este tipo de programas es muy predecible y más segura, y su desarrollo es simple y sistemático reduciendo la posibilidad de errores.

Ventajas de las aplicaciones monolíticas:

- Desarrollo y despliegue más sencillo: se trabaja con una estructura común y los cambios y actualizaciones se despliegan de usa sola vez, e.g. un paquete o ejecutable.
- Menos problemas transversales: al contar con un único código de base es más sencillo gestionar para realizar auditorías, logging, regulación de tasas de funcionamiento, etc.
- Mejor rendimiento: tienen mayor rendimiento, especialmente porque la comunicación entre los componentes software se realiza a través de código y memoria compartida.

Inconvenientes de las aplicaciones monolíticas:

- El código crece desordenadamente: con el tiempo, a medida que se desarrollan productos y aumentan su alcance, la estructura del software se vuelve farragosa, y el código se hace difícil de entender y modificar, especialmente para desarrolladores que no lo conozcan.
- Dificultad para adoptar nuevas tecnologías: añadir nuevas tecnologías o funcionalidades a la aplicación puede suponer tener que reescribir toda la aplicación de cero.
- Poca agilidad ante los cambios: cada pequeño cambio que se produzca en el código requiere una validación de todos los componentes y la distribución completa de la nueva aplicación. La coordinación entre varios equipos trabajando sobre el mismo código se reduce notablemente.
- Un bug no controlado en algún módulo interno (e.g. memory leak) puede tirar abajo la aplicación completa o hacer que otro módulo se comporte de manera no esperada.

4.5.2.1.2. Aplicaciones cliente servidor

Modelo clásico de aplicaciones en internet (servidor web).

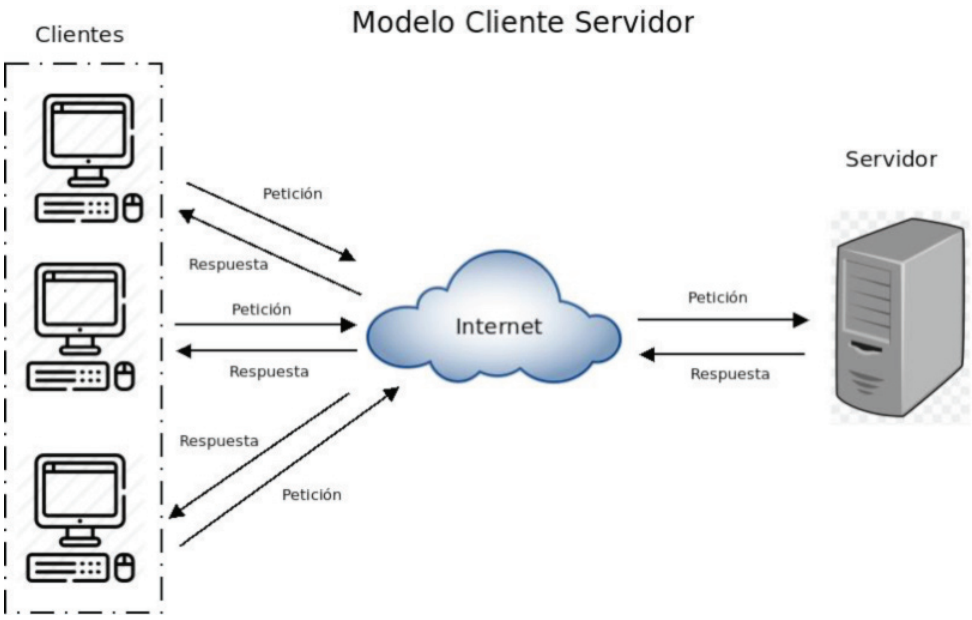


Figura 13: Ejemplo de una arquitectura cliente-servidor.

Ventajas de las aplicaciones clientes-servidor:

- Se centraliza la distribución y configuración de la aplicación, pudiéndose hacer actualizaciones desde el punto de vista del cliente.
- A la hora de trabajar equipos pequeños esta manera de trabajar en desarrollo de nuevas características es la más rápida.

Inconvenientes de las aplicaciones cliente-servidor:

- A la hora de escalar este tipo de aplicaciones solo lo podemos hacer mediante un escalado vertical.
- A la hora de trabajar equipos de desarrollo grandes es difícil "desacoplar" funcionalidades y código de manera independiente.

4.5.2.1.3. Arquitecturas orientadas a servicios (SOA)

Las arquitecturas orientadas a servicios (SOA) se refieren a una aplicación compuesta de diferentes agentes software desacoplados entre sí que interactúan para realizar una determinada función.

Los agentes pueden desempeñar dos roles, proveedor o consumidor de servicios. Los agentes exponen sus funcionalidades a través de protocolos estándar, e.g. SOAP, y pueden tener un tamaño pequeño o representar lógicas de negocio importantes.

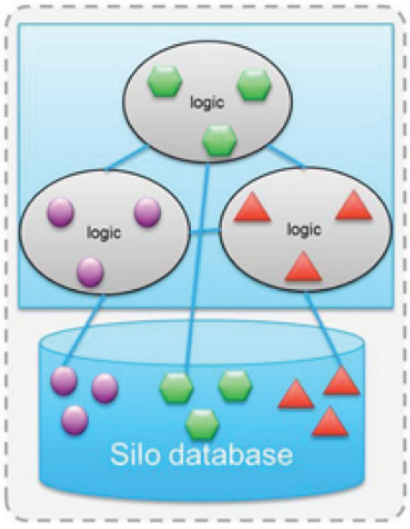


Figura 14: Ejemplo de una aplicación con diversos componentes.

Ventajas de las arquitecturas orientadas a servicios (SOA):

- Reutilización de servicios: al ser servicios autocontenidos y desacoplados se pueden reutilizar en diferentes aplicaciones fácilmente.
- Más fácil de mantener: al tratarse de unidades individuales es mucho más sencillo actualizar y mantener los agentes sin afectar al resto de servicios.
- Mayor fiabilidad: se pueden depurar y testear más fácilmente al tener funcionalidades más acotadas y las interfaces bien definidas.
- Desarrollo en paralelo: cada uno de los servicios independientes se puede desarrollar en paralelo y ser integrado en un punto determinado.

Inconvenientes de las arquitecturas orientadas a servicios (SOA):

- Gestión complicada: se añade una mayor complejidad ya que cada servicio tiene que garantizar que los mensajes se entregan a tiempo y el número de mensajes que intercambian los servicios puede crecer exponencialmente.
- Mayor sobrecarga: los diferentes agentes tienen que interactuar entre sí y esto incrementa el tiempo de respuesta y disminuye el rendimiento.

4.5.2.1.4. Microservicios

Los microservicios son una especie de evolución o tipo de arquitectura SOA, en el que se divide la aplicación en partes más pequeñas que pueden funcionar de manera independiente interactuando entre sí a través de APIs. La mayor diferencia es que los servicios en este caso existen como elementos desplegables completamente independientes, permitiendo una mayor agilidad y escalabilidad. Cada microservicio se ejecuta independientemente de los demás en su propio proceso, máquina virtual o contenedor.

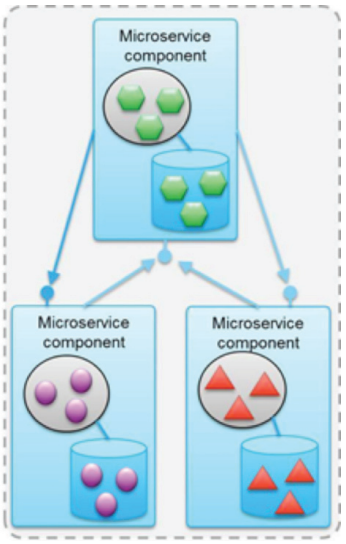


Figura 15: Ejemplo de una aplicación basada en microservicios.

Las organizaciones pueden utilizar una arquitectura de microservicios para dar mayor flexibilidad a sus aplicaciones y permitir una innovación más rápida. La arquitectura de microservicios desacopla sistemas complejos de gran tamaño en proyectos sencillos e independientes. Las aplicaciones se dividen en muchos componentes individuales (servicios) y cada servicio abarca un solo propósito o función y se opera independientemente de los demás servicios y de la aplicación general. Esta arquitectura reduce los gastos de coordinación necesarios para actualizar las aplicaciones. Cuando cada servicio se asigna a equipos pequeños y ágiles que se hacen responsables del mismo, las organizaciones pueden avanzar con rapidez. En el caso del SASCTI, los microservicios corresponderían a las aplicaciones (o parte de ellas) que implementarán la lógica de negocio definida en los casos de uso o funcionalidades.

Ventajas de las arquitecturas orientadas a microservicios:

- Facilita el desarrollo, testing y despliegue: cada elemento cubre una funcionalidad muy reducida. Las iteraciones son más rápidas y permite corregir rápidamente problemas.
- Mayor agilidad: varios equipos de desarrollo pueden estar trabajando en diferentes funcionalidades sin interferir, permitiendo desplegar nuevas funcionalidades sin tirar abajo

la aplicación y sin tener que lanzar una versión completa de la aplicación.

- Escalable horizontalmente: permite aumentar fácilmente el número de servicios en un pool, incluso de manera automatizada según las necesidades.
- Múltiples tecnologías: permite trabajar e integrar múltiples tecnologías y lenguajes de programación fácilmente, en función de las necesidades de cada funcionalidad o de las propias capacidades de los desarrolladores.

Inconvenientes de las arquitecturas orientadas a microservicios:

- Mayor complejidad: dividir una aplicación en microservicios independientes genera más elementos para gestionar, lo que requiere una planificación cuidadosa.
- Necesidad de prestar atención a la seguridad: al utilizar APIs entre los microservicios para comunicarse es necesario prestar especial atención para implementar las medidas de seguridad necesarias.

4.5.2.1.5. Resumen de aproximaciones

A continuación, se presenta una tabla con las diferencias entre las respectivas aproximaciones respecto al punto de vista de desarrollo de plataformas de procesamiento distribuido.

Actualmente el modelo más utilizado para desarrollar arquitecturas de plataformas distribuidas es el enfoque de microservicios, este tipo de sistemas permite a diferentes equipos desarrollar en paralelo de manera desacoplada y usar los mejores lenguajes y herramientas de desarrollo para cada diferente funcionalidad. Además, este tipo de arquitectura permite tener amplia escalabilidad tanto horizontal como vertical, lo único que hay que tener en cuenta a la hora de utilizar este tipo de paradigma es el tamaño de los microservicios, teniendo en cuenta que al principio es interesante empezar con pocos de tal forma que se pueda ir más rápido, así como facilitar el "debugging" en caso de ser necesario.

4.5.2.2. Alternativas en el mercado para el encapsulamiento

Para desplegar y ejecutar una arquitectura basada en microservicios existen tres grandes aproximaciones:

- Virtualización de máquinas.
- Contenedores de servicios.
- Lambda, funciones como servicio en entornos sin servidores.

	Velocidad desarrollo (equipos pequeños)	Velocidad desarrollo (equipos grandes)	Actualizaciones & Configuración Centralizadas	Escalabilidad	Complejidad de debugging
Monolíticas	XXX	X	No	X	X
Cliente-Servidor	XXX	X	Sí	XX	XX
SOA	XX	XX	Sí	XX	XX
Microservicios	XX	XXX	Sí	XXX	XXX

Tabla 2: Comparación de arquitecturas SW.

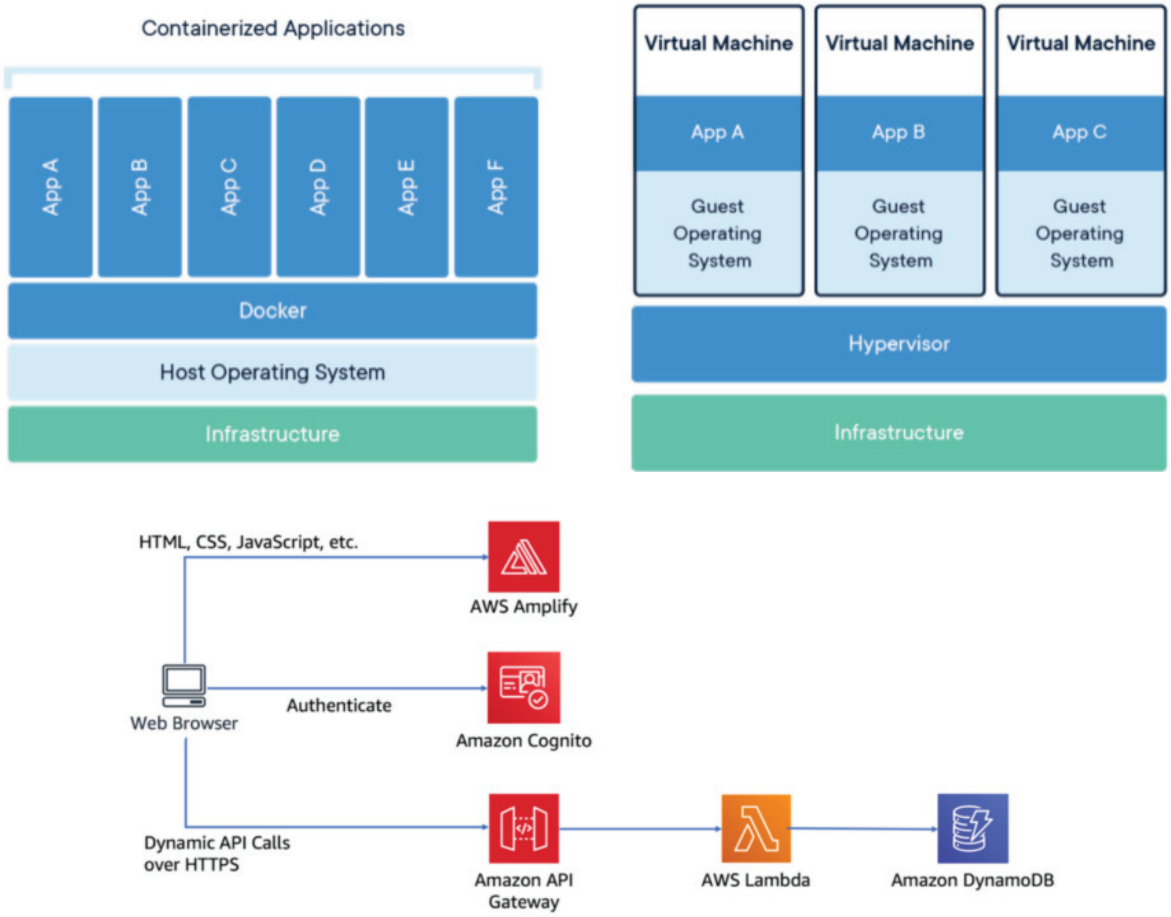


Figura 16: Tendencias de encapsulamiento en contenedores, máquinas virtuales y funciones.

4.5.2.2.1.Máquinas virtuales

Una máquina virtual es una imagen completa de un sistema operativo (guest) ejecutándose sobre otro sistema operativo (host), que a través de lo que se conoce como hypervisor expone los recursos físicos (RAM, CPU, disco, etc) a la máquina virtual.

Esta aproximación permite ejecutar aplicaciones en un sistema concreto independientemente de la plataforma que utilice el servidor, incluso lanzando varias máquinas virtuales en paralelo. Pero requiere ejecutar un sistema operativo completo en cada máquina virtual, lo que añade una sobrecarga en el uso de los recursos de la máquina host.

Últimamente existe una vertiente hacia la virtualización ligera con sistemas tipo Firecracker[2]. Este tipo de sistemas son los utilizados por los proveedores de nube pública normalmente para proveer de sistemas Serverless y poder asegurar la privacidad del código ejecutado.

4.5.2.2.2. Contenedores de aplicaciones

Los contenedores se basan en el concepto de virtualización del sistema operativo. Cada contenedor es un paquete cerrado de software que incluye una aplicación y todas las dependencias que necesita para ejecutarse.

La principal diferencia entre máquina virtual y contenedor es la forma en la que cada capa de virtualización utiliza los recursos de la máquina. En el caso de los contenedores, éstos comparten el kernel del sistema operativo del host, junto con binarios y librerías.

Los contenedores son mucho más ligeros que las máquinas virtuales, ocupan menos espacio de disco y arrancan en cuestión de unos pocos segundos como mucho.

Aunque los contenedores tienen más de 10 años de historia y existen varias implementaciones, ha sido gracias a Docker que se haya popularizado y consolidado, llegando a convertirse

[2]https://aws.amazon.com/blogs/aws/firecracker-lightweight-virtualization-for-serverless-computing/

en la tecnología Open Source de facto para contenedores, utilizada por todos los grandes proveedores como Microsoft, Google y Amazon Web Services, y grandes compañías como Paypal o VISA.

4.5.2.2.2.1. Docker

Docker es una plataforma de virtualización ligera y un conjunto de herramientas que nos ayudan a:

- Aislar nuestros servicios y componentes dentro de contenedores Docker.
- Empaquetar y distribuir los contenedores sobre nuestros entornos.
- Desplegar los contenedores en nuestro entorno productivo (Cloud o Edge).

Sus principales características son:

- Aceleración del despliegue.
- Escalado sencillo.
- Permite entornos de alta densidad de servicios y carga.
- Proporciona un SaaS para compartir y manejar contenedores Docker.

Docker usa una arquitectura cliente/servidor. Gestionando las tareas de construir, ejecutar y distribuir los contenedores. Tanto el cliente como el servidor Docker pueden correr en el mismo sistema y se comunican vía TCP o a través de un API RESTful.

Los componentes sobre los que se basa la plataforma Docker son tres:

- **Imágenes Docker:** plantillas de sólo lectura, por ejemplo, un SO Ubuntu, una aplicación Spring Boot, etc.
- **Registros Docker:** se encargan de mantener las imágenes. El registro público se llama Docker Hub[4], pero se pueden utilizar también registros privados.
- **Contenedores Docker:** su contenido es similar a un directorio. Contienen todo lo necesario para ejecutar una aplicación. Pueden ser ejecutados, iniciados, parados, movidos, borrados, reemplazados, etc.

Todos los componentes de infraestructura indicados en el modelo de implementación conforman uno o varios contenedores Docker.

Cada uno de los microservicios se incorporan en un contenedor Docker.

4.5.2.2.3. Funciones como servicio (FaaS)

Los entornos de FaaS (Functions as a service) encapsulan y gestionan funciones abstrayendo al suministrador del código de aprovisionar ni administrar servidores.

El encapsulamiento en funciones permite ejecutar microservicios escritos en determinados lenguajes para casi cualquier tipo de aplicación o servicio backend sin tener que realizar tareas de administración.

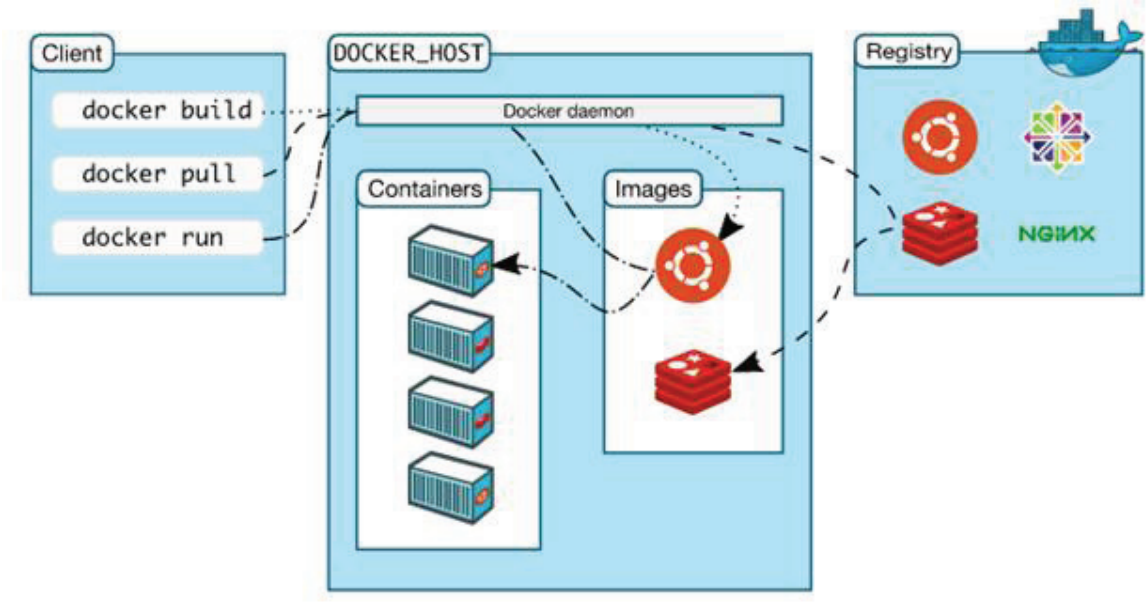


Figura 17: Arquitectura de funcionamiento de Docker.

[4]https://hub.docker.com/

La plataforma FaaS más extendida y con extensiones para su distribución Edge es AWS (https://docs.aws.amazon.com/lambda/latest/dg/lambda-app.html)

Las plataformas FaaS una vez cargada una función en un lenguaje compatible se encarga de todo lo necesario para ejecutar y escalar el código en alta disponibilidad y habilitar su acceso desde otras funciones o cualquier aplicación web o móvil.

Principales características del encapsulamiento en funciones

- Se encapsula el código del microservicio en alguno de los servicios soportados: Node .js, Java, Go, Python and C#
- Los microservicios se ejecutan en un runtime especializado que es el que proporciona el acceso a los recursos y la interacción con el resto de microservicios y el exterior.
- La plataforma FaaS realiza la administración y de las funciones (activación periódica o basada en eventos) gestión recursos: servidores, Sistema operativo, monitorización del código, logging, aprovisionamiento de recursos.
- El uso de la infraestructura cloud se factura cada vez que se ejecuta una función, en base a los recursos de ejecución necesarios y el tiempo de ejecución.

4.5.2.2.4. Comparativa alternativas encapsulamiento

En la tabla siguiente se resumen las características de las tres alternativas básicas de encapsulamiento potencialmente aplicables a la distribución Edge de funcionalidad.

Tipo de encapsulamiento	Qué se encapsula	Qué se comparte	Tamaño medio	Agilidad de arranque/ rendimiento	Modo de licenciamiento	Proveedores
Máquinas Virtuales	- Aplicaciones - Librerías - Sistema operativo	- Infraestructura	1 GB	Bajo. Acceso indirecto a infraestructura puede reducir el rendimiento	Propietario y Open Source	Propietarias: vmware hiper-v Oracle VM Open source Virtualbox Openstack KVM. ...
Contenedores de aplicaciones	- Aplicaciones -Librerías	- Sistema operativo - Infraestructura	5-100 MB	Alta Mejor rendimiento al reducir capas de abstracción	Open source	Open source Docker Cri-o
Funciones como servicio	-Código (Node .js, Java, Go, Python and C#)	- Runtime - Sistema operativo - Infraestructura	1KB – 1 MB	Muy alta. Rendimiento dependiente de eficiencia de run time. Comparable y superior a contenedores	Propietario pago por uso.	Propietarias: - AWS Lambda - Azure Functions - Google Cloud Functions. - IBM OpenWhisk Open source –Fn -OpenWhisk -OpenFaas

Tabla 3. Alternativas para el encapsulamiento de funciones en el SASCTI...

4.5.3. La distribución de la inteligencia. Edge, Core y Cloud

Las plataformas de procesamiento distribuido habilitan la distribución de la lógica de procesamiento, análisis y control en distintos niveles.

Las arquitecturas de tres capas, correspondiendo estas al conjunto formado por los dispositivos (edge devices), los nodos (edge servers) y la infraestructura (cloud), surgen para dar respuesta a los principales problemas asociados al procesado de los datos de manera centralizada. En muchos casos, la privacidad de los datos recogidos por los dispositivos en entornos de producción es un factor que determina la inviabilidad de su tratamiento directo en nubes públicas. Por otro lado, el ingente volumen de información bruta enviada hacia el Cloud provoca la sobrecarga de los recursos de red, haciendo necesario que una parte de esos datos se procesen en los nodos de manera distribuida. Adicionalmente, determinadas aplicaciones pueden conllevar una toma de decisiones en tiempo real y la latencia inherente al envío de datos al Cloud es incompatible con esta funcionalidad.

A menudo se refiere al edge como toda la computación fuera de la nube que ocurre en el borde de la red; en realidad, muchas soluciones adoptan un enfoque híbrido, procesando por lotes algunos de los datos en el edge, antes de enviarlos a un servidor de procesamiento intermedio lejos del sistema de nube centralizado (a veces también conocido como

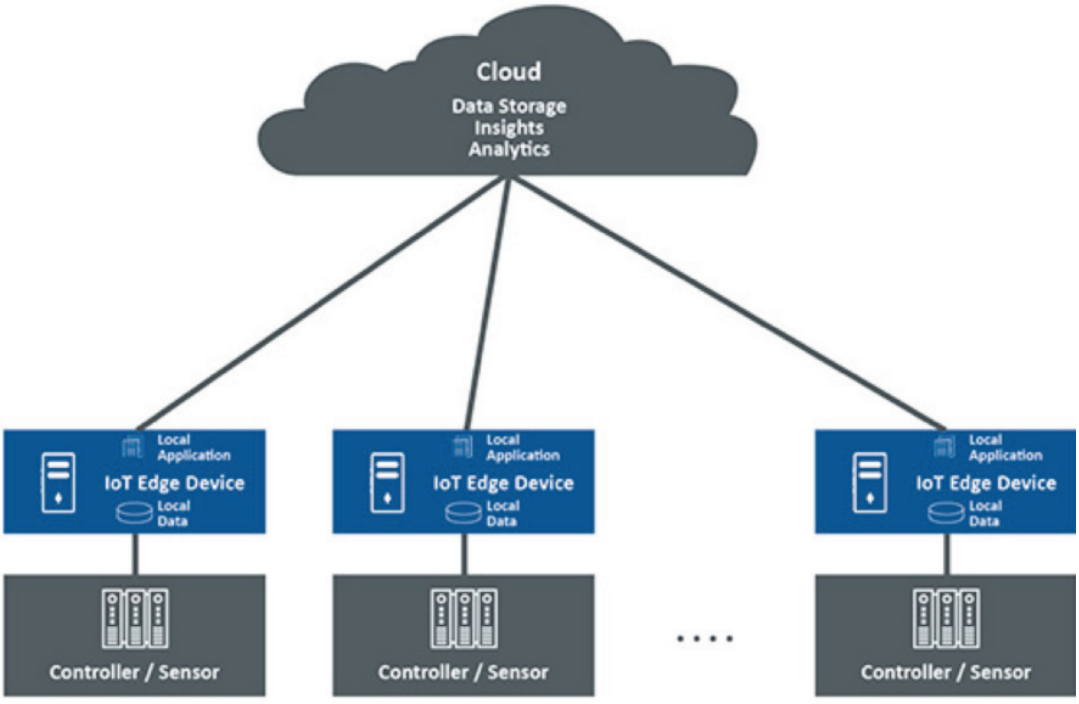


Figura 18: Ejemplo de arquitectura de tres capas.[5]

[5]https://www.controlengeurope.com/article/177728/From-the-cloud-to-the-edge.aspx

fog), o volver a la nube para actividades más exigentes como procesamiento de grandes volúmenes de información o almacenamiento de datos. En la siguiente figura se muestra una comparación en paralelo de la computación en la nube y en el borde.

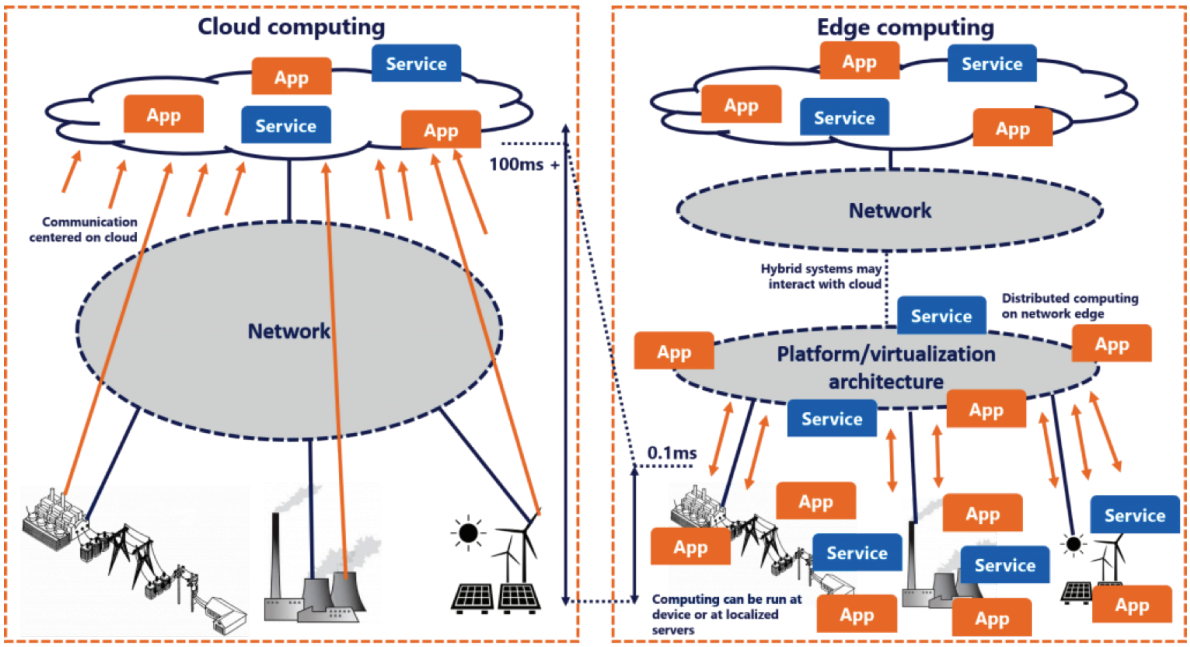


Figura 19: Dos posibles esquemas de distribución del procesamiento.

De este modo, el procesamiento se tiende a distribuir, utilizando las herramientas mencionadas a lo largo del estado del arte, beneficiándose por ejemplo de métodos de aprendizaje descentralizados. En estos, un modelo global es replicado en múltiples nodos, de forma que cada réplica continúa el entrenamiento de éste a partir de sus propios datos recogidos. Así, se crean diferentes subconjuntos del modelo global para posteriormente actualizarlo y hacerlo más consistente y, en definitiva, reducir notablemente los recursos necesarios en comparación con el equivalente centralizado.

La naturaleza heterogénea de este tipo de arquitecturas de tres capas da lugar a una serie de retos asociados a la gestión de la carga computacional de manera distribuida. Los requisitos más importantes a los que es necesario prestar especial atención son los siguientes:

- **Energía**: en entornos distribuidos, una parte de los nodos es posible que esté alimentada por baterías, ya sea por ser nodos integrados en componentes móviles o por no disponer de otro tipo de alimentación debido a su localización. Es por ello por lo que la gestión de la energía cobra vital importancia a través del uso de algoritmos y protocolos de comunicación eficientes.
- **Disponibilidad**: dado que las comunicaciones son un elemento esencial en este tipo de arquitecturas, es importante que se garantice la disponibilidad y calidad de estas. Para ello, una posibilidad es hacer uso de más de una interfaz de red, de manera que en cada momento se utilice la más apropiada en función de una serie de parámetros de monitorización.
- **Capacidad**: los métodos de aprendizaje distribuidos mencionados anteriormente se caracterizan por reducir significativamente el ancho de banda necesario. Sin embargo, hace falta considerar la totalidad de los datos que se van a trasmitir (actualizaciones del modelo, resultados, métricas, datos que

sí se procesan directamente en el Cloud...) para poder dimensionar el sistema adecuadamente.

- **Latencia**: si la aplicación en cuestión cuenta con requisitos de tiempo real para la toma de decisiones, es preciso prestar atención a la latencia de las comunicaciones. En general, el procesado de los datos en el Cloud cuenta con recursos computacionales "ilimitados", por lo que a priori el tiempo de computación va a ser menor que en el Edge y la limitación va a venir por la parte del envío y recepción de los datos. El procesado de datos en el Edge, a pesar de ser más lento, elimina esa latencia, por lo que se deberá computar cual es la vía más adecuada en cada caso.
- **Seguridad**: todo nodo que cuente con funcionalidades de adquisición, tratamiento o almacenamiento de datos debe cumplir una serie reglas que garanticen la seguridad e integridad de los propios datos. Este apartado está más ampliamente explicado en una sección dedicada del presente documento (ciberseguridad).

4.5.4. Gestión y orquestación

4.5.4.1. Gestión/Orquestación de entorno Cloud

Existen diferentes formas de gestionar y orquestar los distintos componentes que viven en entornos cloud. Últimamente la tendencia es usar sistemas que permiten gestionar mediante técnicas de DevOps (Infrastructure as Code) los recursos de cómputo de sistemas distribuidos como si de un único sistema se tratara.

- **Kubernetes**

  Kubernetes[6] Completamente de código abierto (Fully Open Source).

  Soporte "autogestionado" en todas las nubes. Ahora mismo es la tecnología más adoptada. Vía opciones como Anthos y plugins de malla como Calico o Itsio podemos gestionar cargas hibridas. Es decir, si un centro de transformación tiene cierta capacidad de cómputo podría entrar en esta categoría.

- **Nomad**

  Nomad[7] es un orquestador Open Source desarrollado como parte del ecosistema Hashicorp. Tiene versión OpenSource pero la funcionalidad avanzada y soporte sería de pago. Es un sistema interesante ya que permite ejecutar aparte de contenedores todo tipo de procesos usando los cgroups de Linux. Mediante políticas de red de Consul, sistema de DNS y descubrimiento de servicios desarrollado por Hashicorp, también podemos gestionar cargas entre diferentes redes por lo que esta característica podría utilizarse para entornos Edge.

  Consul tiene un "sidecar" que permite añadir de manera sencilla este tipo características a nuestros servicios sin que haya realizar cambios en ellos.

- **Mesos**

  Mesos[8] es un proyecto nacido de la universidad de Berkley y adoptado por empresas como Twitter o Apple. Es el sistema más avanzado desde el punto de vista de gestión de recursos, así como capacidades de orquestación. Aparte, es el orquestador que mejor soporte para entornos Big Data provee, sin embargo, Kubernetes con el apoyo de la comunidad le está alcanzando rápidamente. Como Nomad, permite la gestión de procesos aparte de contenedores. Su sistema de gestión de dos capas permite hacer virguerías como ser capaz de correr varios clústeres de Kubernetes dentro. Fully Open Source, pero para montarse algo en producción mejor ir a la opción de pago (DC/OS). Tiene soporte para cargas hibridas, pero dada la complejidad de la solución es descartable su posible uso en entornos Edge.

4.5.4.2. Gestión y orquestación entre el Cloud y el Edge

Dado que los recursos en el Edge son considerados limitados, las herramientas de gestión y orquestación entre el Cloud y el Edge se basan finalmente en herramientas de gestión remota de contenedores, en algunos casos con alguna particularidad añadida. Algunas de las herramientas más utilizadas son las siguientes:

[6]https://kubernetes.io/
[7]https://www.nomadproject.io/
[8]http://mesos.apache.org/

- **KubeEdge**[9]: herramienta de código abierto que extiende la orquestación de contenedores de aplicaciones y la gestión de los dispositivos a los nodos Edge. Está construida sobre Kubernetes y proporciona soporte de gestión de red, despliegue de aplicaciones y sincronización de metadatos entre el Cloud y el Edge.
- **Nebula**[10]: orquestador de contenedores cuyo objetivo es proporcionar una capa de abstracción de forma que los dispositivos IoT puedan ser tratados como contenedores de aplicaciones distribuidos. Está especialmente diseñado para no imponer límites a la hora de escalar el número de nodos, así como para tolerar diversos problemas de red.
- **Swarm**[11]: funcionalidad nativa de Docker que permite la gestión de clústeres de nodos ejecutando Docker. Cuenta con un diseño descentralizado, opciones de escalado o herramientas de gestión de carga, entre otros.

Existen otras soluciones más específicas para la orquestación entre el Cloud y el Edge. **AWS IoT Greengrass** proporciona una serie de conectores entre los nodos Edge y el Cloud de forma que todo ello es fácilmente integrable en el conjunto AWS, como se describe en la sección 5.1.6.3. Por otra parte, existe también el equivalente de Microsoft con Azure IoT, en el que cabe destacar **Azure IoT Edge**[12], un plugin de Jenkins que permite configurar un entorno de integración y despliegue continuos de dispositivos IoT. Asimismo, Azure tiene la posibilidad de mover de manera dinámica contenedores de la nube a dispositivos Edge. De manera adicional, existen soluciones menos extendidas pero cuyo cometido es el mismo, como **Nuvla**[13], que proporciona un entorno continuo de orquestación de nodos desde el Edge hasta el Cloud.

4.5.4.3. DevOps

El término DevOps, que es una combinación de los términos ingleses Development (desarrollo) y Operations (operaciones), designa la unión de personas, procesos y tecnología para ofrecer valor a los clientes de forma constante.

DevOps permite que los roles que antes estaban aislados (desarrollo, operaciones de TI, ingeniería de la calidad y seguridad) se coordinen y colaboren para producir mejores productos. Al adoptar una cultura de DevOps junto con prácticas y herramientas de DevOps, los equipos adquieren la capacidad de responder mejor a las necesidades de los clientes, aumentar la confianza en las aplicaciones que crean y alcanzar los objetivos empresariales en menos tiempo.

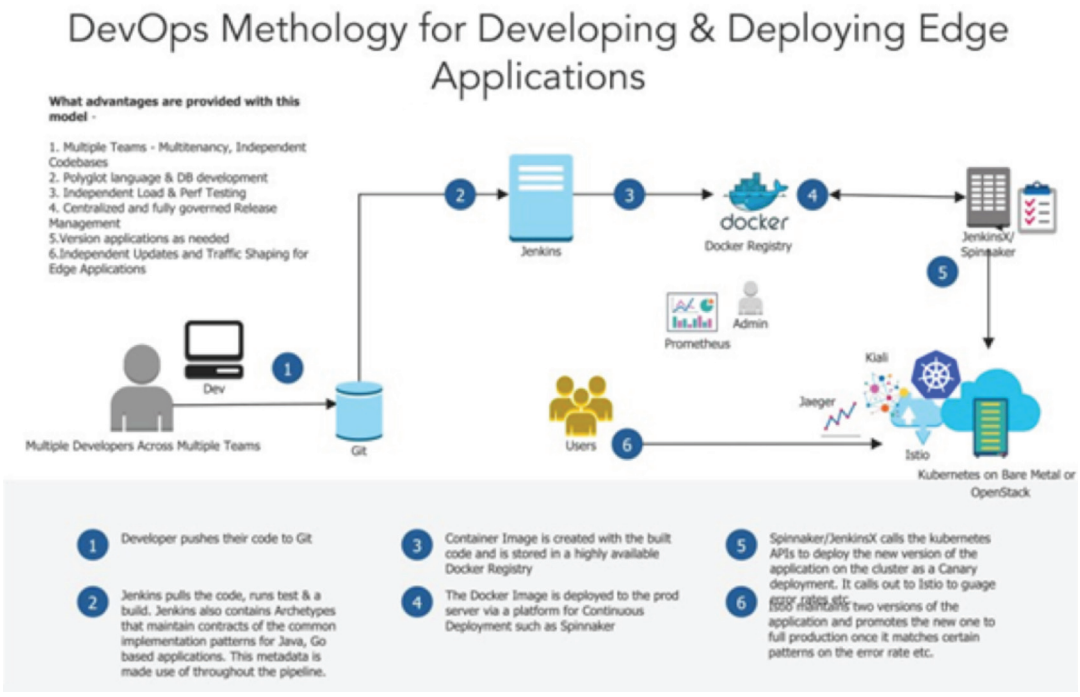


Figura 20: metodología DevOps aplicada al desarrollo Edge.

[9] https://kubeedge.io/en/
[10] https://nebula-orchestrator.github.io/
[11] https://docs.docker.com/engine/swarm/
[12] https://plugins.jenkins.io/azure-iot-edge/
[13] https://sixsq.com/products-and-services/nuvla/overview

La metodología DevOps, utilizada para desarrollar y desplegar aplicaciones en el "borde" de la red, ayuda a resolver los retos operativos de la administración de los contenedores facilitando la combinación de muchos microservicios y una mayor frecuencia de publicación, lo que se traduce en una mayor cantidad de implementaciones.

4.5.4.3.1. Ventajas de DevOps

Esta mejora de la colaboración y la productividad es fundamental también para alcanzar objetivos de negocio como:

- Reducción del tiempo de comercialización.
- Adaptación al mercado y a la competencia.
- Mantenimiento de la estabilidad y la confiabilidad del sistema.
- Mejora del tiempo medio de recuperación.

4.5.4.3.2. DevOps y el ciclo de vida de las aplicaciones

DevOps influye en el ciclo de vida de las aplicaciones a lo largo de las fases de planificación, desarrollo, entrega y uso. Cada fase depende de las demás y las fases no son específicas de un rol. En una auténtica cultura de DevOps, todos los roles están implicados de algún modo en todas las fases:

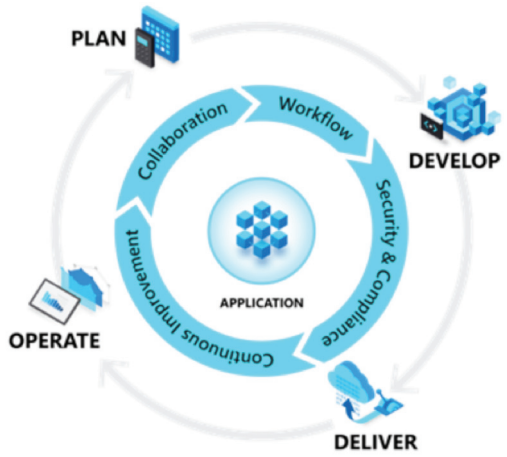


Figura 21: Fases del desarrollo DevOps.

En la fase de **planificación**, los equipos de DevOps conciben, definen y describen las características y la funcionalidad de las aplicaciones y los sistemas que van a crear. La creación de registros de trabajo pendiente, el seguimiento de los errores, la administración del desarrollo de software ágil con Scrum, el uso de paneles Kanban y la visualización del progreso son algunas de las formas en las que los equipos de DevOps planean con agilidad y visibilidad.

La fase de **desarrollo** incluye todos los aspectos de la programación (escritura, pruebas, revisión e integración del código por parte de los miembros del equipo) y la compilación de ese código en artefactos de compilación que se pueden implementar en varios entornos. Los equipos de DevOps automatizan los pasos rutinarios y manuales, e iteran el código en pequeños incrementos mediante pruebas automáticas e integración continua.

La **entrega** es el proceso de implementar aplicaciones en entornos de producción de un modo constante y confiable. En la fase de entrega, los equipos definen un proceso de administración de versiones con fases de aprobación claras. La automatización de estos procesos hace que estén controlados y sean escalables y repetibles.

La fase de **uso** implica mantener y supervisar las aplicaciones, así como solucionar los posibles problemas, en los entornos de producción. Los equipos de DevOps buscan identificar los problemas antes de que afecten a la experiencia del cliente y mitigarlos rápidamente a medida que surgen.

4.5.4.3.3. Prácticas de DevOps

La implementación de una metodología DevOps implica adopción de las siguientes prácticas:

- **Integración y entrega continuas (CI/CD):** es una práctica de desarrollo de software en la que los desarrolladores fusionan mediante combinación los cambios de código en la rama de código principal con frecuencia. En la integración continua se utilizan pruebas automáticas, que se ejecutan cada vez que se hace "commit" de código nuevo. De este modo, el código de la rama principal siempre es estable, se reducen los problemas que pueden surgir en ese proceso y se permiten actualizaciones más frecuentes.
- **Control de versiones:** es la práctica de administrar el código por versiones, haciendo un seguimiento de las revisiones y del histo-

rial de cambios para facilitar la revisión y la recuperación del código.

- **Desarrollo ágil de software**: el método ágil es un enfoque de desarrollo de software que hace hincapié en la colaboración en equipo, en los comentarios de los clientes y usuarios, y en una gran capacidad de adaptación a los cambios mediante ciclos cortos de lanzamiento de versiones. Kanban y Scrum son dos marcos populares asociados al método ágil.
- **Infraestructura como código:** define las topologías y los recursos del sistema de un modo descriptivo que permite a los equipos administrar esos recursos igual que lo harían con el código. Las diferentes versiones de esas definiciones se pueden almacenar en sistemas de control de versiones, donde se pueden revisar y revertir, de nuevo, igual que el código.
- **Administración de configuración:** hace referencia a la administración del estado de los recursos de un sistema, incluidos los servidores, las máquinas virtuales y las bases de datos.
- **Supervisión continua:** supervisión continua significa tener visibilidad total y en tiempo real del rendimiento y el estado de toda la pila de aplicaciones, desde la infraestructura subyacente donde se ejecutan las aplicaciones hasta los componentes de software de niveles superiores. código.

4.5.5. Comparativa plataformas

El edge computing se está convirtiendo en una tendencia en los últimos años en la industria del IoT. En la actualidad, existen varios proyectos que intentan abordar este tema, proyectos que normalmente vienen apoyados por una empresa principal y alrededor una comunidad de colaboradores más o menos abierta.

Estas plataformas se diseñan para recoger, procesar y analizar información cerca de su origen sin tener que enviar toda la información a la nube y permitiendo dar una respuesta mucho más rápida en términos de latencia.

Alguna de las principales plataformas son las que se detallan en la tabla a continuación, aunque es necesario apuntar que existen otras que pudieran ser tomadas en consideración pero que no se mencionan por motivos de extensión del documento.

	Licencia	Link
EdgeXFoundry	Open source	https://www.edgexfoundry.org/
Eclipse Kura	Open source	https://www.eclipse.org/kura/
Google Cloud IoT Edge	Free to use, ligada a plataforma Google Cloud	https://cloud.google.com/blog/products/gcp/bringing-intelligence-edge-cloud-iot
AWS IoT Greengrass	Free to use, ligada a plataforma AWS	https://aws.amazon.com/es/greengrass/
MS Azure IoT Edge	Open source, ligada a plataforma Azure	https://azure.microsoft.com/es-es/services/iot-edge/
IBM Edge Application Manager	Comercial	https://www.ibm.com/es-es/cloud/edge-application-manager
Minsait Oneasait Things	Plataforma abierta basada en estándares open source + Solución comercial para la monitorización y gestión local y central de despliegues Edge	https://www.onesait.com/products/things
Nutanix Intelligent Edge	Comercial	https://www.nutanix.com/es/products/iot
CISCO	Comercial	
Pixeom (Siemens)	Startup, basado en Open Source	https://www.pixeom.com
Zededa	Startup, basado en Open Source	https://www.zededa.com

Tabla 4. Plataformas de computación distribuidas consideradas.

En los siguientes apartados analizaremos brevemente alguna de las opciones con más fuerza en la actualidad.

4.5.5.1. Edge X Foundry

Es un proyecto Open Source con cierto recorrido, creado por la Linux Foundation en 2017. Su objetivo es proporcionar interoperabilidad y ser agnóstico de la plataforma software que se utilice a nivel de SO. El ecosistema que define permite integrar fácilmente múltiples componentes y que puedan ser desplegados fácilmente en una plataforma edge.

Se basa en una arquitectura de microservicios, donde los diferentes componentes se empaquetan como contenedores Docker. La comunicación entre los diferentes servicios se realiza a través de servicios API REST.

El núcleo de EdgeX[14] se ha migrado recientemente a Go para mejorar la falta de rendimiento y el excesivo uso de recursos de las primeras versiones.

Su principal contribuidor es Dell y está disponible con licencia Apache.

4.5.5.2. Eclipse Kura

Fue uno de los primeros proyectos Open Source para edge computing y tiene 6 años de recorrido, en los cuales se ha popularizado como framework para el IoT en el edge. Se basa en Java/OSGi y soporta una gran variedad de protocolos industriales (e.g. Modbus, OPC-UA, S7). Permite también la conexión a nubes remotas a través de MQTT.

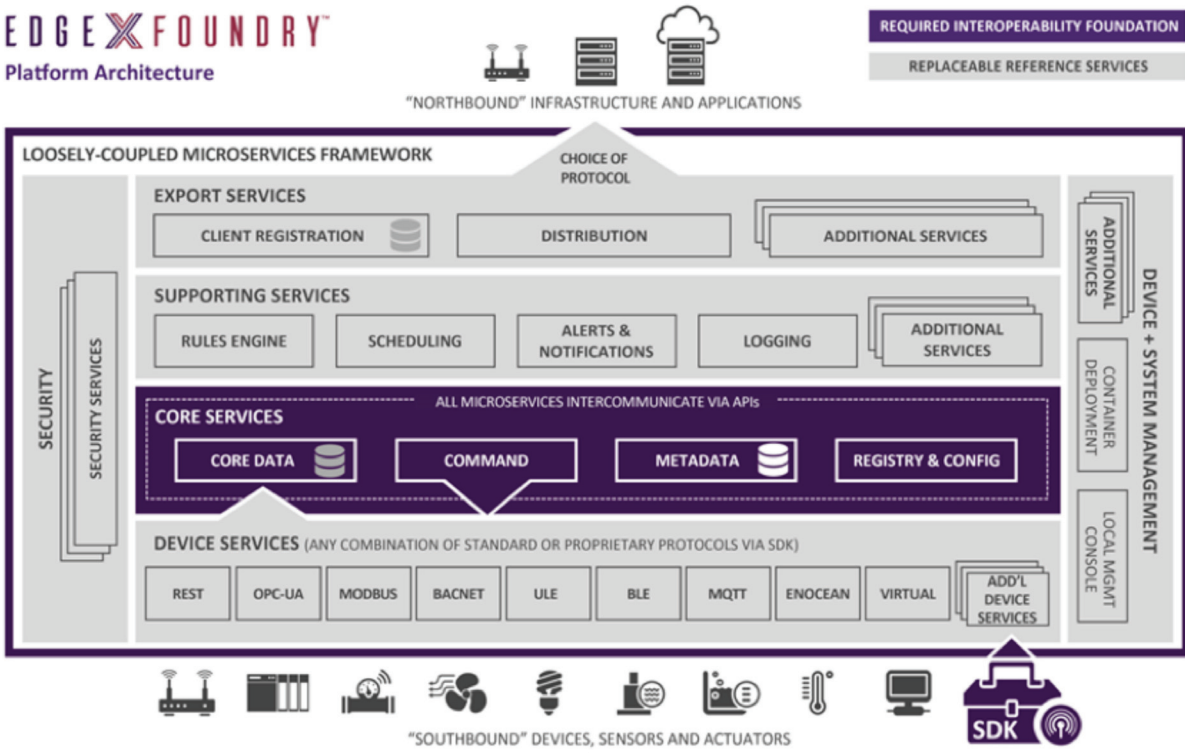


Figura 22: Arquitectura plataforma Edge X Foundry.

[14] https://www.edgexfoundry.org/

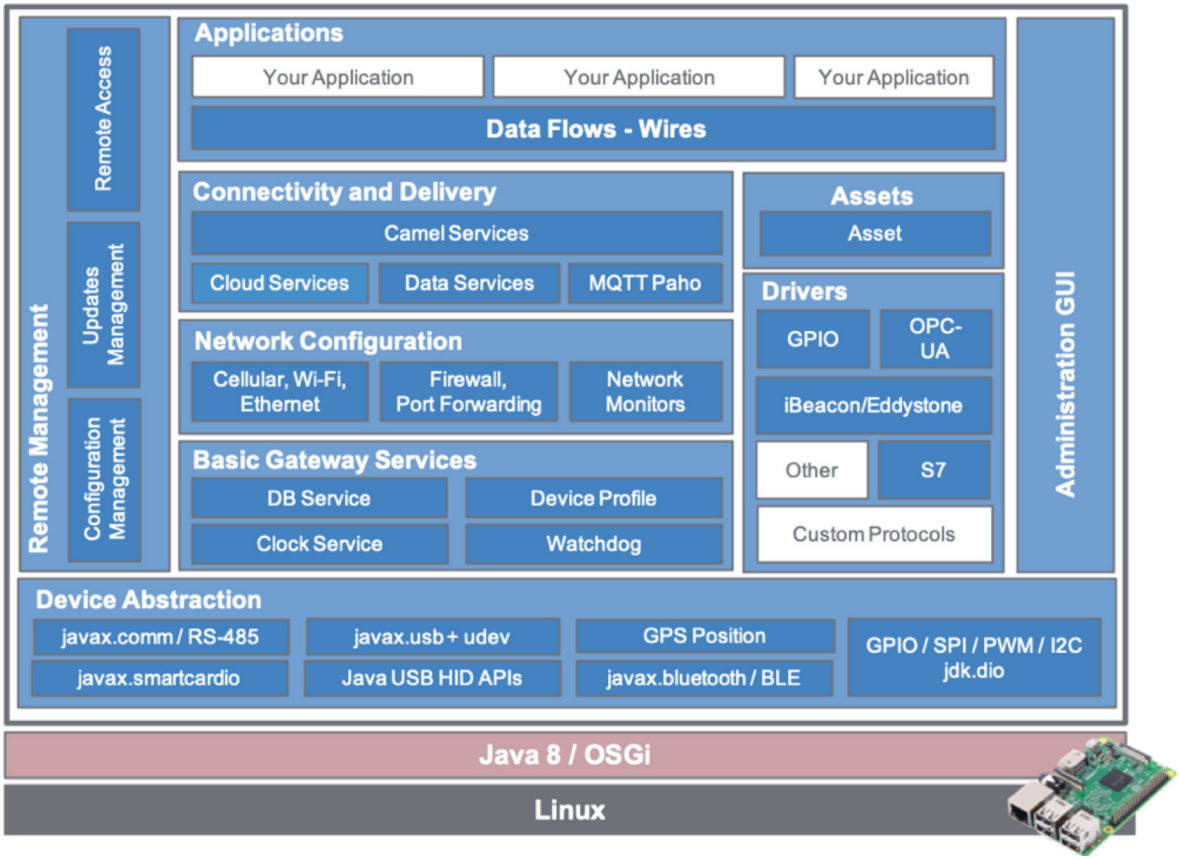


Figura 23: Arquitectura plataforma Kura.

La mayor parte de los componentes de Kura[15] son en Java, aunque se pueden invocar otros a través de JNI y depende en el sistema operativo Linux como base.

Su principal contribuyente es Eurotech y se licencia bajo los términos de la Eclipse Public License.

4.5.5.3. Google Cloud IoT Edge

Los esfuerzos de Google se han centrado en desarrollar una plataforma de Edge-Computing que extiende las capacidades actuales de Cloud-Computing y Machine Learning sobre dispositivos Edge[16].

Google no solo se ha centrado en desarrollar el software necesario para soportar la arquitectura, sino que también está trabajando en dispositivos físicos para colocar en los extremos de la red, además de contar con partners tecnológicos que proporciones todo el hardware necesario para integrar e implementar la red[17].

[15]https://www.eclipse.org/kura/

[16]https://cloud.google.com/solutions/iot3

[17]https://cloud.google.com/blog/products/gcp/bringing-intelligence-edge-cloud-iot

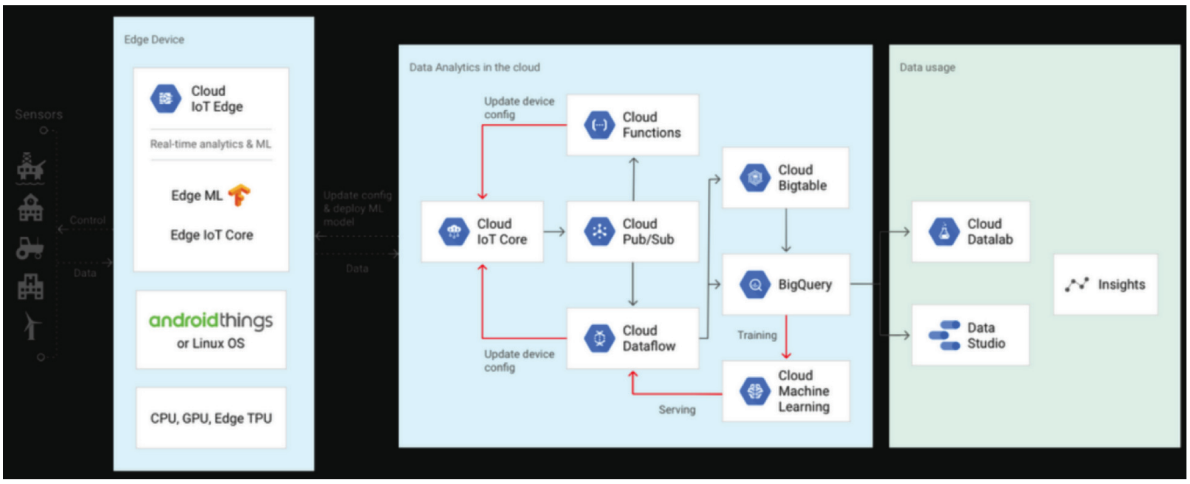
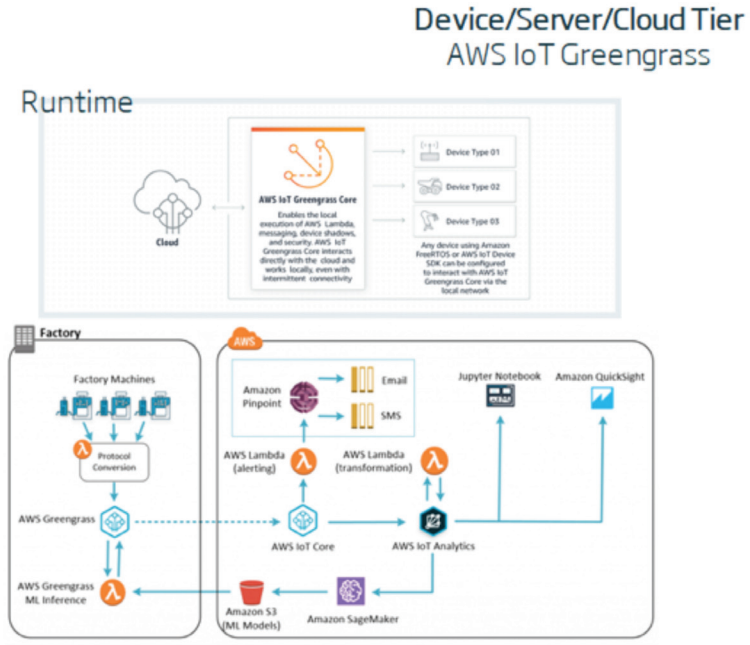


Figura 24: Arquitectura Google Cloud IoT Edge.

4.5.5.4. AWS Greengrass

AWS Greengrass[18] es la solución software proporcionada por AWS para extender sus servicios en la nube al edge, permitiendo a los dispositivos edge manejar localmente los datos que recibe o genera, mientras que se integra con la nube para el almacenamiento durable y funciones avanzadas de analítica.

Fue lanzada por AWS en 2017, y permite utilizar conceptos existentes en la nube, como las funciones Lambda y manejo de shadows, de forma local sin estar conectado a la nube. Permite también desplegar muy fácilmente modelos de ML, mientras se siguen entrenando en la nube.



AWS Lambda

Language or platform	GGC version
Python 3.7	1.9 or later
Python 2.7	1.0 or later
Java 8	1.1 or later
Node.js 12.x	1.10 or later
Node.js 8.10 *	1.9 or later
Node.js 6.10 *	1.1 or later
C, C++	1.6 or later

Figura 24: Esquema funcionamento plataforma AWS Greengrass.

[18]https://aws.amazon.com/es/greengrass/

Es una solución muy popular porque está nativamente integrada con AWS IoT Core, pero se trata de una solución cerrada, muy acoplada con los servicios de AWS en la nube y no es posible utilizar o migrar fácilmente a otro proveedor.

AWS[19] proporciona una variedad de servicios para los dispositivos de borde, como el AWS IoT Greengrass, que extiende AWS a los dispositivos de borde para que puedan actuar localmente en los datos mientras siguen utilizando la nube para la gestión, análisis y almacenamiento.

En el caso de AWS IoT Greengrass los servicios edge se distribuyen en funciones lambda que corren directamente sobre un runtime.

Estas funciones lambda tienen que estar programadas en determinados lenguajes que son los soportados por el runtime: Python, Java, Node.js, C/C++.

4.5.5.5. Microsoft Azure IoT Edge

Microsoft ofrece actualmente una solución Open Source para el IoT Edge[20], pero con la limitación de que está solución está atada al uso de la plataforma en la nube de Microsoft, Azure IoT. Este servicio fue lanzado un año después que AWS Greengrass, a principio de 2018.

Se basa en el uso de contenedores Docker y los componentes están escritos principalmente en C#. Incorporar características para ejecutar modelos de machine learning (ML) en el edge, pudiendo ser entrenados en su plataforma cloud y después desplegados en el edge fácilmente.

Azure Stack Edge[21], conocido anteriormente como Azure Data Box Edge, lleva la capacidad de proceso, el almacenamiento y la inteligencia de Azure (AI) ya sea su centro de datos corporativo, a su oficina o a un recurso de campo remoto.

Azure IoT Edge suministra el runtime Azure IoT Edge Runtime que gestiona el espacio de aplicaciones encapsuladas mediante contenedores docker. Adicionalmente suministra en cloud IoT Hub para la gestión cloud de los dispositivos Edge y de los contenedores desplegados, así como la gestión de sus flujos de información.

La coordinación Edge de los dispositivos Edge con su cloud se realiza a través de mensajería MQTT.

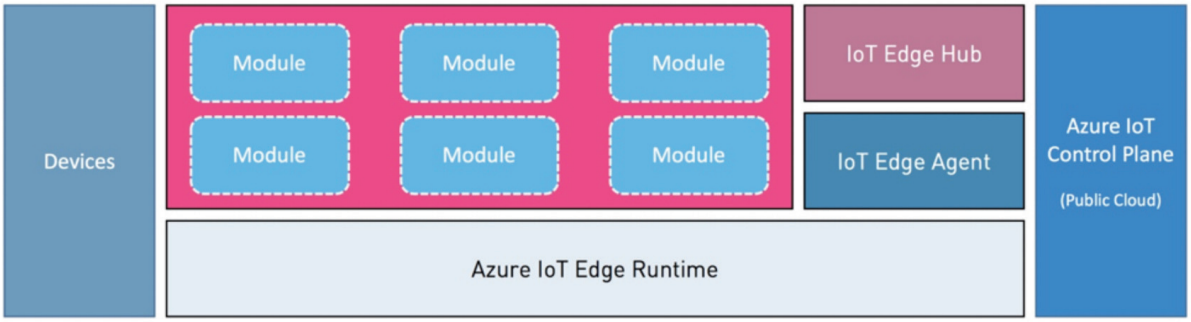


Figura 26: Arquitectura software genérica Azure IoT Edge.

[19] https://www.crn.com/slide-shows/internet-of-things/20-hot-edge-computing-companies-to-watch-in-2020/2

[20] https://azure.microsoft.com/es-es/services/iot-edge/

[21] https://docs.microsoft.com/es-es/azure/marketplace/iot-edge-module

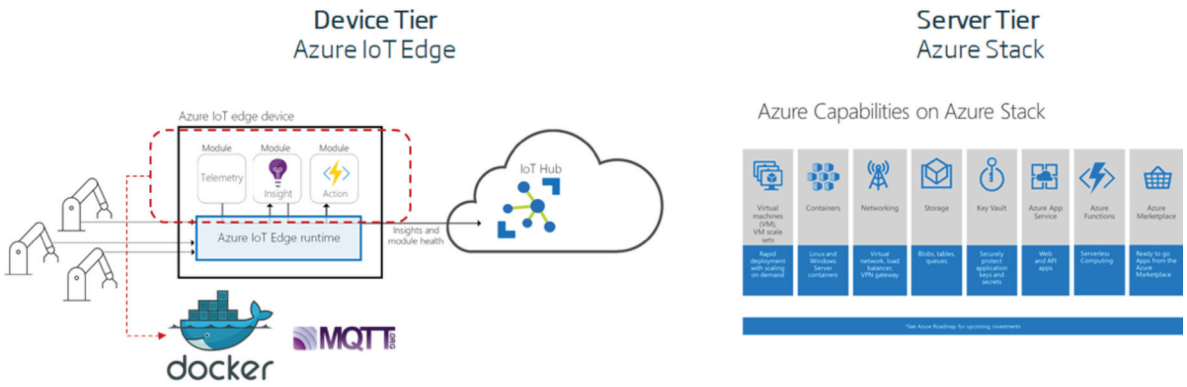


Figura 27: Arquitectura Azure Iot Edge.

4.5.5.6. IBM Edge Computing

Las soluciones de IBM[22] funcionan en Red Hat OpenShift, la plataforma empresarial líder de Kubernetes que se ejecuta en todas partes, desde el centro de datos OnPremises, en múltiples nubes públicas, y hasta el Edge.

IBM ha anunciado IBM Edge Ecosystem, para ayudar a las empresas a crear oportunidades de edge computing e IBM Telco Network Cloud Ecosystem, que reúne a un conjunto de socios de la industria de las telecomunicaciones para ayudar a los proveedores a implementar sus plataformas de red en la nube.

Estos ecosistemas abiertos incluyen a fabricantes de equipos, proveedores de redes y TI y proveedores de software, con miembros como Cisco, Dell Technologies, Juniper Networks, Intel, NVIDIA, Samsung, Packet, Equinix, Hazelcast, Sysdig, Turbonomic, Portworx, Humio, Indra Minsait, Eurotech, Arrow Electronics, ADLINK, Acromove, Geniatech, SmartCone, CloudHedge, Altiostar, Metaswitch, F5 Networks y ADVA

IBM Edge Computing encapsula las funciones/servicios mediante contenedores Docker gestionados mediante distintos agentes basados en Kubernetes.

IBM identifica cuatro capas en la arquitectura Edge:

1. Edge devices. Nivel de dispositivos inteligentes.
2. Edge Server Gateway. Nivel Edge gestionando directamente en campo los dispositivos.
3. Edge Network/Microdatacenter. Nivel Core, equivalente a despacho de control generalmente on-premise.
4. Enterprise Hybrid Multicloud. Nivel en nube cloud.

4.5.5.7. Minsait – Onesait Things

Minsait como parte de su plataforma IoT Onesait Platform, extiende la capacidad de procesamiento distribuido al Edge a través de Onesait Things,

Onesait Things es una plataforma modular e hibrida Cloud/core -Edge que permite cubrir el ciclo completo del dato de forma distribuida, así como hacer la gestión integral de dispositivos y nodos Edge tanto a nivel de información como de aplicaciones y analítica.

[22] https://www.datacenterdynamics.com/es/noticias/ibm-y-red-hat-lanzan-nuevas-soluciones-de-edge-computing-para-la-era-del-5g/

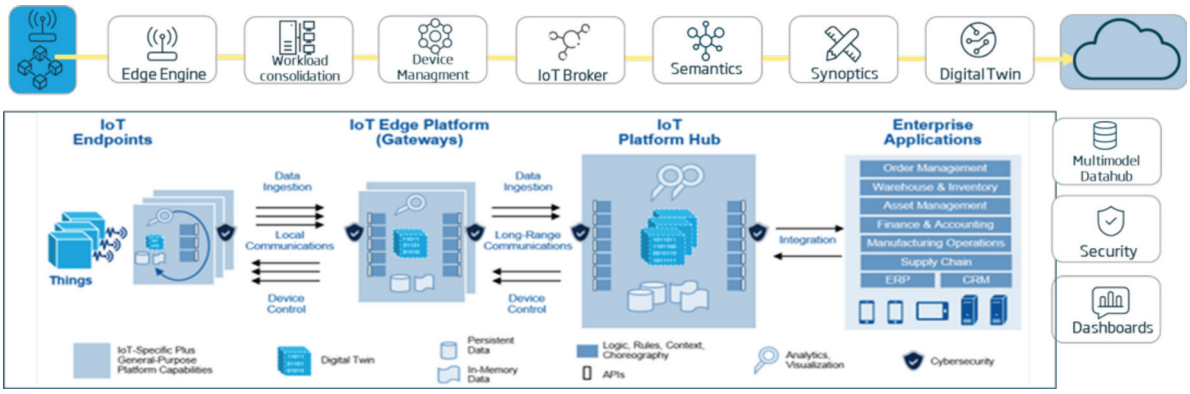


Figura 28: Arquitectura plataforma hibrida de gestión distribuida de Minsait Onesait Things.

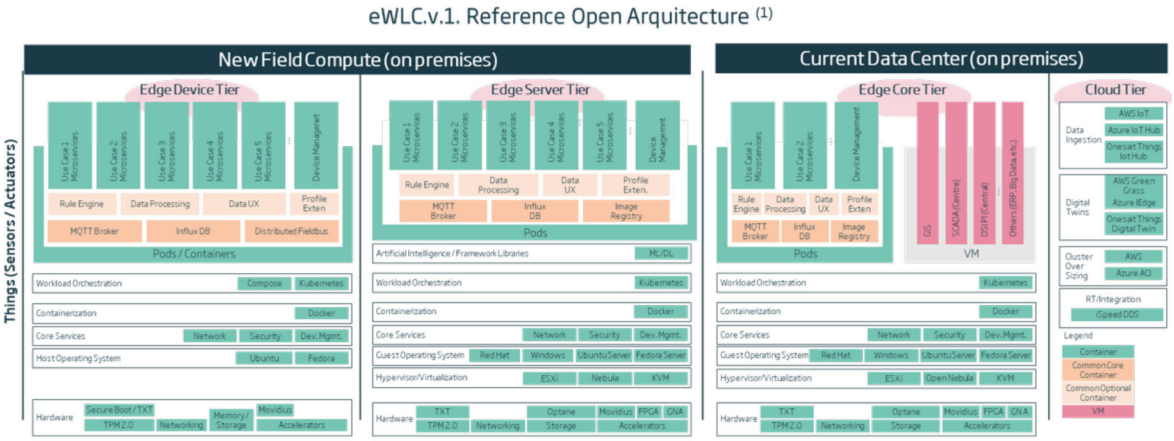
Las principales características de esta plataforma de computación distribuida son:

- **Estrategia híbrida.** Cloud2device o distribuida/Edge. Permitiendo la gestión dispositivo – cloud directa como dispositivo- Nodo Edge – Central.
- **Protocolos de IT / OT.** Los componentes de la plataforma incluye tanto:
  - Conectores OT industriales y específicos del sector eléctrico: OPC-DA, OPC-UA, modbus, 61850, PRIME-STG, 104, 101, DLMS, DNP3, ...
  - Conectores IoT/IT: middlewares de tiempo real DDS, mensajería MQTT, Kafka, ...
- Implementación **digital twin**. Habilitando un framework basado en WoT para la declaración, descubrimiento e intercambio de servicios entre dispositivos, aplicaciones y sistemas.
- **Independencia del hardware** implementado. Arquitecturas Intel y ARM compatibles.
- **Gestión proactiva de rendimiento y software de dispositivos y puertas de enlace.** Con una suit de herramientas orientadas a la monitorización y gestión integral de los dispositivos conectados en el Edge y la información generada y actuaciones habilitada por estos.
- **Seguridad extremo a extremo. Con bastionado del HW Edge, cifrado de comunicaciones y autentificación segura.**
- **Workload Consolidation.** Arquitectura de referencia Minsait-Intel eWLC.v.1, abierta para la distribución de inteligencia y balanceo de carga de procesamiento de la información entre los distintos niveles de la arquitectura distribuida.
- **Estrategia híbrida para procesar datos** cerca de donde se generan. Aumento de la velocidad, la seguridad y la reducción de costes.
- **Distribución optimizada de la carga** de trabajo entre nodos y servidores perimetrales.
- Convergencia en tiempo real IT / OT basado en modelos de Ontología para la integración semántica
- **Control proactivo, gestión y suministro de software** en cualquier punto del sistema. Habilita un entorno completo DevOps y herramientas empresariales para este control y gestión.
- **Componentes Edge optimizados** para minimizar los requerimientos de recursos HW en el borde de la red y el procesamiento en tiempo real con baja latencias s/ms.

Arquitectura:

Arquitectura distribuida en tres niveles:

- Edge device.
- Edge Server. Equipos intermedios entre el Edge Server y el cloud con mayor capacidad de procesamiento. Equivalente a los nodos distribuidos en una arquitectura Fog computing.
- Data Center. Cloud o centro de control.



(1) https://software.intel.com/www/us/en/develop/articles/edge-workload-consolidation-ewlc.html

Figura 29: Arquitectura plataforma Minsait Onesait Things Edge.

4.5.5.8. Nutanix: Intelligent Edge

La plataforma IoT de Nutanix proporciona computación local e Inteligencia Artificial a los dispositivos IoT en el Edge, convergiendo las ubicaciones (Edge, CPD, Cloud) en una plataforma transparente de procesamiento de los datos. La plataforma IoT elimina la complejidad, acelera los despliegues, y permite a los desarrolladores centrarse en la lógica de negocio de las aplicaciones y los servicios IoT. Los desarrolladores pueden utilizar una plataforma de desarrollo con codificación reducida para crear software de aplicaciones via APIs.

Gestión del ciclo de vida de aplicaciones e infraestructura a gran escala: Proporciona una infraestructura Edge transparente que permita el funcionamiento y despliegue sin conflictos o fricciones entre todos los intervinientes en la solución IoT, incluyendo a los usuarios finales, operadores TI, desarrolladores de aplicaciones, y data scientists.

Visibilidad de los datos con codificación reducida: Gestiona localmente y en tiempo real la información de los flujos de datos recibidos desde los sensores gracias a servicios y dataflows abiertos, mientras que permite que los datos una vez filtrados o transformados se dirijan de forma segura a su ubicación de destino utilizando servicios nativos. El PaaS (Platform-as-a-Service) en el Edge proporciona al desarrollador APIs, flujos de datos reutilizables, y una arquitectura de Machine Learning integrable para posibilitar el desarrollo rápido y el despliegue global de aplicaciones IoT modernas. La plataforma IoT permite incorporar de forma sencilla multitud de frameworks abierto al runtime, permitiendo entornos de runtime personalizados, e incorporar modelos ML de cualquier origen.

Convergencia entre ubicaciones: Permite mover los datos fácilmente desde los dispositivos en el Edge a cualquier ubicación (CPD, Cloud) según las necesidades de la aplicación IoT. Nutanix proporciona ciertas ventajas sobre las soluciones basadas en gateways tradicionales, que incluyen:

- Procesamiento en tiempo real en el edge para visibilidad de los datos resultantes en tiempo real.
- Metodologías de baja codificación para la migración de los datos resultantes a la ubicación requerida (CPD, Cloud).
- Implementación y Configuración sencilla con capacidad de gestionar miles de ubicaciones Edge desde un plano de control SaaS centralizado.

Arquitectura:

La solución IoT se compone de un plano de control SaaS y una plataforma Edge ejecutando en el dispositivo Edge. El plano de control SaaS proporciona una Plataforma completa gestionada de forma centralizada desde el cloud a través de una interfaz de usuario sencilla para el desarrollo de aplicaciones y las

operaciones para poder desplegar fácilmente miles de ubicaciones edge. Se puede desplegar la solución en el Edge en modo bare metal o como una máquina virtual en nodos dedicados o compartidos.

La Plataforma utiliza Kubernetes, que permite la consolidación de las aplicaciones tradicionales de IoT así como el desarrollo de aplicaciones de nueva generación basadas con capacidades de machine learning sobre contenedores.

4.5.5.9. Cisco Kinetic + IOx

CISCO[23] ofrece una gran cantidad de productos y servicios de vanguardia, desde servidores de construidos especialmente hasta hardware de redes de IOT. Cisco permite a los clientes desplegar servicios de borde de baja latencia en su infraestructura líder del mercado. Proporciona un camino hacia 5G, nuevas aplicaciones verticales, eficiencia de red y mejor latencia.

La plataforma Kinetic (IOx) encapsula la funcionalidad en forma de máquinas virtuales que habilitan espacios de ejecución Java y Python y suministra a través de servicios IOx la conectividad con los dispositivos, la persistencia y la conectividad cloud.

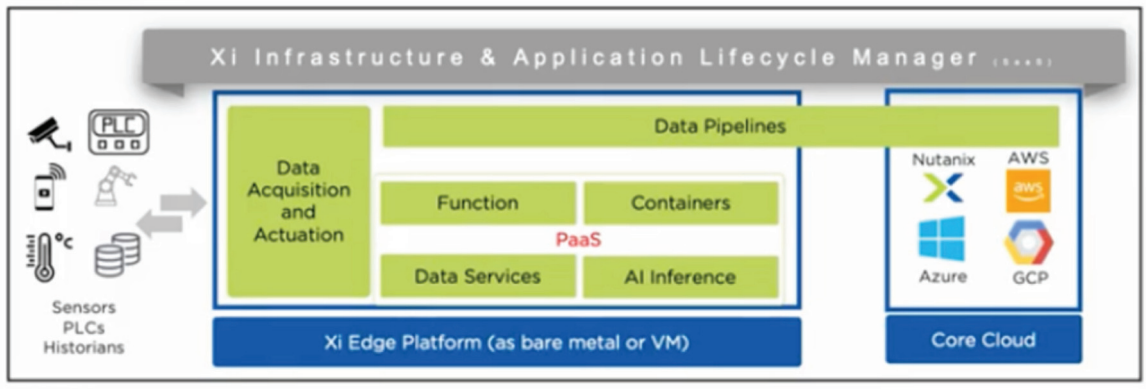


Figura 30: Stack PaaS de Edge Computing de Nutanix.

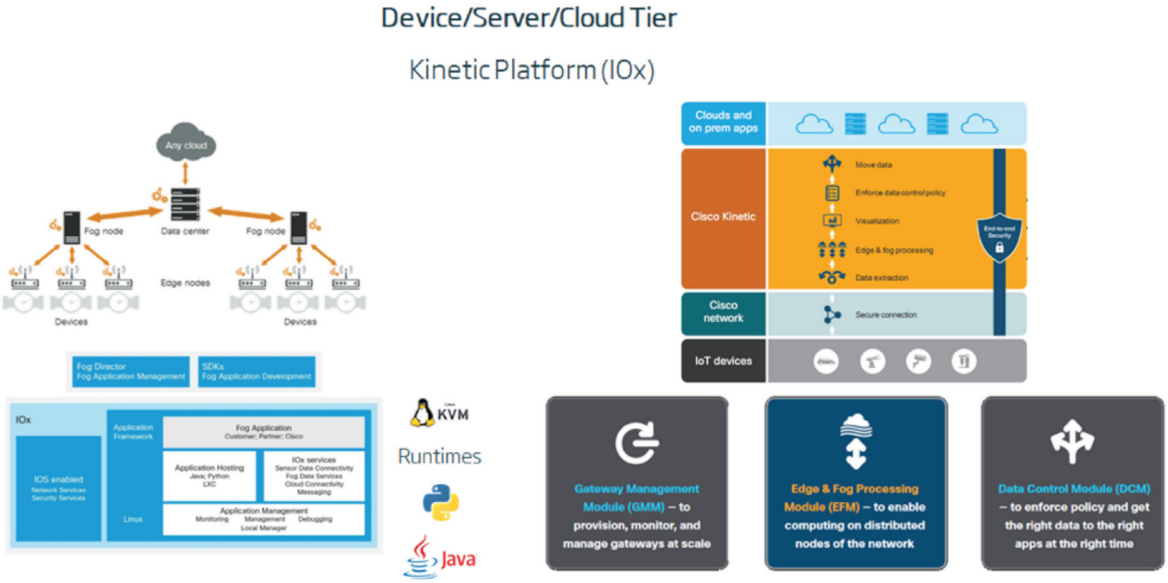


Figura 31: Arquitectura Kinetic IOx.

[23]https://www.crn.com/slide-shows/internet-of-things/20-hot-edge-computing-companies-to-watch-in-2020/3

4.5.5.10. Pixeom

Una de las capacidades clave de Pixeom es la capacidad de empaquetar, implementar y orquestar aplicaciones en la nube en hardware básico a través de la containerización, lo que brinda a las empresas la capacidad de ejecutar este tipo de aplicaciones en servidores perimetrales y locales sin necesidad de ninguna configuración de hardware específica.

Pixeom, fundada en 2014, recaudó 19,6 millones de dólares de Intel y National Grid y creó una plataforma informática de vanguardia que puede ejecutar múltiples aplicaciones. Sin la necesidad de comprar hardware para ejecutar el software, la puesta en marcha se ha reducido para los nuevos usuarios del edge. La capacidad de ejecutar varias aplicaciones en el mismo dispositivo periférico de forma aislada también reduce los costos debido a la consolidación del servidor. Los sectores de energía e industrial representaron el 30% de los ingresos y el 50% del crecimiento. Los clientes de energía han informado de una reducción del 20% en los costos de mantenimiento, reparación y operaciones, así como una reducción en el inventario de seguridad y los costos administrativos para administrar y reabastecer el inventario.

En octubre de 2019, Pixeom fue adquirida por Siemens en su parte de negocio de automatización industrial. Permitir un ecosistema abierto para aplicaciones y dispositivos de diferentes fabricantes es un componente clave, según la compañía.

En el lado del software, Pixeom es relativamente independiente de la nube. Una característica de la plataforma es que es compatible con API con Google Cloud Platform, AWS y Azure y ofrece un subconjunto extenso de los servicios de computación y almacenamiento central de esas plataformas, incluido un conjunto de herramientas de aprendizaje automático. La implementación de Pixeom puede ser diferente, pero para una aplicación, el edge device en una máquina Pixeom reacciona de la misma manera que su equivalente en AWS, por ejemplo.

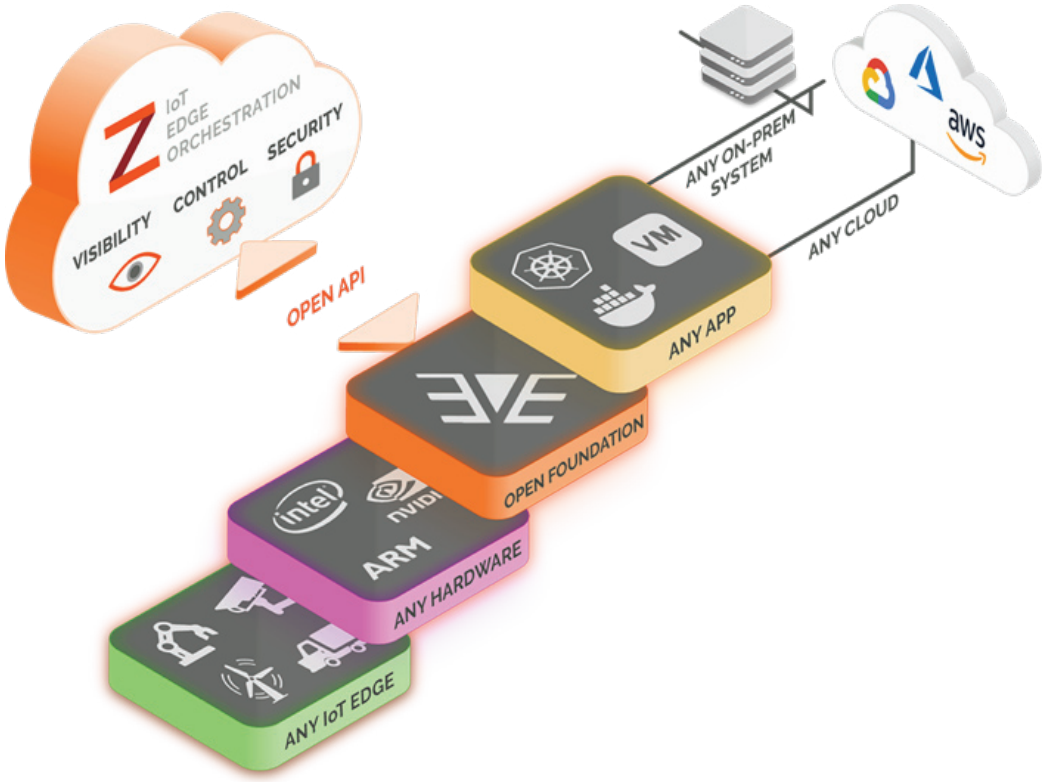


Figura 32: Arquitectura Pixeon Edge (SIEMENS Industrial Edge).

4.5.5.11. Zededa

ZEDEDA es una solución de orquestación de edge simple y escalable basada en la nube que brinda visibilidad, control y seguridad para el edge distribuido con la libertad de implementar y administrar cualquier aplicación en cualquier hardware a escala y conectarse a cualquier nube o sistemas locales. Con ZEDEDA, los clientes ahora pueden implementar y administrar sin problemas cualquier dispositivo de cómputo de edge para aprovechar instantáneamente el valor de los datos de IoT, tomar decisiones en tiempo real, maximizar la eficiencia operativa e impulsar nuevos resultados comerciales.

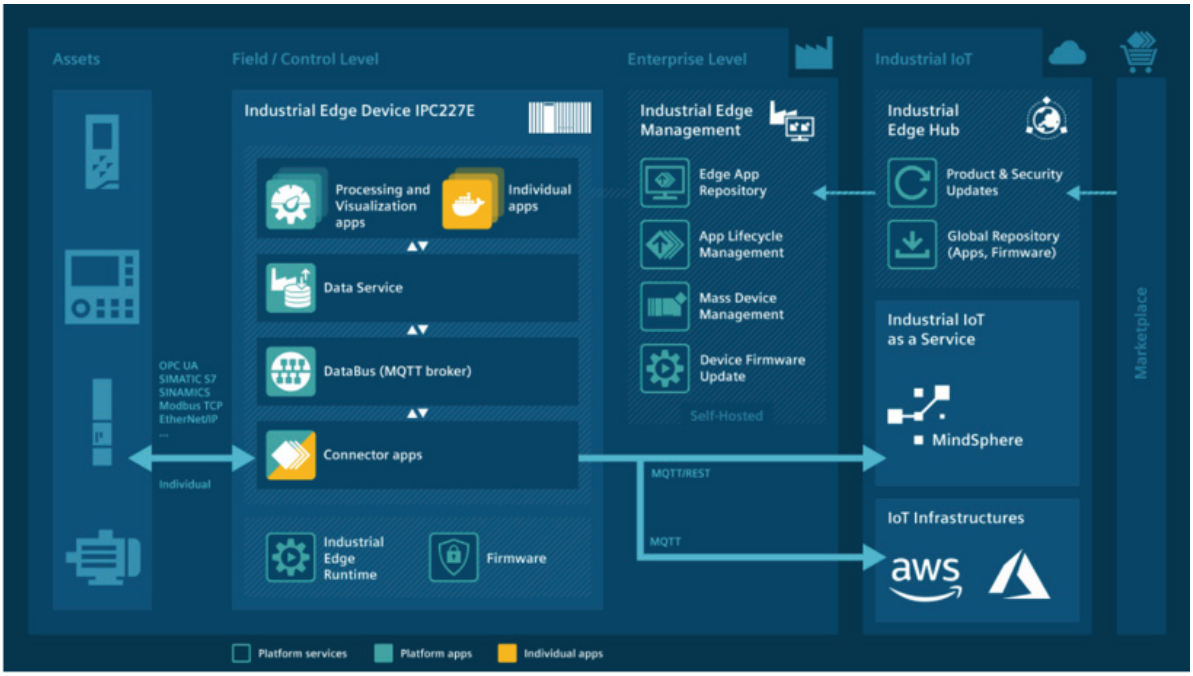


Figura 33: Arquitectura Zededa.

ZEDEDA aprovecha el Proyecto EVE, un motor de procesamiento distribuido de código abierto, independiente del proveedor, como parte de la organización LF Edge de la Fundación Linux. El propósito de EVE es simplificar la implementación, la orquestación y la seguridad de las aplicaciones heredadas y nativas de la nube en los nodos edge distribuidos. EVE cifra los datos, mantiene la integridad del software y del dispositivo a través de la raíz de confianza del hardware (por ejemplo, TPM) y admite máquinas virtuales, contenedores y clústeres (Docker y Kubernetes) para crear una base flexible para que los clientes consoliden cargas de trabajo e implementaciones de borde preparadas para el futuro.

4.5.5.12. Ressmen comparativa plataformas.

Se recoge a continuación en formato tabular las características de las principales plataformas analizadas.

Plataforma	Encapsulamiento Funciones	Componentes	Comunicaciones			Especialización red eléctrica
			Dispositivos Edge	Interna	Central	
EdgeXFoundry **https://www.edgexfoundry.org/**	Docker	Open source. Agnóstico plataforma Edge: - Conectores - Espacio virtual de contenedores con servicios core. - Servicios de gestión Edge. Core - Servicios de gestión remota. - Gestión despliegue contenedores.	REST OPC_US Modbus Bacnet ULE BLE MQTT	API Rest	MQTT	No IoT Generalista
Eclipse Kura **https://www.eclipse.org/kura/**	Aplicaciones Java / OSGI	Gestión OSGI de aplicaciones Java agnóstico de plataforma Edge: - Digital twin. - Conectores - Servicios de gestión Edge. Core: - Servicios de gestión Remota. - Servicios de despliegue de aplicaciones	GPIO OPC-UA iBeacon/ Eddystone S7	Web Services	MQTT	No IoT Generalista
Google Cloud IoT Edge **https://cloud.google.com/blog/products/gcp/bringing-intelligence-edge-cloud-iot**	Orientado a computación central Aplicaciones analíticas y Machine learning Tensor flow para control de flujo de información.	Servicios asociados a plataforma Google Cloud. Edge: - Servicios de gestión Edge. - androidthings para dispositivos Core Servicios Google Cloud - Cloud Analytics: Data lab/Insigths/Data Studio, Machine Learning - Cloud data storage. - Cloud Dataflow - Servicios de gestión Remota IoT Core	HTTP MQTT	API REST	HTTP MQTT	No IoT Generalista: - Energía. - Smart parking. - Transporte y logística.
AWS IoT Greengrass **https://aws.amazon.com/es/greengrass/**	Funciones lambda sobre runtime propietario: - Python - Java - Node.js - C,C++	Servicios asociados a plataforma Amazon. Edge: - Conversores Edge de protocolo - Soporte para funciones de ML Edge - Conectividad Edge. Core sobre Plataforma Cloud Amazon AWS IoT - Gestión despliegue funciones: Amazon S3.. - Monitorización remota AWS IoT Core - Servicios almacenamiento y analíticos.	HTTP MQTT		HTTP MQTT	No IoT Generalista: - Hogar conectado. - Agricultura. - Smart City

Plataforma	Encapsulamiento Funciones	Componentes	Comunicaciones			Especialización red eléctrica
			Dispositivos Edge	Interna	Central	
MS Azure IoT Edge **https://azure.microsoft.com/es-es/services/iot-edge/**	Docker	Servicios asociados a plataforma MS Azure Cloud. Edge Open Source: - Gestión de aplicaciones: Azure IoT Edge Runtime. - Analítica: Insigths Core Plataforma Cloud Azure IoT: - Gestión remota Edge: IoT Hub. - Gestión flujos de información. - Gestión de dispositivos y monitorización.	HTTP MQTT Web sockets	HTTP MQTT	HTTP MQTT AMQP	No IoT Generalista: - Salud - Comercialización. - Industria manufactura.
IBM Edge Application Manager **https://www.ibm.com/es-es/cloud/edge-application-manager**	Docker	Servicios de pago. Edge: - Orquestación OpenShift Core On-Premise o Cloud IBM Watson IoT Platform: - Gestión remota Edge: - Gestión de dispositivos - Analítica de tiempo real. - Blockchain	HTTP MQTT	HTTP MQTT	HTTP MQTT	No IoT Generalista: - Agricultura - Industria manufactura. - Edificios inteligentes
Minsait Oneasait Things **https://www.onesait.com/products/things**	Docker	Componentes agnósticos plataforma, despliegues on-Premise o en Cloud. Edge: - Sistema operativo Linux: standard - Orquestación open source: Compose/ Swarm/ Openshift - Gestión Edge monitorización y gestión de despliegues y contenidos: Agente Edge especializado comercial. - Conectores OT especializados para integración de dispositivos eléctricos. Core agóstico on-Premise o Cloud: - Sistema EMS de gestión central de despliegues Edge: dev_ops, securización, Monitorización y gestión central de dispositivos. - Gestión de dispositivos. - Plataforma IoT de historificación y analítica sobre información Edge.	Conectores OT industriales: OPC-DA, OPC-UA, modbus, DLMS, 61850, PRIME-STG, 104, 101, DLMS, DNP3, ... HTTP MQTT	MQTT HTTPS	Conectores IT-OT industriales: OPC-DA, OPC-UA, modbus, DLMS, 61850, PRIME-STG, 104, 101, DLMS,DNP3, ... HTTP MQTT TLS	Si. Despliegues en Centros de transformación Irlanda, España, USA y Australia. Casos de uso : control CT + gestión de BT+gestión de MT+ Seguridad + integración y gestión de recursos distribuidos RED

Plataforma	Encapsulamiento Funciones	Componentes	Comunicaciones			Especialización red eléctrica
			Dispositivos Edge	Interna	Central	
Nutanix Intelligent Edge **https://www.nutanix.com/es/products/iot**	Docker + funciones lambda + Aplicaciones sobre SO.	Plataforma cloud SaaS sobre cualquiera de los proveedores+ CaaS en el Edge. Edge: - Gestión kubernettes de contenedores y de funciones Lambda. - Servicios PaaS Da almacenamiento y analítica IA. Core sobre Plataforma Cloud SaaS - Gestión despliegue funcionalidad. - Monitorización remota Nodos Edge.	HTTP MQTT	HTTP MQTT	HTTP MQTT	IoT Generalista
CISCO	Máquinas Virtuales: Java y Python	Plataforma cloud SaaS sobre cualquiera de los proveedores+ CaaS en el Edge. Edge: - Servicios IOx de conectividad con dispositivos y cloud, securizada - Servicio de gestión de aplicaciones: Monitorización, gestión, depuración, gestión local. Core Cisco IoT Control Center: - Fog director: Gestión despliegue y monitor de máquinas virtuales en Edge - SDK para desarrollo de aplicaciones. - Machine Learning	HTTP MQTT	HTTP MQTT	HTTP MQTT	IoT Generalista: - Vehículos conectados. - Industria manufactura. - Smart City
Pixeom (Siemens) **https://www.pixeom.com**	Contenedores Docker.	Compatible con API en Google Cloud Platform, AWS y Azure. Fuerte dependencia Cloud. Edge: Servicios Edge equivalentes a AWS Core Pixeon Edge oT Publisher: - Servicios de almacenamiento central. - Servicios de aprendizaje automático.	HTTP ¿?	HTTP ¿?	HTTP ¿?	IoT Generalista: - Energía - Industria.
Zededa **https://www.zededa.com**	Contenedores Docker. Máquinas virtuales	Servicio SaaS sobre plataforma on-premise o cloud sobre cualquiera de los proveedores IaS. Edge: - Sistema Operativo EVE OS - Gestión kubernettes de contenedores y de máquinas virtuales. - Monitorización, control y seguridad Edge. Core basado EVE proyecto de la Linux Fundation. - Gestión despliegue funcionalidad. - Monitorización remota Nodos Edge.	HTTP MQTT	HTTP MQTT	HTTP MQTT	IoT Generalista:

4.5.5.13. Conclusiones

- **Nuevo paradigma de computación**

  El cambio a la informática perimetral (Edge-Computing) permite a los proveedores de servicios en la nube acceder a segmentos de clientes empresariales a los que no habían podido acceder fácilmente, ya sea porque había clientes potenciales que aún no estaban preparados para migrar a la nube pública o porque tenían requisitos específicos que no se pueden cumplir con la nube (por ejemplo, gobierno del dato).

- **Limitaciones del nuevo paradigma respecto al 'Cloud-Computing'**

  El problema principal del Edge-Computing no solo es la escalabilidad, sino también la distribución. Sobre el primer punto, el escalamiento horizontal hacia varios sitios pequeños puede resultar más complicado que agregar la capacidad equivalente a un centro de datos principal. También es importante contar con personal técnico especialista.

  Es necesario que las operaciones de gestión del sitio se puedan reproducir en todos los sitios de edge computing para simplificar la gestión, evitando el "desajuste en la configuración". En este nuevo paradigma, la seguridad física del sitio suele ser mucho menor. Esto puede dar como resultado un mayor riesgo de situaciones maliciosas o accidentales, por ejemplo, la desconexión de un cable por error.

- **Evolución del mercado** [24] [25]

  Microsoft, Amazon y Google dominan a día de hoy el mercado del Edge-Computing y las perspectivas de desarrollo e implantación de nuevas funcionalidades auguran un mercado al alza.

  Para finales de 2021, más del 50% de las grandes corporaciones desplegarán al menos un caso de uso bajo el paradigma de Edge-Computing permitiendo soporte IoT, contra menos del 5% registrado en 2019.

Para finales de 2023, más del 50% de las grandes corporaciones desplegarán al menos seis casos de uso bajo el paradigma de Edge-Computing desplegados para IoT, contra menos del 1% registrado en 2019.

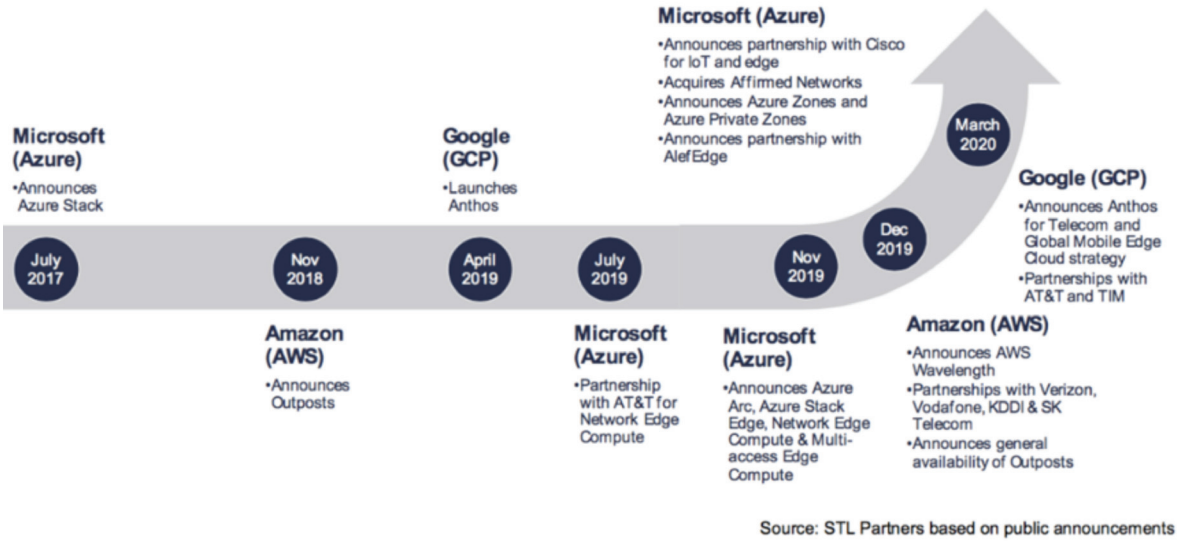


Figura 34: Evolución de mercado en plataformas.

[24] https://www.gartner.com/doc/reprints?id=1-1-OIB65YZ&ct=190917&st=sb

[25] https://stlpartners.com/edge-computing/aws-azure-google-at-the-edge-how-much-of-it-is-telco-edge-computing/

• **Comparativa de provedores Edge-Computing**[26]

La tecnología de encapsulamiento más presente en todas las plataformas son contenedores Docker, en menor medida algunas de las plataformas soportan también o únicamente máquinas virtuales o funciones lambda.

MQTT y HTTP son las tecnologías de interoperabilidad más extendidas, siendo soportadas por la mayoría de las plataformas.

Salvo el caso de la plataforma de Minsait el resto de plataformas tienen una aproximación IoT generalista sin adaptaciones específicas al mundo de gestión de la red eléctrica.

4.6. Telecomunicaciones

Se pueden diferenciar 4 niveles de comunicaciones en una arquitectura distribuida a nivel de SASCTI:

1. Comunicaciones SASCTI-Sistemas Centrales: SCADA, SPVBT, STG.
2. Comunicaciones SASCTI: tanto servicios generales, como elementos de protección y automatización de la red de BT o recursos distribuidos conectados a la misma.
3. Comunicaciones entre aplicaciones nodo Edge SASCTI: red de ethernet común para todos los dispositivos presentes en el SASCTI.
4. Comunicaciones con otros SASCTI.

4.6.1. Comunicaciones entre el SASCTI y Sistemas Centrales

Son las comunicaciones que se encargan de transportar todos los servicios del SASCTI hasta las plataformas de gestión de cada servicio. Se parte de que actualmente la mejor solución es utilizar un solo equipo de comunicaciones para todos los servicios del SASCTI, dado que en cuanto a ancho de banda y Qos es posible transportarlos todos a la velocidad y latencia adecuadas, y en caso de colisión establecer prioridades de forma que los servicios más críticos no sufran retardo alguno.

Los servicios a transportar entre el SASCTI y Sistemas son los siguientes ordenados de mayor a menor criticidad:

- Automatización de la MT
- Automatización de la BT
- Monitorización del cuadro de BT
- Telegestión de contadores inteligentes
- Gestión de los equipos
- Otros servicios generales

Este mismo orden se puede establecer en cuanto a requisitos de la comunicación, es decir los primeros elementos necesitan menor latencia y mayor disponibilidad que los últimos.

Existen diferentes tecnologías para implementar las comunicaciones entre el SASCTI y sistemas centrales:

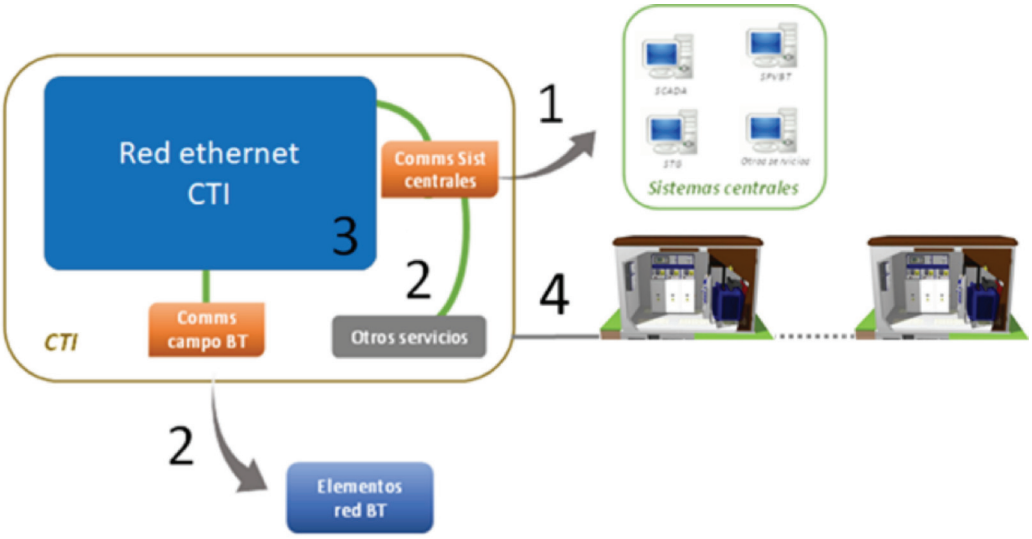


Figura 35: Niveles de comunicaciones en un SASCTI.

[26]https://www.g2.com/compare/azure-iot-edge-vs-google-cloud-iot-core-vs-ibm-watson-iot-platform-vs-aws-iot-core

4.6.1.1.Redes celulares 4G/5G

Las tecnologías celulares han sido las más utilizadas hasta la fecha para comunicar los CTs, por la facilidad de despliegue, amplia cobertura y coste económico reducido. La posibilidad de priorizar el tráfico de las utilities en la red del operador supone una mejora importante.

4.6.1.2. Redes LTE con infraestructura propia de la compañía eléctrica

Muchas compañías eléctricas disponen de infraestructura radio (emplazamientos para repetidores) que se están utilizando actualmente para redes propias de radios digitales. Las redes LTE propias son el heredero natural de dichas radios digitales, mejorando grandemente su ancho de banda y capacidad de transporte.

4.6.1.3. BPL sobre MT

Tecnología dotada de un buen ancho de banda, latencia y seguridad al tratarse de una red propia, si bien necesita de una planificación y de la utilización de diferentes tipos de acopladores para cada tipo de infraestructura (aérea/subterránea) además de los propios equipos de comunicaciones.

4.6.1.4. Fibra óptica - ethernet

En caso de disponer de fibra óptica, es sin duda la mejor opción por las características de ancho de banda, latencia y seguridad de una red propia. Además, la tecnología ethernet sobre fibra es una tecnología madura y capaz de proporcionar redundancias. Si fuera necesario por el tamaño y complejidad de la red, existen tecnologías Ethernet que pueden aportar características más avanzadas como SLAs.

4.6.1.5. FTTH

Tecnología utilizada masivamente para dotar de acceso de internet a abonados domésticos, por lo que comparte algunas características con las redes celulares públicas como la dependencia de un operador externo y la no priorización de tráfico crítico, si bien el cable de fibra óptica es más seguro frente a interferencias y con mayor ancho de banda que el medio radio.

4.6.1.6. Otras tecnologías

Radio mesh. Buen ancho de banda y capacidad de enrutamiento. Necesidad de grandes cantidades de dispositivos para resultar eficiente económicamente y enrutable. No parece la más adecuada para comunicar centros de transformación

Wimax. Tecnología con buen ancho de banda, pero con poco desarrollo y desplegada en pocas áreas por lo que no representa una buena opción.

NBIoT. La tecnología NBIoT no parece la más adecuada como canal de comunicación único de centros de transformación hacia arriba, dado que no dispone del ancho de banda necesario para transportar todos los servicios del centro con la latencia adecuada y dando prioridad a los servicios más exigentes o críticos sobre los demás. Tampoco existe en el centro de transformación una escasez de energía que obligue al uso de baterías y a limitar al máximo el ancho de banda y tiempos de conexión

4.6.2. Comunicaciones del SASCTI

Se parte de la idea de que el elemento central de control del SASCTI será el Nodo Edge Computing (NEC), donde se ejecutarán diversas aplicaciones que tendrán conexión directa con los equipos conectados al SASCTI. Estos equipos podrán ser los alojados en el propio SASCTI, pero también los distribuidos por la red de BT, incluyendo no sólo a elementos de protección y automatización, sino también a los inversores de paneles fotovoltaicos, baterías o vehículos eléctricos, de manera que se facilite una gestión eficiente y coordinada de la red de BT, donde la regulación lo permita.

Los principales servicios transportados en la red del SASCTI, y gestionadas mediante aplicaciones ejecutadas en el NEC serán:

- Protección y automatización de líneas.
- Protección y automatización de la acometida.
- Supervisión de acometida y línea.
- Regulación de tomas de transformador de distribución.
- Medidor de calidad de onda.
- Elementos de protección y automatización desplegados en la MT del SASCTI.
- Elementos de protección y automatización desplegados a lo largo de la red de distribución de BT
- Recursos distribuidos, tales como inversores, baterías y los sistemas de carga/descarga de los vehículos eléctricos.

El NEC tendrá una función de Gateway para comunicar con cada elemento, e implementará diferentes protocolos utilizados por cada servicio y las plataformas de gestión correspondientes:

- DLMS-TCP para comunicar con:
  - Supervisor de acometida
  - Supervisión avanzada de línea
  - Interruptores de línea
  - Interruptor de acometida
  - Regulador de transformador
  - Contadores Inteligentes
- Web Services para comunicar con sistemas centrales (STG_DC, ...)
- IEC60870-5-104 para comunicar con SCADA

Dentro de la red del SASCTI dependiendo de los requerimientos de aislamiento, se podrían diferenciar o no dos segmentos de red: el segmento al que están conectados los dispositivos del lado de MT y el segmento BT al que están conectados los elementos de automatización de BT desplegados aguas abajo del transformador y a los diferentes recursos distribuidos. Cuando la comunicación sea interna se puede usar un cable Ethernet, o lo que convenga en cada caso. El soporte físico de la subred ethernet podría ser un Switch Ethernet de rango industrial de Nivel 2.

Desde el SASCTI también será necesario comunicar con equipos desplegados en la red de BT. Hasta el momento, en España, los contadores inteligentes comunicados mediante PLC de BT con dos variantes: PRIME, y METERS&MORE. Las tecnologías de comunicaciones más adecuadas para la comunicación de los elementos de automatización en campo pueden ser inalámbricas tipo NB-IoT o Lora, o también tipo PLC, por ejemplo BPL (Broadband over PowerLines) de BT, que permite un ancho de banda de 20Mbps y alcance máximo de 1 Km. Esta última no interfiere en el espectro del PLC de BT y puede complementarlo en el tramo desde el SASCTI hasta la Caja General de Protección (CGP). Para aplicaciones de automatización presenta una disponibilidad mucho mayor que las comunicaciones PLC de BT para contadores, porque esta menos afectado en su banda por ruidos.

Si se virtualiza la función del DCU de elaboración de informes de contadores inteligentes para el sistema central en el propio NEC, más adelante se podría incluso plantear utilizar un único canal PLC por BPL que sustituyera la comunicación PRIME/METERS&MORE en el SASCTI. Así la aplicación ejecutada en el NEC se abstraería del medio físico usando DLMS-TCP para comunicarse con los contadores.

Este esquema de funcionamiento da una gran flexibilidad ya que posibilita virtualizar nuevas funcionalidades en el NEC, permitiendo integrar cualquier funcionalidad y equipo nuevos, incluso los 'legacy' existentes.

En el caso de los recursos distribuidos, se plantea que su gestión sea realizada mediante un Router IoT que facilite la coordinación eficiente de los distintos recursos conectados a la red de BT con el SASCTI: inversores de paneles fotovoltaicos o mini aerogeneradores, baterías y carga/descarga del vehículo eléctrico. La inmensa mayoría de equipos comerciales de esta clase disponen de comunicaciones cableadas estándar, como son Modbus (en sus versiones RTU y TCP) o protocolos propietarios. Debido a las considerables distancias entre el SASCTI y los recursos distribuidos, la comunicación directa entre el Router IoT del SASCTI y dichos recursos no será posible en muchos casos. Por ello se propone una arquitectura de comunicaciones en varios niveles a través de varios Routers IoT. Se dispondría de un "master" a nivel de SASCTI, que se comunicaría con el NEC, y de diferentes "slaves" que controlarían los recursos distribuidos.

Este esquema de comunicaciones facilitaría la coordinación de la operación del smart transformer con los distintos recursos distribuidos para gestionar de manera eficiente y coordinada las potenciales congestiones locales en la red de BT generadas por el despliegue de esos mismos recursos distribuidos. Si se dota de suficiente inteligencia y capacidad de cálculo a dicho Router IoT, permitiría una gestión más autónoma de los recursos distribuidos, siguiendo las consignas de alto nivel del NEC.

4.6.2.1. Arquitecturas de red alternativas en el SASCTI

La tecnología ethernet IP es la seleccionada con seguridad por todas las compañías eléctricas para implementar las comunicaciones internas en el futuro SASCTI, tanto para equipos principales (remotas o nodos), como para equipos secundarios (sensórica).

Partimos de la red de un CT equipado con todas las funcionalidades disponibles actualmente como telegestión de contadores inteligentes, automatización de MT, supervisión avanzada de BT y comunicaciones.

A partir de esta situación existen varias posibilidades de evolución mediante retrofiting o sustitución de equipamiento con el objetivo final de disponer de un equipo único central del CT llamado Nodo de Edge computing (NEC).

En esta evolución se ha de tener en cuenta factores como la disponibilidad de comunicaciones con suficiente ancho de banda y reducida latencia, aislamiento entre dispositivos de MT y BT, amortización de los equipos ya desplegados, etc. Por todo esto cada distribuidora eléctrica podrá trazar diferentes caminos intermedios o fases hasta llegar al Nodo único de Edge computing.

Una opción intermedia, mostrada en la siguiente figura, es la que se divide la red local del CT en dos subredes ethernet de MT y BT con objeto de aislar las dos redes mediante fibra óptica, añadiendo futuras funcionalidades como comunicaciones IoT y BPL y cuadro de BT automatizado. Como se puede comprobar el número de equipos electrónicos en el CT es muy elevado.

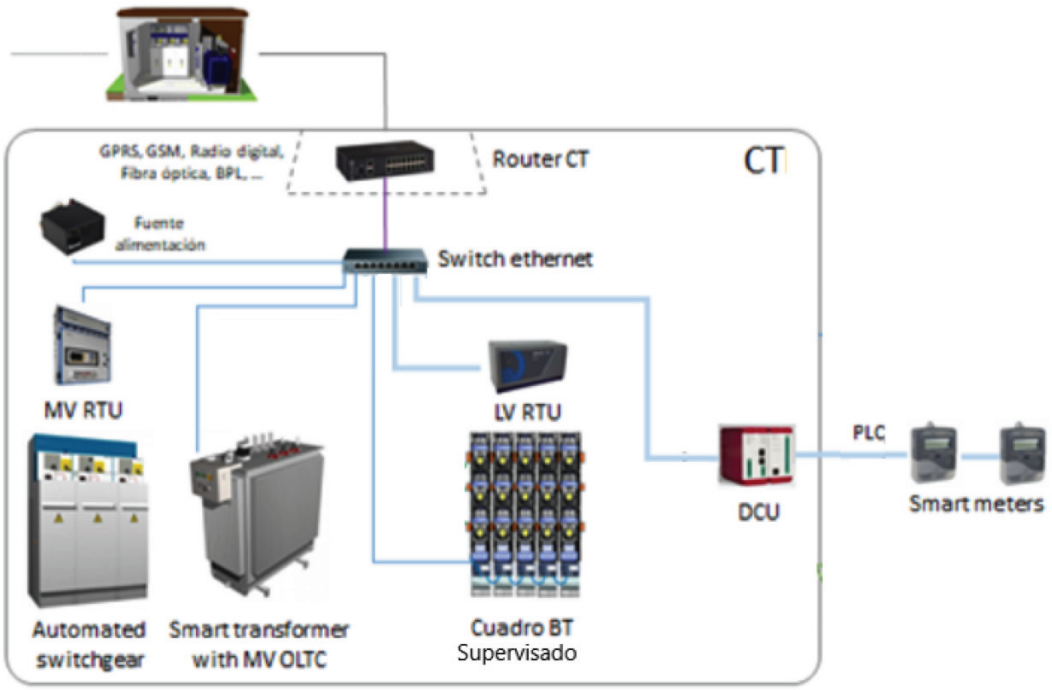


Figura 36: Esquema red ethernet dentro del SASCTI.

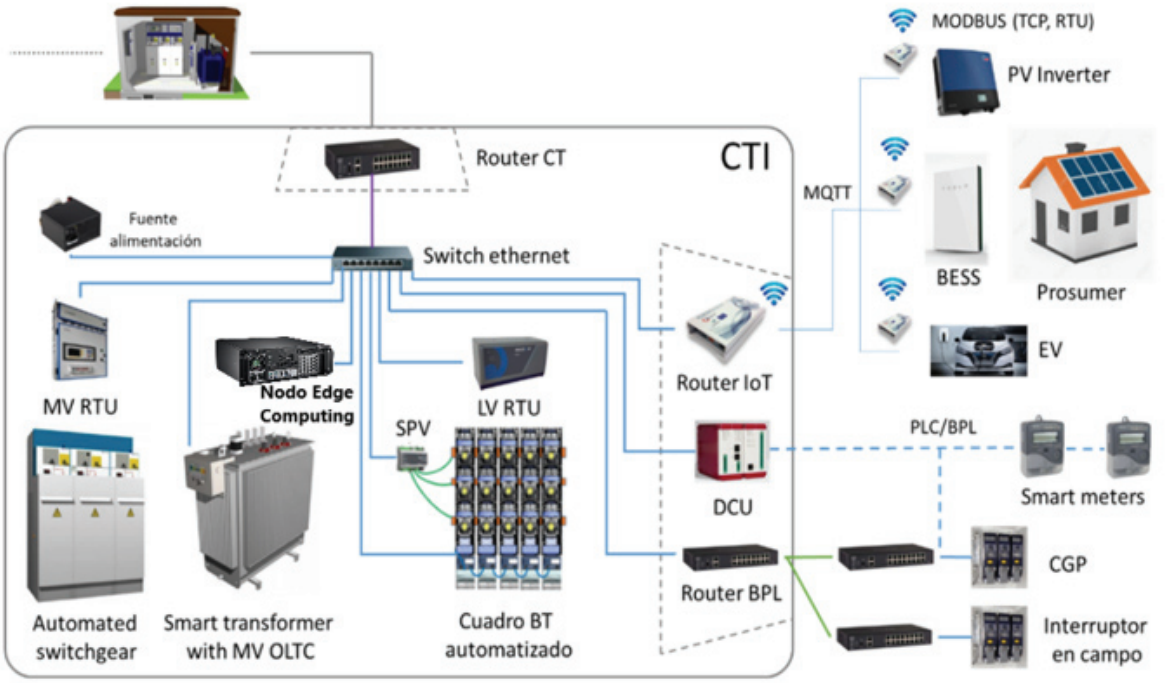


Figura 37: Flujo de comunicaciones de control actual dentro de un CT.

El Nodo Edge con objeto de hacer retrofitting de los CTs convencionales, integraría o podría estar integrado en uno de los dispositivos que forman parte del SASCTI. En este proceso el NEC podría ir incorporando la funcionalidad de aquellos equipos que vayan llegando al final de su vida útil, como remota de MT, SABT o DCU (Concentrador de Datos).

Finalmente, se alcanzaría una red unificada en un único Nodo Edge computing SASC-TI (NEC). Se puede observar la reducción de equipamiento dado que el NEC ha asumido las funciones de la remota SABT, el DCU y la remota de BT. Los únicos equipos adicionales al NEC serian la sensórica de MT y de BT.

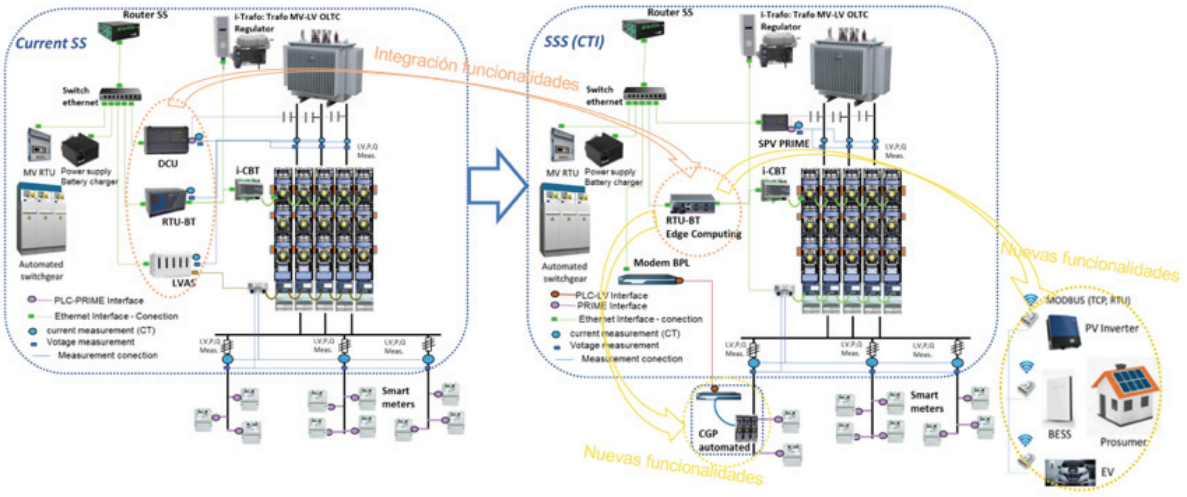


Figura 38: esquema unificación equipos

Para una arquitectura con subredes de MT y BT aisladas localmente se separarían en dos switches conectados al router mediante fibra, el esquema sería la siguiente:

cerrar un anillo Ethernet con todos los dispositivos en modo serie contra el Switch cabecera. Si bien esta arquitectura reduce el tendido de cable, aumenta la complejidad de los dispositivos por la necesidad de gestión de los anillos,

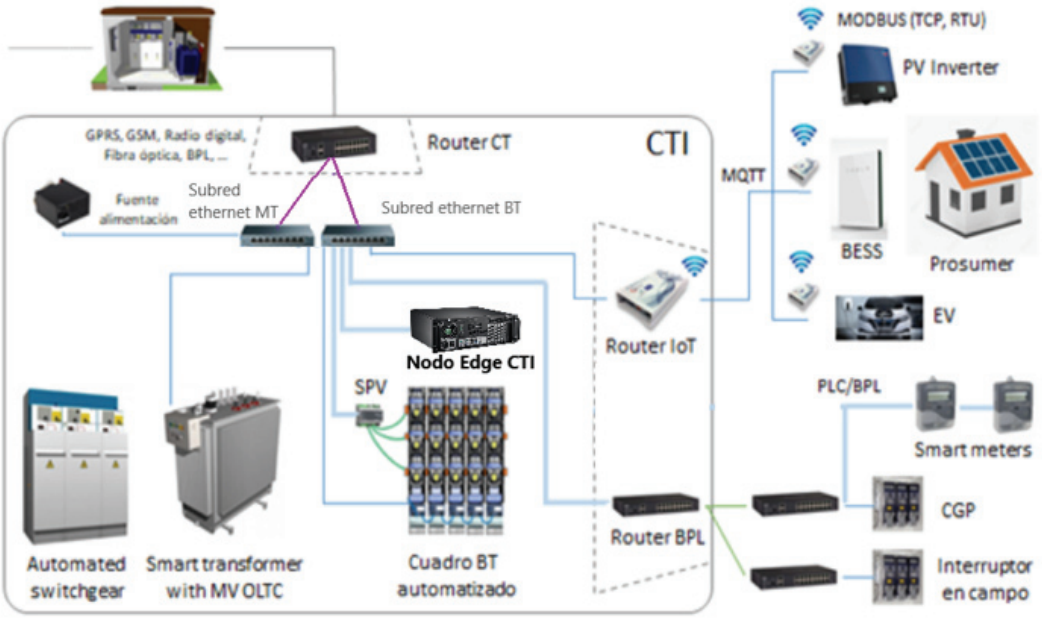


Figura 39: Aislamiento equipos con referencia MT y BT.

Para minimizar la centralización de cableado y necesidad de switches con número excesivo de puertos Ethernet, también se puede plantear una arquitectura de tipo Daisy Chain, donde cada dispositivo (sensórica) disponga de dos puertos Ethernet, de manera que permita

para evitar que un mal funcionamiento de uno de los equipos o un tramo de cable afecte al resto de equipos que cuelgan de él, además de la complejidad de incorporación de protocolos de gestión de anillos que requiere switches con funcionalidades avanzadas y por lo tanto con mayor coste.

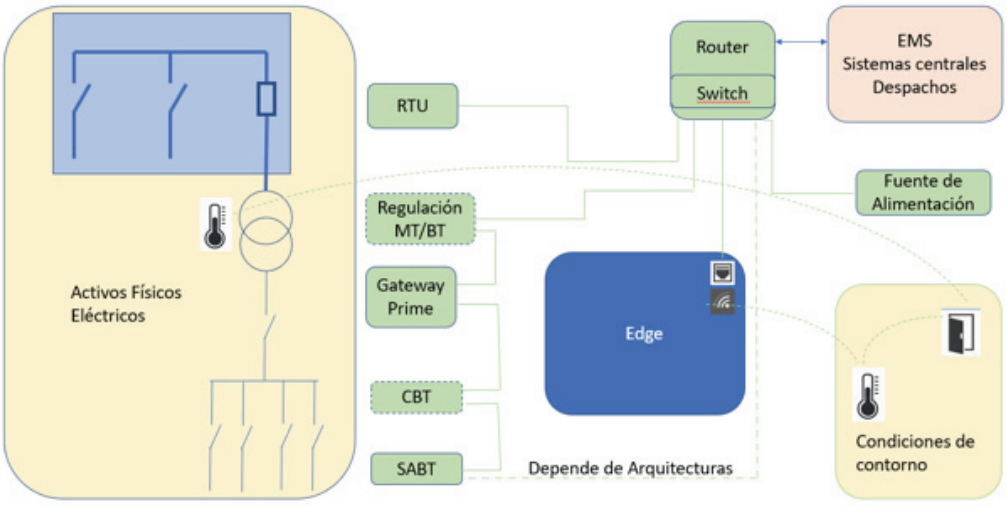


Figura 40: Esquema arquitectura tipo daisy chain.

Siguiendo este mismo criterio sería posible crear una red de swiches (más pequeños) que conecten diferentes tipos de sensórica, por ejemplo, incluir un switch normalizado y precableado por cada CBT con las tarjetas de SABT e iCBT conectadas en anillos daisy chain, y tener todos los switches interconectados por fibra, con posibilidad también de cerrar anillos.

4.6.3. Comunicaciones entre CTIs del mismo anillo de MT

En el ámbito de la MT, el despliegue de comunicaciones entre CTIs permitirá una mayor efectividad en la detección de fallos, localización y aislamiento de fallos, la aparición de herramientas de diagnóstico on-line en cables, la gestión de fenómenos asociados a la generación distribuida como el funcionamiento en isla y la necesaria coordinación entre los smart transformers presentes en el mismo anillo de MT.

Para poder comunicar un gran número de centros de transformación entre sí, y teniendo en cuenta todos los requerimientos técnicos, se recomienda el uso de comunicaciones MV-BPL, fibra óptica, 4G/5G, o en última instancia comunicaciones vía satélite, de manera individual o combinada, en función de la necesidades.

4.7. Ciberseguridad

Debido a la evolución de los sistemas presentes en la Smart Grid hacia tecnologías utilizadas dentro de las TICs su capacidad y rango de oportunidades se ha incrementado considerablemente, así como lo han hecho también su exposición a posibles ciberataques. Al tratarse de infraestructuras críticas, el impacto que puede tener una interrupción del servicio, la rotura o un mal funcionamiento de los dispositivos que la componen es muy elevado.

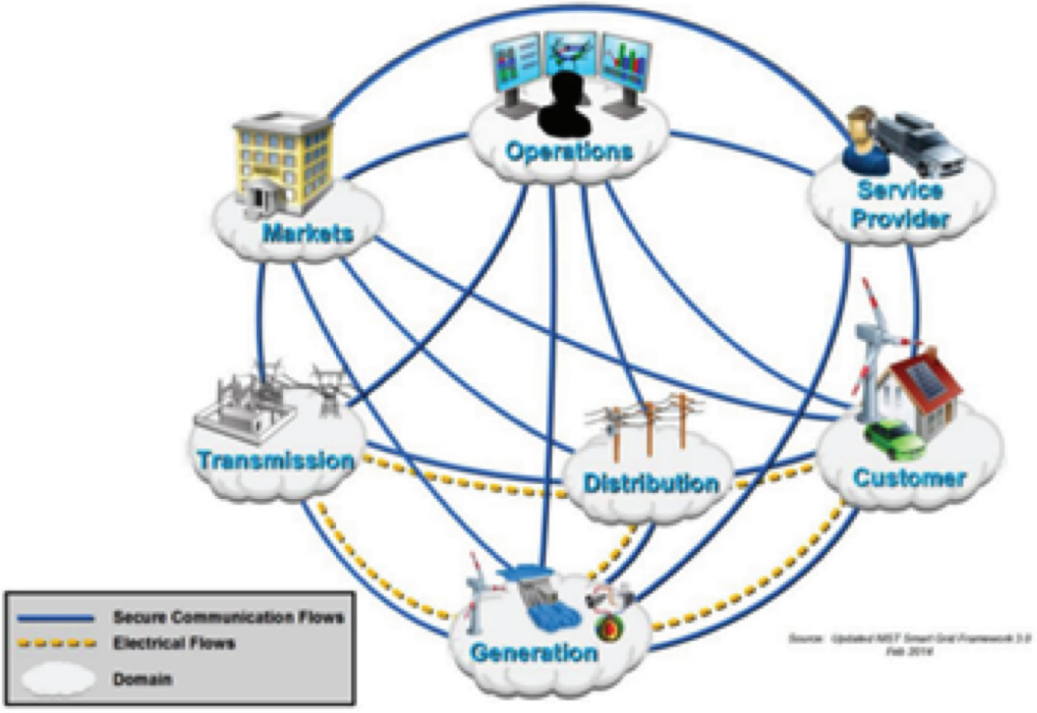


Figura 41: Múltiples partes presentes en Smart Grid. (Fuente NIST.IR.7628).

Por este motivo es necesario aplicar medidas de protección que permitan operar a la red en todos sus niveles de un modo seguro. Es importante subrayar la necesidad de proteger todos y cada uno de los elementos y niveles presentes en el sistema realizando una defensa en profundidad por dos motivos fundamentales:

- La complejidad del sistema y variedad de equipos y comunicaciones existentes en entornos Smart Grid.
- No existe una única medida de ciberseguridad que puede proteger frente a todas las amenazas.

- Aplicar medidas de seguridad y bastionado a los equipos presentes.
- Establecer relaciones de confianza entre las diferentes entidades participantes a través de roles y responsabilidades.
- Desplegar una infraestructura de gestión criptográfica.

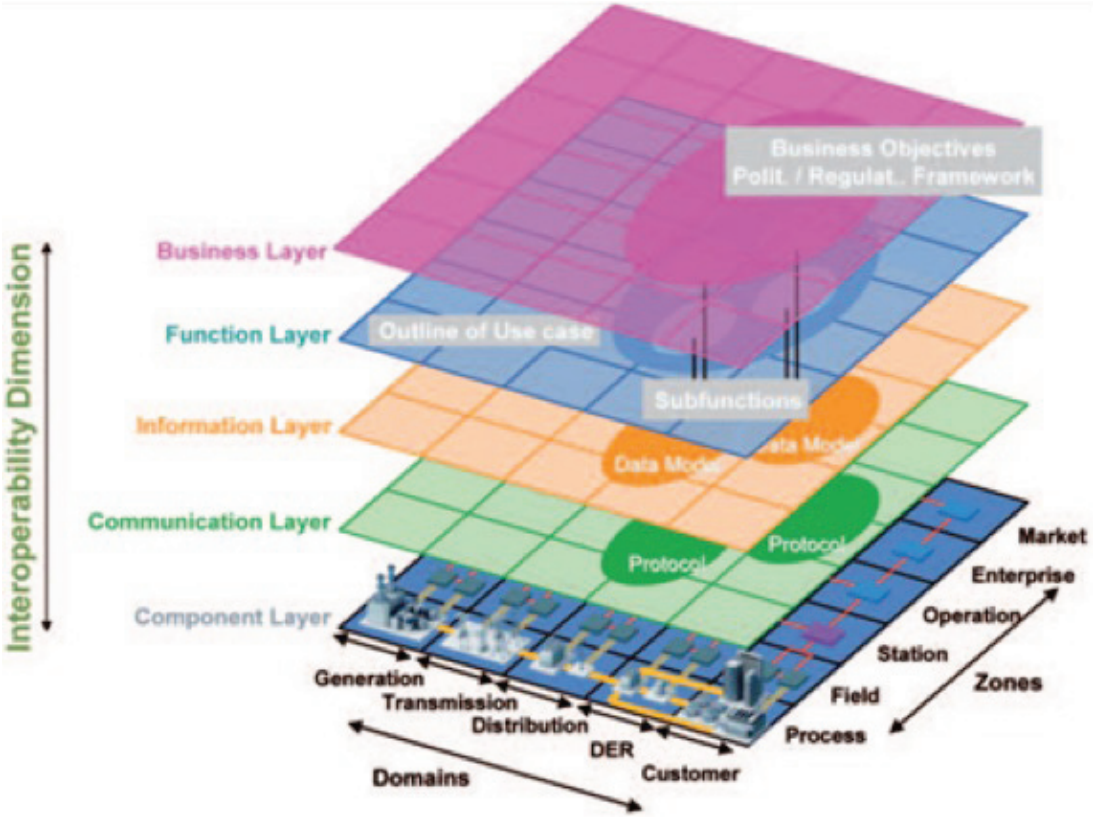


Figura 42: Modelo SGAM (CEN/CENELEC/ETSI).

Este hecho se acentúa en entornos distribuidos como el que se está planteando y que puede venir reflejado en el modelo de arquitectura SGAM (Smart Grids Architecture Model) desarrollado por el CEN/CENELEC/ETSI.

Una estrategia de defensa en profundidad no tiene que abordar solo los temas técnicos, sino que tiene que integrar a los procesos y a las personas, teniendo en cuenta los siguientes puntos[27]:

- Aplicar técnicas de defensa en diferentes lugares del sistema.
- Crear capas de protección: al no existir elementos 100% seguros.

- Instalar diferentes sistemas de detección y prevención de intrusiones y ataques.
- Disponer de una plantilla formada en ciberseguridad: desarrollo competencias.
- Considerar todo tipo de amenazas: como son, entre muchas otras, las de denegación de servicio, vulnerabilidades presentes, control no autorizado de equipamiento, robo o destrucción de datos, alteración de datos y/o software crítico.
- Tener en cuenta todos los posibles vectores de ataque: malware, APTs, ingeniería social...

[27]http://dx.doi.org/10.6028/NIST.IR.7628r1

- Ser conscientes de la gravedad de las APTs (Advanced Persistent Threads): por su dificultad de detección, tiempo de operación, y su capacidad para coordinar y maximizar el impacto. La sofisticación de los ataques llevados a cabo en entornos de Smart Grids hace necesaria la comprensión completa de las cadenas de ataques existentes (Cyber Kill Chain).

campo de la ciberseguridad provenientes del mundo de las TICs no pueden aplicarse directamente. Esto ha llevado a la evolución de los estándares existentes a nivel de ciberseguridad industrial para adaptarlos a los requisitos de las redes eléctricas.

Actualmente existe un extenso abanico de normas aplicables a la Smart Grid. Su representación según el enfoque adoptado se muestra en la siguiente figura.

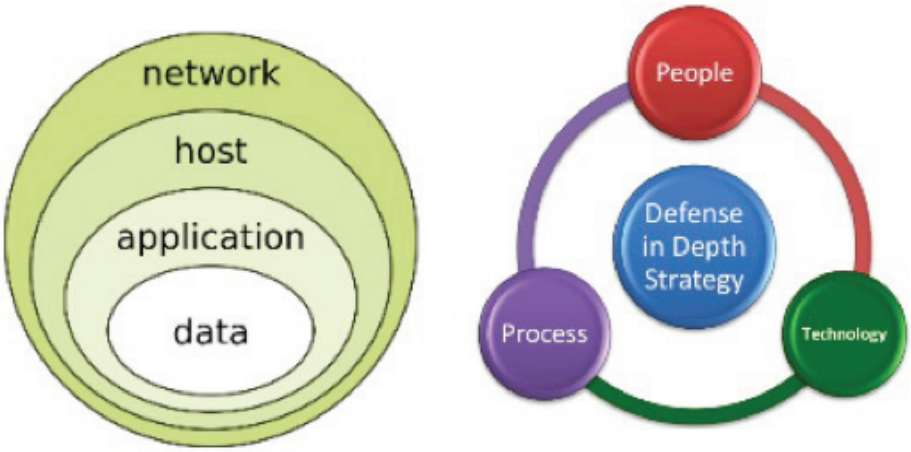


Figura 43: Defensa en profundidad (Adaptado de NIST.IR.7628r1).

4.7.1. Normativas Ciberseguridad

Debido a las particularidades de este tipo de sistemas, las estrategias y normativas en el

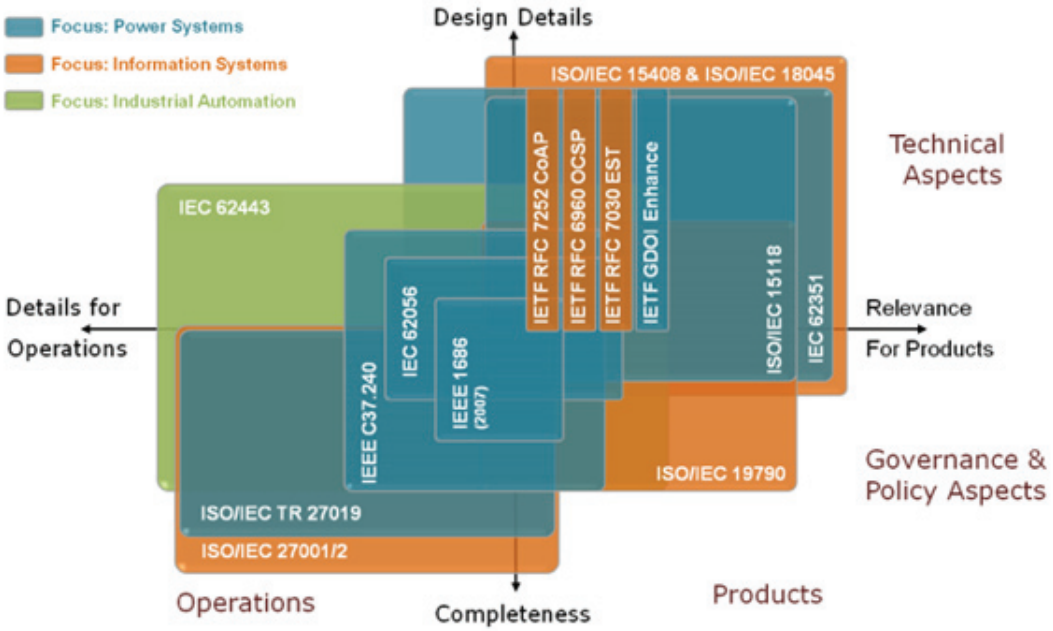


Figura 44: Fuente: CEN-CENELEC-ETSI Smart Grid Coordination Group (2014).

Entre las más destacables por su orientación a Smart Grid o presencia internacional se encuentran las siguientes:

- IEC 62351
- IEEE 1686
- IEC 62443
- IEC 27019 - ISO/IEC 27001
- NISTIR 7628 Guidelines for Smart Grid Cyber Security
- NERC CIP: Critical Infrastructure Protection
- Common Criteria (ISO/IEC 15408)
- CEN/CENELEC/ETSI: Smart Grid Information Security

como ocurre en el caso de la IEC62351 e IEEE1686 o el apartado 4 de la IEC62443.

Esta última sin embargo también cubre aspectos relacionados con la unión del mundo OT a IT estableciendo prácticas de ciberseguridad que podrían extrapolarse al Cloud.

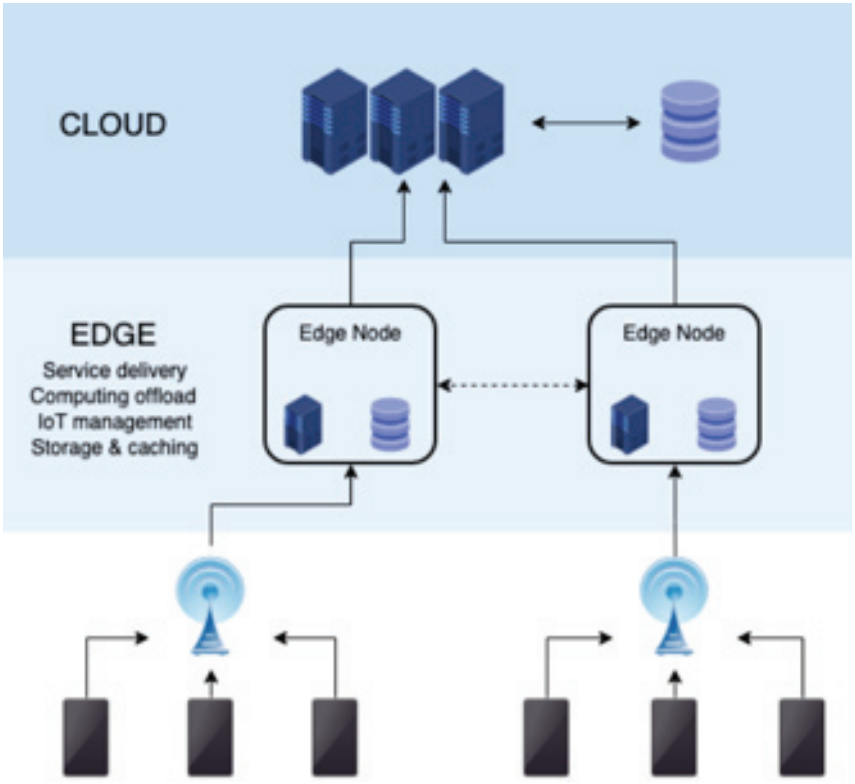


Figura 45: Dispositivos - Edge - Cloud.

Todas ellas presentan puntos comunes, siendo algunas más generales y otras estando más enfocadas en los dispositivos, en las operaciones, en el diseño o en los procesos.

Muchas de las normas mencionadas cubren la mayor parte de los aspectos que se pueden encontrar desde el dispositivo hasta el Edge

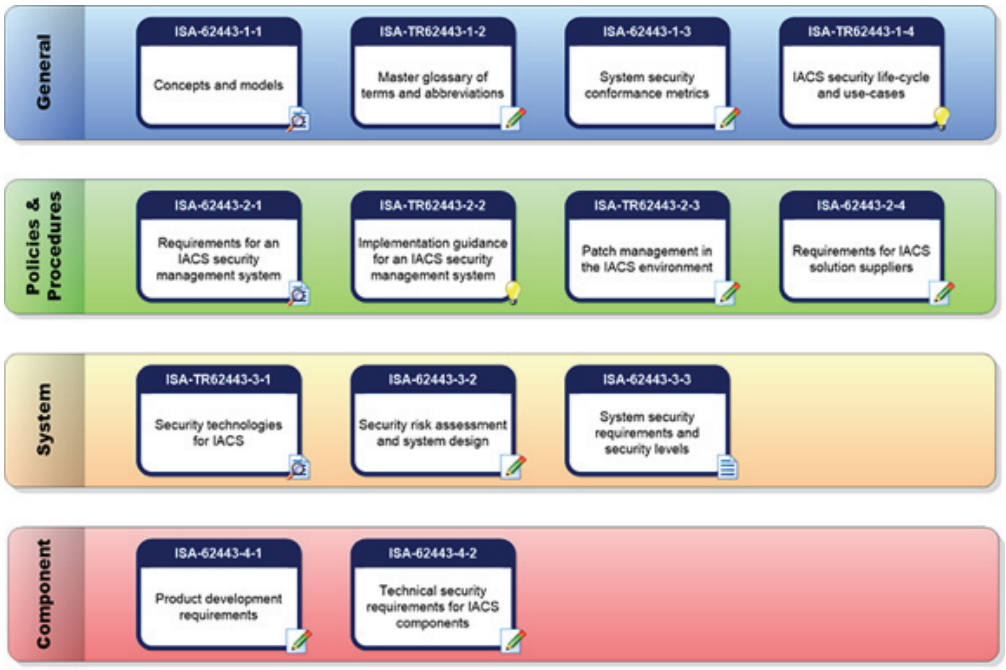


Figura 46: IEC62443.

Concretamente el apartado 3 de sistema de la norma, podría incluir el despliegue y la conexión de los elementos cloud, para posteriormente chequear su cumplimiento contra IEC62443-3-3.

4.7.2. Ciberseguridad en entornos distribuidos Edge-Cloud

Dependiendo del tipo de servicio utilizado o contratado (PaaS, IaaS o SaaS), la responsabilidad de la ciberseguridad de cada uno de los elementos es diferente.

Cada una de las partes debe de estar correctamente protegida por cada parte implicada. Aun así, incluso en soluciones SaaS no es suficiente el disponer de un proveedor de servicios seguro, sino que la política de accesos y los roles por parte de los usuarios necesitan estar cubiertos por políticas y procedimientos seguros.

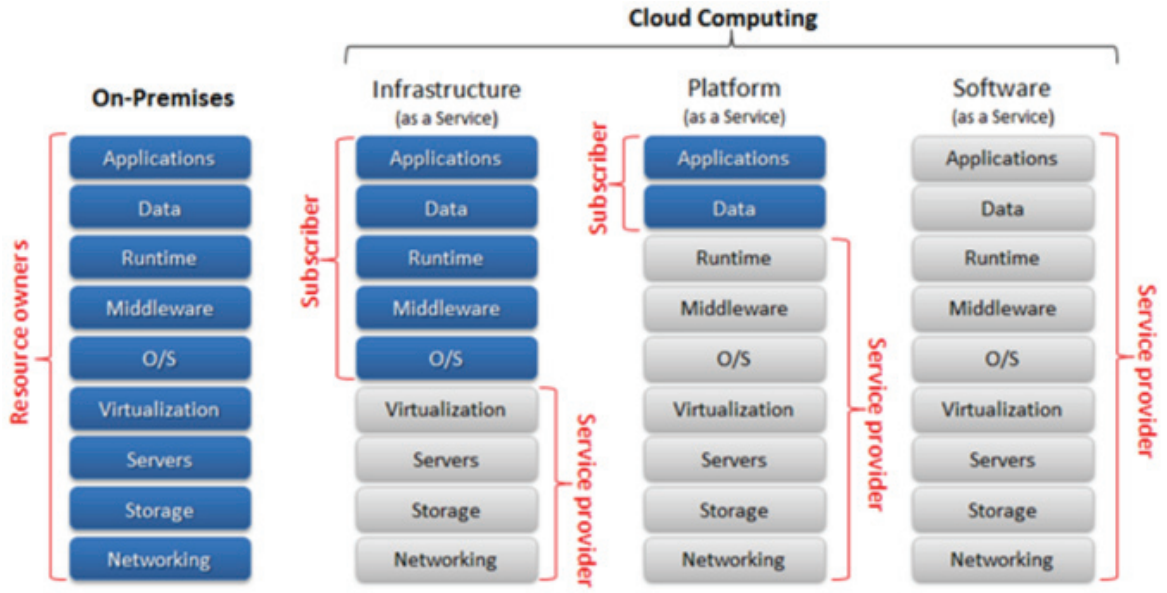


Figura 47: Separación de responsabilidades (fuente: Cigre TB 796).

Cuatro de los principales vectores de ataque en infraestructuras cloud identificadas dentro del marco de la Smart Grid son las siguientes:

- Amenazas internas: por parte de atacantes que conocen bien el sistema.
- Credenciales comprometidas.
- Fallos en la configuración.
- APIs de interfaz no seguras.

En este tipo de entornos distribuidos la importancia de la monitorización de todos los elementos que lo componen es clave. Elementos como los denominados 'Cloud Access Security Brokers' (CASB) pueden ayudar a reforzar las políticas de ciberseguridad.

4.8. Normativa y estándares de referencia aplicables.

En el informe publicado por CEN-CENELEC-ETSI Coordination Group on Smart Energy Grids (CG-SEG) en enero de 2017[28], se identifican las normas de referencia de la tabla siguiente en el apartado dedicado a sistemas avanzados de gestión de la distribución:

Capa	Estandard	Ámbito
	IEC 61869	Transformadores de medida y sensores
	IEC 62271 series	Aparamenta de AT
Comunicaciones	IEC 61968-100	Application integration at electric utilities - System interfaces for distribution management - Part 100: Implementation profiles
Comunicaciones	IEC 62351 (all parts)	Cyber-security aspects (refer to section 9.4)
Comunicaciones e Información	EN 61970 (all parts)	Some issues will be relevant of this family of standards but focus in this family of standards is on transmission
Comunicaciones e Información	IEC/EN 61850 (all parts)	See substation automation
Comunicaciones	IEC 60870-5-101	Telecontrol
Comunicaciones	IEC 60870-5-102	Medida
Comunicaciones	IEC 60870-5-103	Protección y control
Comunicaciones	IEC 60870-5-104	Telecontrol
Comunicaciones	IEC 61158 series	Buses de campo
Comunicaciones	IEC 61400-25	Parques eólicos
Comunicaciones	IEC 61588 (IEEE 1588)	Sincronización horaria (PTP)
Comunicaciones	IEC 62056-5-3	DLMS/COSEM
Comunicaciones	IEC 62351 series	Ciberseguridad
Comunicaciones	IEC 62361 series	Modelos de datos (CIM)
Comunicaciones	IEC 62488-1 (Formerly EN60663) - Part 1	PLC
Comunicaciones	IEEE 1901	PLC de banda ancha
Comunicaciones	ISO/IEC 12139-1	Capa MAC
Comunicaciones	ISO/IEC 14908	Control de red
Comunicaciones	ISO/IEC 15118	V2G

[28]SEGCG/M490/G_Smart Grid Set of Standards Version 4.1, 06/01/2017

Comunicaciones	ISO/IEC 15802 IEEE 802.1	Intercambio de datos entre sistemas
Comunicaciones	ISO/IEC 7498-1	Modelo de referencia OSI
Comunicaciones	ISO/IEC 8802-3	Intercambio de datos entre sistemas
Comunicaciones	ITU-T G.7042	Esquema de ajuste de la capacidad del enlace para señales concatenadas virtuales
Comunicaciones	ITU-T G.707	Interfaz de nodo de red para la jerarquía digital síncrona
Comunicaciones	ITU-T G.709	Interfaces para la red óptica de transporte
Comunicaciones	ITU-T G.783	Características de los bloques funcionales del equipo de la jerarquía digital síncrona
Comunicaciones	ITU-T G.798	Características de los bloques funcionales del equipo de la jerarquía de la red óptica de transporte
Comunicaciones	ITU-T G.803	Arquitectura de redes de transporte basadas en la jerarquía digital síncrona
Comunicaciones	ITU-T G.872	Arquitectura de las redes ópticas de transporte
Comunicaciones	ITU-T G.983.1	Sistemas de acceso óptico de banda ancha basados en redes ópticas pasivas
Comunicaciones	ITU-T G.983.2	interfaz de control y gestión de terminales de red óptica para redes ópticas pasivas de banda ancha
EMC	IEC 61000 Series	EMC, Environmental, Mechanical
EMC	IEC 61326	Material eléctrico para medida, control y uso en laboratorio
General	EN 61968-1	Application integration at electric utilities - System interfaces for distribution management - Part 1: Interface architecture and general requirements
General	IEC 62357	Reference architecture power system information exchange
General	ISO/IEC 27001	Seguridad de la información
General	ISO/IEC 27002	Seguridad de la información
Information	EN 61968-11	Application integration at electric utilities - System interfaces for distribution management - Part 11: Common information model (CIM) extensions for distribution

Information	EN 61968-13	Application integration at electric utilities - System interfaces for distribution management - Part 13: CIM RDF Model exchange format for distribution
Information	EN 61968-2	Application integration at electric utilities - System interfaces for distribution management - Part 2: Glossary
Information	EN 61968-3	Application integration at electric utilities - System interfaces for distribution management - Part 3: Interface for network operations
Information	EN 61968-4	Application integration at electric utilities - System interfaces for distribution management - Part 4: Interfaces for records and asset management
Information	EN 61968-6	Application integration at electric utilities - System interfaces for distribution management - Part 6: Interfaces for maintenance and construction
Information	EN 61968-8	Application integration at electric utilities - System interfaces for distribution management - Part 8: Interface Standard For Customer Support
Information	EN 61968-9	Application integration at electric utilities - System interfaces for distribution management - Part 9: Interfaces for meter reading and control
Information	IEC 62361-100	CIM profiles to XML schema mapping
Protección	IEC 60255-24	Relés de protección, control y medida

4.8.1. IEC TC57: "Power system management and associated information exchange"

Los trabajos del Comité Técnico 57 del IEC tendrán que ser muy tenidos en cuenta para realizar la especificación técnica del sistema SASCTI.

Una de las principales funciones del IEC TC57 es la incorporación de nuevos estándares provenientes de mundo de las Tecnologías de la Información y Comunicaciones (pe IoT). Esto es precisamente lo que se busca en la especificación del SASCTI.

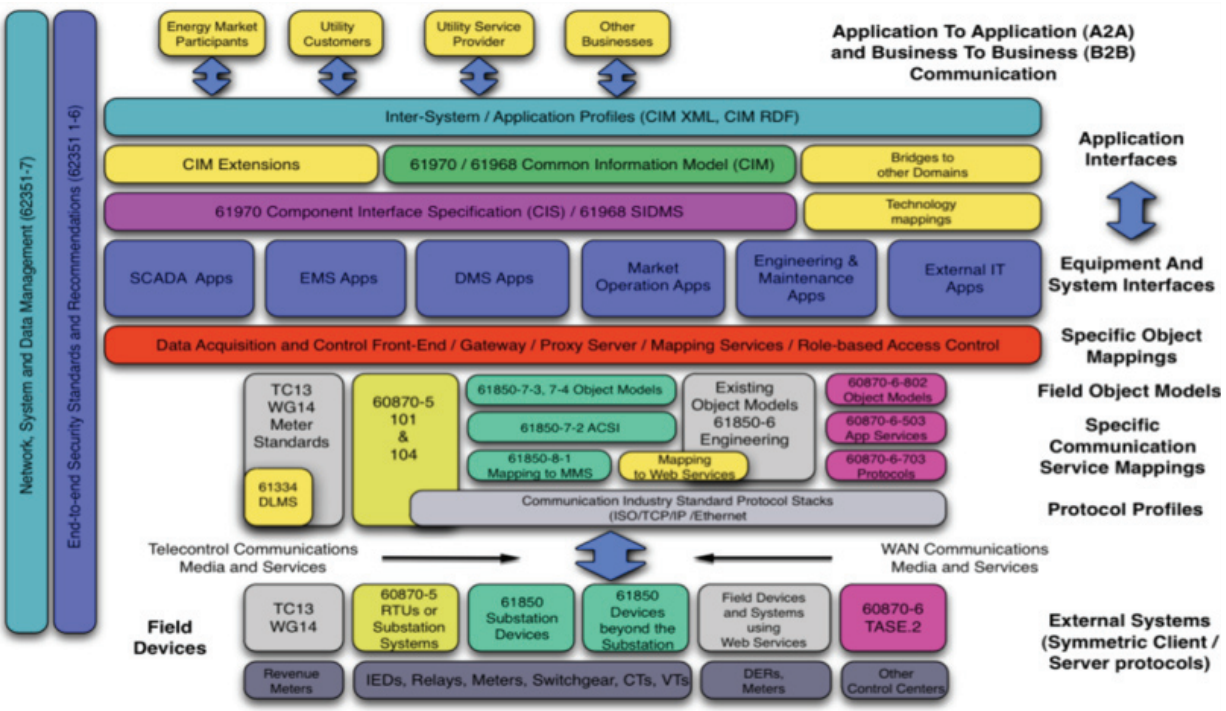


Figura 48: Arquitectura de referencia (IEC TC57).

Los objetivos de este comité técnico son: "proporcionar estándares de interoperabilidad para el intercambio de información dentro y hacia los sistemas de energía. Esto incluye interfaces de comunicación, seguridad de la información y especificaciones del modelo de datos que cubren la automatización de las redes eléctricas, gestión de DER, SCADA, sistemas de gestión de energía (EMS), sistemas de gestión de distribución (DMS), comunicación con mercados, así como intercambio de información entre el sistema de energía y la automatización del hogar, la construcción y la industria".

Con respecto a los modelos de datos establece el CIM (IEC 61968, IEC 61970 y IEC 62325) y el IEC 61850 como las referencias, además los ubica en el plano Smart grid como se puede observar en la figura.

El IEC TC57 está constituido por los siguientes grupos de trabajo:

- WG03 Telecontrol protocols.
- WG09 Distribution automation using distribution line carrier systems.
- WG10 Power system IED communication and associated data models.
- WG13 Energy management system application program interface.
- WG14 System interfaces for distribution management.
- WG15 Data and communication security.
- WG16 Deregulated energy market communications.
- WG17 Communication systems for distributed energy resources (DER).
- WG18 Hydroelectric power plants – Communication for monitoring and control.
- WG19 Interoperability within TC57 on long term.

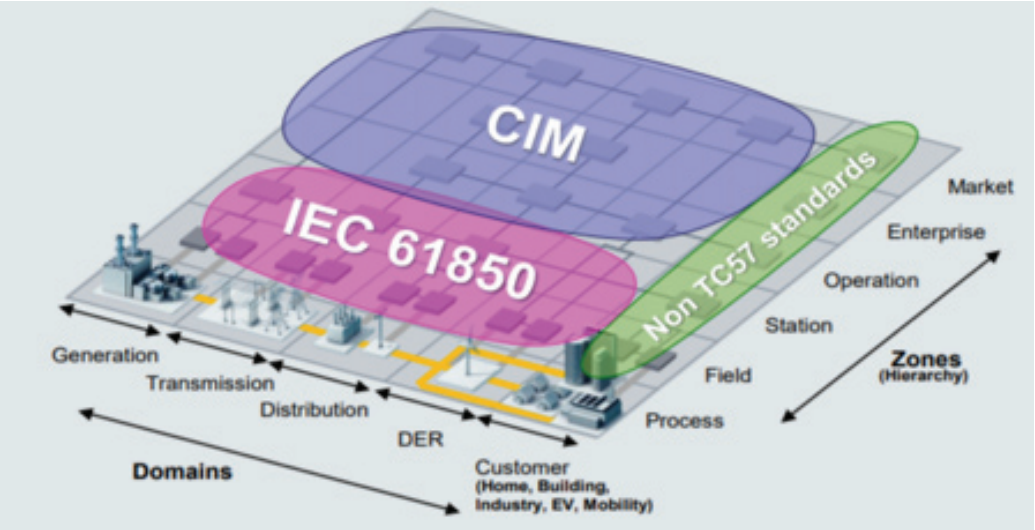


Figura 49: IEC 61850 y CIM en el plano Smart Grid (IEC TC57).

- WG20 Planning of (single-sideband) power-line carrier systems.
- WG21 Interfaces & protocol profiles relevant to systems connected to the electrical grid.
- AHG8 Relevance of IPv6 technology across TC57.
- Chairman Advisory Group.

4.8.2. CIM

El IEC TC57 da soporte a la especificación de CIM (Common Information Model). CIM es un modelo abstracto que representa los objetos involucrados en la operación de una red eléctrica en todos los dominios. Al proporcionar una forma estándar de representar los recursos del sistema de energía como clases

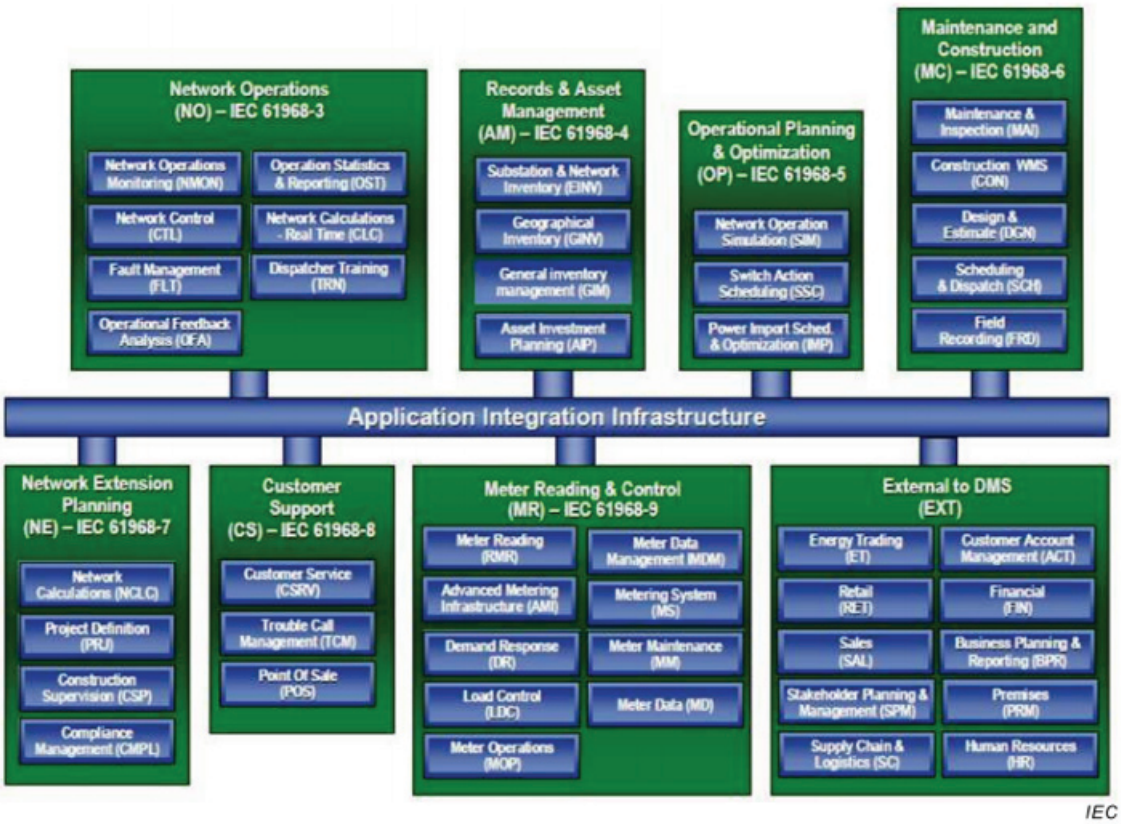


Figura 50: Dominios de aplicación CIM (IEC TC57).

de objetos y atributos, junto con sus relaciones, CIM facilita la integración de aplicaciones de red desarrolladas de forma independiente por diferentes proveedores, también facilita la comunicación de aplicaciones con responsabilidades en diferentes ámbitos de la organización (operación/mantenimiento, operación/mercados, etc).

CIM facilita la integración al definir un lenguaje común (es decir, una semántica) para permitir que estas aplicaciones o sistemas accedan a datos públicos e intercambien información independientemente de cómo se represente internamente dicha información.

Dado que en este documento se describe cómo integrar un nuevo sistema (el SASCTI) con sus casos de uso, el modelo CIM debe de jugar un papel relevante a la hora de interactuar con otros sistemas de la distribuidora eléctrica. También dentro del propio sistema SASCTI, dado que este, como se verá más adelante, albergará Casos de Uso múltiples probablemente desarrollados por distintos fabricantes.

La gestión de la red eléctrica es compleja, diferentes áreas de la compañía ejercen diferentes funciones y los sistemas ayudan a que los procesos orientados a cumplir con estas funciones sean eficientes. La gráfica ilustra muy bien esto, la familia de estándares CIM definen tanto las funciones de estos sistemas como los interfaces, esto es muy importante dado que a la hora de realizar una integración deberemos definir qué mensajes tenemos que intercambiar.

El modelo CIM está compuesto por los siguientes grupos:

- IEC 61968, Para modelado de sistemas de energía e intercambio de datos incluidos EMS, topología, cables, SCADA, etc.
- IEC 61970, Para el modelado de sistemas de energía relacionados con DMS, activos, fuerza de trabajo, GIS, medición y mensajería de aplicaciones.
- IEC 62325, Modelado para los mercados de energía con soporte para los mercados de América del Norte y Europa

4.8.3. El paradigma IEC 61850

El concepto de Smart Grid implica un salto tecnológico que conduce a una gestión que aprovecha los recursos más eficientemente, aumentando las posibilidades de análisis o acción y el control del operador. IEC 61850, es un estándar que nació para ser aplicado en el ámbito de las subestaciones pero que se extendió al resto del sistema eléctrico dado su potencial.

IEC 61850 es un estándar completo para la automatización de cualquier sistema de suministro eléctrico. Aunque una de sus características principales es la implantación de una red LAN, se trata de mucho más que un protocolo. Sus fundamentos técnicos se resumen en tres grandes bloques:

- **Modelo de datos semántico:** un modelo de información orientado a objetos cuyos elementos tienen una denominación que reflejan la realidad física. Se trata de una estructura de datos jerárquica cuyo elemento fundamental es el nodo lógico, que representa funciones básicas dentro del sistema. En el ámbito de los CT destacan los siguientes nodos lógicos:
  - XCBR/XSWI/CSWI: control de interruptores y seccionadores.
  - SCBR/SSWI: supervisión de interruptores y seccionadores.
  - YPTR: transformador
  - SPTR: supervisión del transformador.
  - YLTC y ATCC: intercambiador de tomas
  - Nodos de protección: PTOC (sobreintensidad), PTTR (imagen térmica), etc.
  - ITCI: telecontrol
  - MMXU: medidas

  Los nodos lógicos se agrupan para formar dispositivos lógicos que están ubicados en dispositivos físicos.
- **Servicios:** las operaciones de control y protección se llevan a cabo a partir del intercambio de información entre los equipos. La información en cualquier punto de la subestación pasa a estar disponible instantáneamente en cualquier otra ubicación.

Esto permite optimizar las funciones existentes y desarrollar otras nuevas.

- **Protocolos de comunicaciones:** la materialización de los servicios tiene lugar mediante la definición de protocolos de comunicación específicos:
  - MMS para el envío de información de telecontrol a la RTU.
  - GOOSE para la comunicación de eventos entre IEDs.
  - Sampled Values para el envío de medidas muestreadas.

Todas estas capacidades se describen y configuran en ficheros de texto estructurados que utilizan un lenguaje común, lo que los hace independientes de las herramientas propietarias y permite establecer procesos de ingeniería y mantenimiento globales basados en sistemas de información centrales.

El principal objetivo del estándar se centra en la interoperabilidad, entendida como la posibilidad de que todos los dispositivos funciones conjuntamente, intercambiando información bajo unas reglas comunes basadas en los conceptos mencionados. Desde el punto de vista

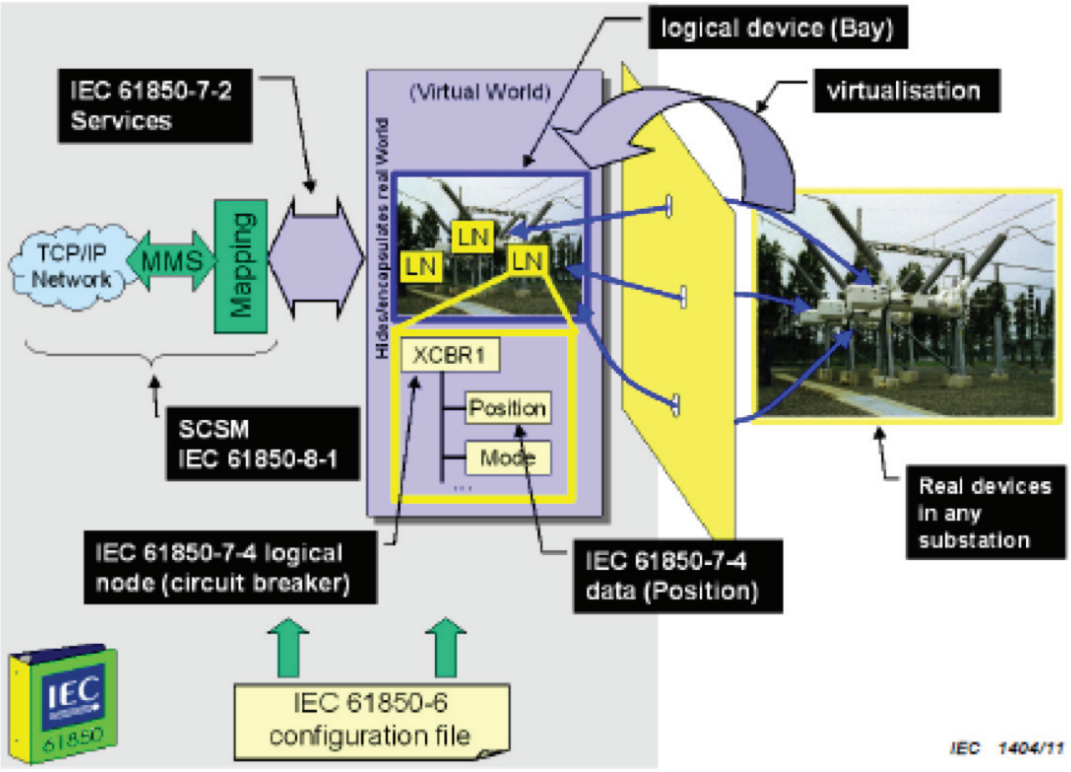


Figura 52: Ecosistema IEC 61850.

La primera implicación de estos conceptos es la sustitución de la mayor parte del tendido de cobre para la señalización de control y protección por una red de comunicaciones. Aunque esto resulta en un primer ahorro material que depende de cada instalación, el verdadero beneficio, del mismo modo que con el SASCTI, llega en el aumento de posibilidades funcionales sin incremento del coste y la optimización de todas las funciones de gestión y mantenimiento debido a la mejora de los tiempos de respuesta y de la capacidad de reacción ante fallos.

pragmático, la interoperabilidad es algo que se logra en las primeras fases experimentales ya que equipos de diferentes fabricantes son capaces de enviar y recibir mensajes con origen y destino en dispositivos de otros fabricantes. El verdadero reto viene al aplicar la idea de intercambiabilidad, es decir, la posibilidad de sustituir un equipo por el de otro fabricante, cuyas dificultades se han debido, principalmente, a los grados de libertad que permite la norma en cuanto al modelado de la información y la configuración.

4.8.4. Protocolos de comunicaciones en entornos IoT.

4.8.4.1. MQTT: Message Queue Telemetry Transport [29]

MQTT es un protocolo estándar de mensajería orientado a IoT. Ha sido diseñado para ser extremadamente ligero utilizado un mecanismo de publicador/subscriptor. Esto lo hace muy eficiente a la hora de ser implementado en equipos remotos con recursos limitados, utilizando un ancho de banda mínimo. Además, implementa mecanismos de seguridad basados en permisos y existen multitud de implementaciones abiertas y está soportado por gran parte de los servidores/brokers el mercado.

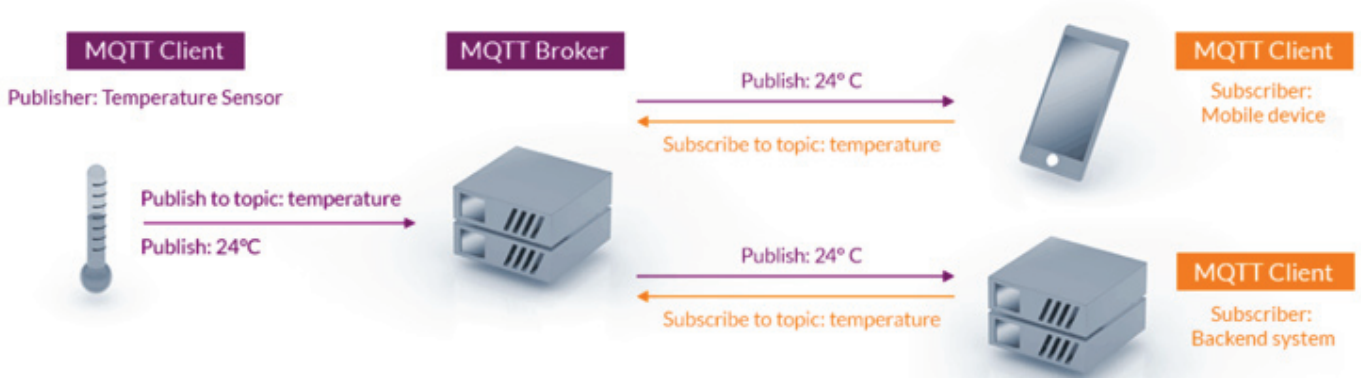


Figura 53: Componentes MQTT.

4.8.4.2. AMQP: Advanced Message Queuing Protocol[30]

Es un protocolo orientado a la fiabilidad, interoperabilidad y seguridad. Está basado en tópicos (topics) y cabeceras (headers) para envío (publicador) y recepción de mensajes (subscriptor), enrutamiento flexible, colas confiables, transacciones y seguridad. Su implementación es más compleja que el MQTT, pero se puede decir que es más completo en las capacidades de administración y gestión de los flujos de información.

El protocolo AMQP resuelve varios problemas al mismo tiempo: por un lado, el protocolo (en colaboración con un bróker de mensajería) se encarga de una transmisión sólida de datos. Por otro, AMQP soporta almacenar mensajes en una cola. Esto, a su vez, permite una comunicación asíncrona: transmisor y receptor no deben actuar al mismo ritmo. El receptor (consumidor) del mensaje no tiene por qué aceptar, procesar la información directamente y confirmar la recepción al emisor (productor). En su lugar, recuperará el mensaje de la cola cuando tenga capacidad disponible para ello. Esto ofrece al productor, entre otras cosas, la posibilidad de seguir trabajando y se evitan los tiempos de inactividad.

4.8.4.3. OPC UA[31]

OPC UA (Open Platform Communications Unified Architecture) es un estándar independiente de la plataforma a través del cual varios tipos de sistemas y dispositivos pueden comunicarse enviando mensajes de solicitud y respuesta entre clientes y servidores o de forma similar a MQTT mediante un modelo de suscripción – publicación.

En los servidores OPC UA se definen los servicios que pueden proporcionar a los clientes, un modelo de objetos que puede ser descubierto dinámicamente por los clientes y un modelo de datos siguiendo los data-types definidos en el propio protocolo.

Un cliente puede comunicarse con uno o varios servidores, un servidor de la misma forma puede comunicarse con varios clientes. Los servidores pueden actuar como clientes para la comunicación con otros servidores.

OPC UA da un espacio de direcciones (AddressSpace) consistente e integrado y un modelo de servicio. Esto permite a un solo

[29] https://mqtt.org/

[30] https://www.amqp.org/

[31] https://opcfoundation.org/about/opc-technologies/opc-ua/

servidor integrar datos, alarmas y eventos en este espacio de direcciones y proveer acceso a ellos usando sus servicios integrados que incorporan mecanismos para que los clientes puedan detectar y recuperar los fallos en la comunicación.

En cuanto a seguridad OPC UA dispone de sesiones encriptadas, firmado de mensajes, secuenciación de paquetes, autenticación, control de los usuarios e información de auditoría.

4.8.4.4. CoAP: Constrained Application Protocol [32]

Es un protocolo cliente-servidor que, a diferencia de MQTT, aún no está estandarizado al 100%. Con CoAP, un nodo cliente puede comandar a otro nodo vía un paquete CoAP. El servidor CoAP lo interpretará, extraerá la información del paquete, y decidirá qué acción realizar dependiendo de su lógica. El servidor no necesariamente realizará la confirmación de la petición.

4.8.4.5. DDS: Data Distribution Service [33]

Es un modelo publicador/subscriptor creado para dispositivos de tiempo real.

Se presenta como un middleware centrado en los datos que especifica dos niveles: DCPS (Data-Centric Publish-Subscribe) que garantiza el reparto de la información de un modo eficiente a los receptores adecuados y DLRL (Data Local Reconstruction Layer) que permite una integración simple de DDS en la capa de aplicaciones.

4.8.4.6. ZeroMQ [34]

Es un middleware de comunicaciones de alto rendimiento orientada a mensajes, destinada a la construcción de aplicaciones distribuidas. Está basada en colas de mensajes, pero a diferencia de otros middlewares orientados a mensajes, ZeroMQ no necesita un broker intermedio.

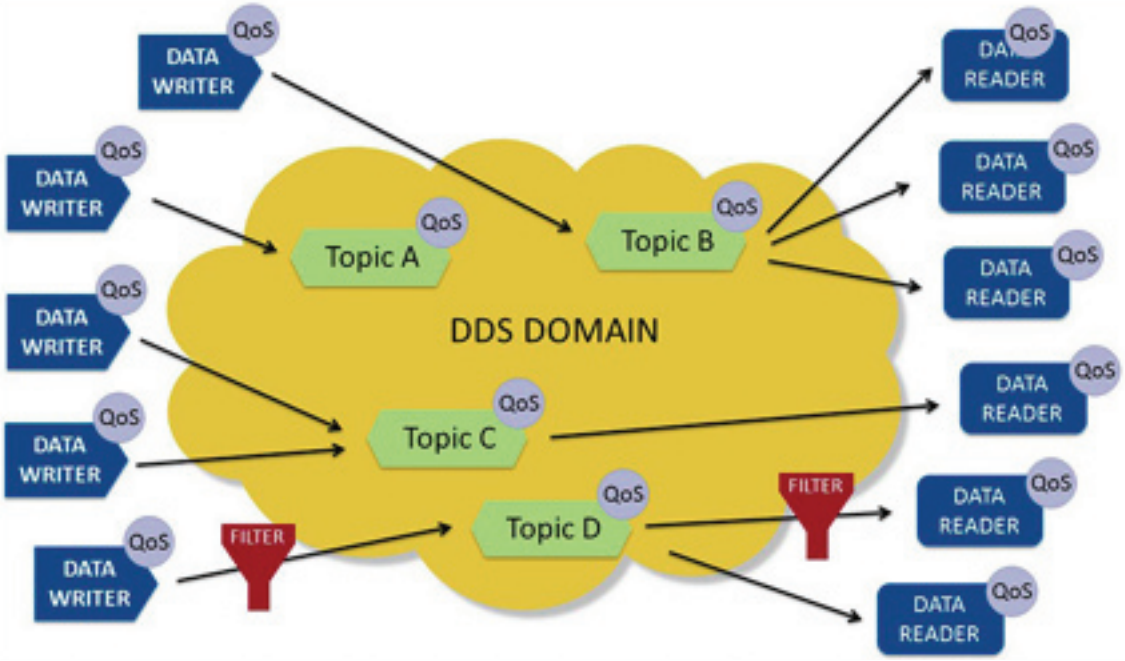


Figura 54: Componentes DDS.

[32] https://tools.ietf.org/html/rfc7252
[33] https://www.dds-foundation.org/what-is-dds-3/
[34] https://zeromq.org/

5. REQUISITOS BASE: SASCTI

5.1. Arquitectura SASCTI

Como ya se ha indicado en varias ocasiones en el documento, en contraposición con la infraestructura en nube tradicional, basada en grandes centros de datos que centralizan el poder computacional, el Edge Computing propone una distribución de esta capacidad de procesamiento hacia los extremos de la red.

Figura 55: Arquitectura de Referencia Empresarial Purdue comparado con un modelo de referencia de Internet de las cosas.

Esta arquitectura no se plantea como un sustituto de las infraestructuras en nube tradicionales, sino como una extensión de las mismas.

Aquellas aplicaciones que requieran del procesado de datos en tiempo real o que por sus características demanden un gran consumo de ancho de banda, podrán sacar partido de la cercanía, baja latencia, seguridad y resiliencia que ofrece el Edge Computing como arquitectura distribuida.

En resumen, el procesamiento distribuido permite que en los Centros de Transformación:

- Los equipos no necesiten estar conectados de forma continua y pueden trabajar de forma autónoma.
- Las necesidades de ancho de banda se reduzcan de forma drástica en algunas aplicaciones.
- Al reducirse la latencia se puedan utilizar soluciones en tiempo real, que son mucho más complicadas cuando el procesamiento se produce en la nube.
- Los datos no se transmitan y se procesen de forma local reduciendo su exposición y aumentando su seguridad y la privacidad. Por otra parte, al referirnos a la necesidad de distribución del procesamiento no solo estamos diciendo que geográficamente se distribuya dicha capacidad para tener una cobertura por redundancia, sino que si lo viéramos desde los niveles de Purdue la capacidad de procesamiento también estaría distribuida entre dichos niveles y no solo en uno de ellos.

Dentro del entorno industrial, el Modelo Purdue de ISA-95, que separa en 5 niveles la red, es una buena guía para su segmentación y para el aumento de la seguridad, ya que los niveles están bien definidos.

El sector eléctrico es un sector crítico y esencial, y con frecuencia un fallo de suministro eléctrico implica una interrupción del canal de comunicaciones. Esta posibilidad de interrup-

ción de las comunicaciones es lo que hace primordial que la capacidad de procesamiento y toma de decisiones, en cuanto a temas de seguridad de las personas e instalaciones (safety), deba distribuirse en los niveles 1 y 2 (dispositivos y centros de transformación).

Por otro lado, existen necesidades de optimización de la explotación de red, reducción de parámetros como pérdidas técnicas o tiempos de interrupción. En este caso, la capacidad de procesamiento hay que elevarla un nivel por encima de los centros de transformación para poder coordinarlos eficientemente.

Para otras aplicaciones de mercado, comparativas, ponderaciones con bases de datos climatológicas, demográficas, estadísticas que buscasen la estimación de vida del activo, planificaciones futuras que no dependen del dato en tiempo real y que el dato de un centro de transformación por sí mismo no aporta tanto como el dato tratado con fuentes externas, se prescribe que el procesamiento se haga centralizado o incluso en la nube, no solo por existir mayor capacidad sino por no reducir la capacidad de procesamiento local que debe atender temas de safety además de reducir riesgos en cuanto a la protección de datos personales en el caso de ser necesarios. Entre estas aplicaciones estarían las consultas de validación de trabajadores en Controlar.

La arquitectura del SASCTI se diseña teniendo en cuenta no sólo el centro de transformación sino también su integración en la red de distribución.

Tomando como referencia el modelo SGAM, esta integración debe darse en tres ejes:

1. En el eje de los dominios:

   Si bien el SASCTI se trata de un sistema instalado en el CT, su ámbito de actuación llega hasta el límite del dominio de las instalaciones de cliente ya que tanto la información que utiliza como el efecto de las actuaciones alcanzan hasta el límite de propiedad de la red, es decir las CGP.

2. En el plano de componentes:

   Los servicios que proporciona el SASCTI van desde la monitorización y operación de los equipos y sistemas del CT (zona de proceso) hasta la toma de decisiones de negocio (zona de empresa). Se podría incluso considerar la zona de mercado

3. En el eje de capas de interoperabilidad

   En consonancia con el ámbito definido en el eje de zonas se determinan las capas de interoperabilidad, que van desde la capa de componentes hasta la de negocio.

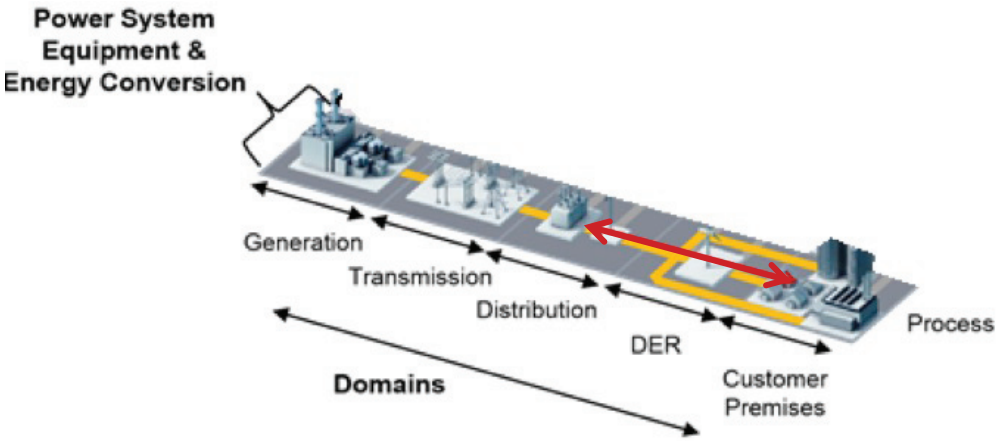


Figura 56: Dominios en el sistema eléctrico según el modelo SGAM.

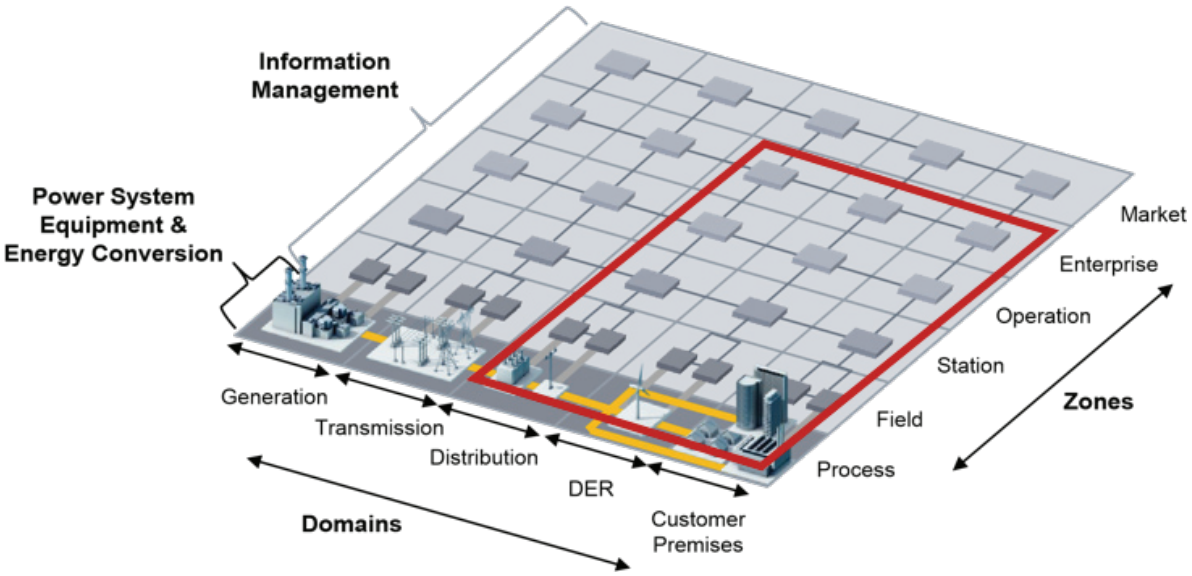


Figura 57: Dominios y zonas de gestión de la información en el sistema eléctrico según el modelo SGAM.

Por lo tanto, el SASCTI, alojado en un CT, proporciona interfaces físicas y lógicas para poder alcanzar:

1. Hasta el límite de propiedad del cliente.
2. Hasta la zona de empresa.
3. Hasta el dominio de negocio.

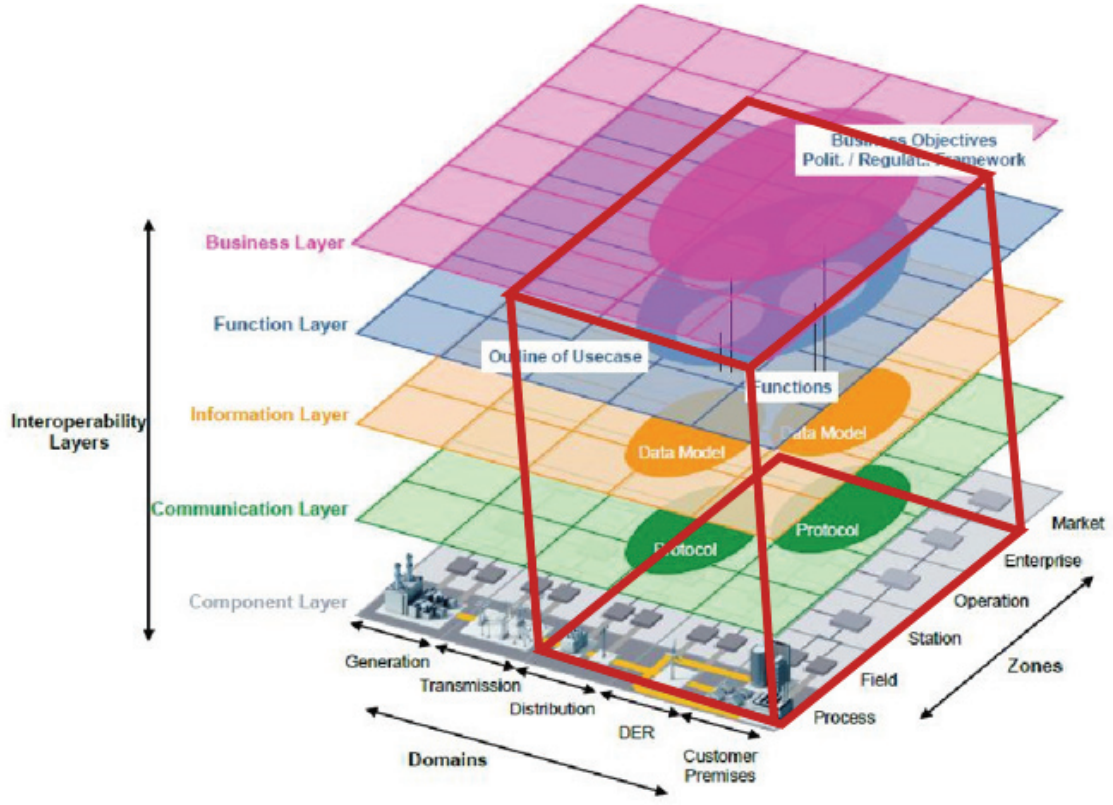


Figura 58: Capas de interoperabilidad del SASCTI según el modelo SGAM.

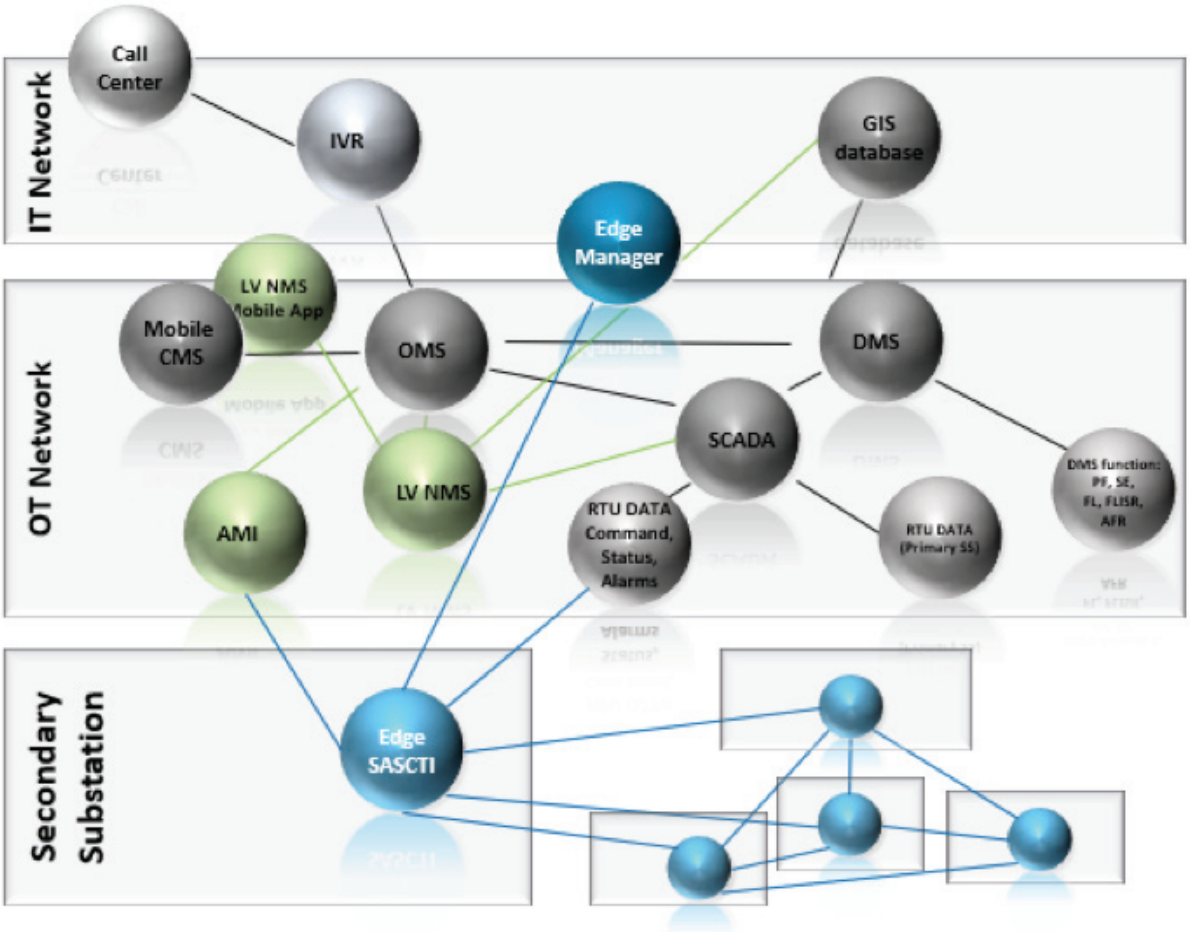


Figura 59: Ejemplo de integración de SASCTI en sistemas IT/OT de la distribuidora.

La arquitectura del SASCTI contempla conexiones directas con distintos dispositivos en campo, así como con distintos sistemas centrales de la Utility como puedan ser sistemas SCADA, sistemas de gestión de la distribución, gestión de medida, mantenimiento, entre otros.

El siguiente esquema muestra la arquitectura software de alto nivel del SASCTI, con los diferentes componentes, sistemas y dispositivos con los que interacciona.

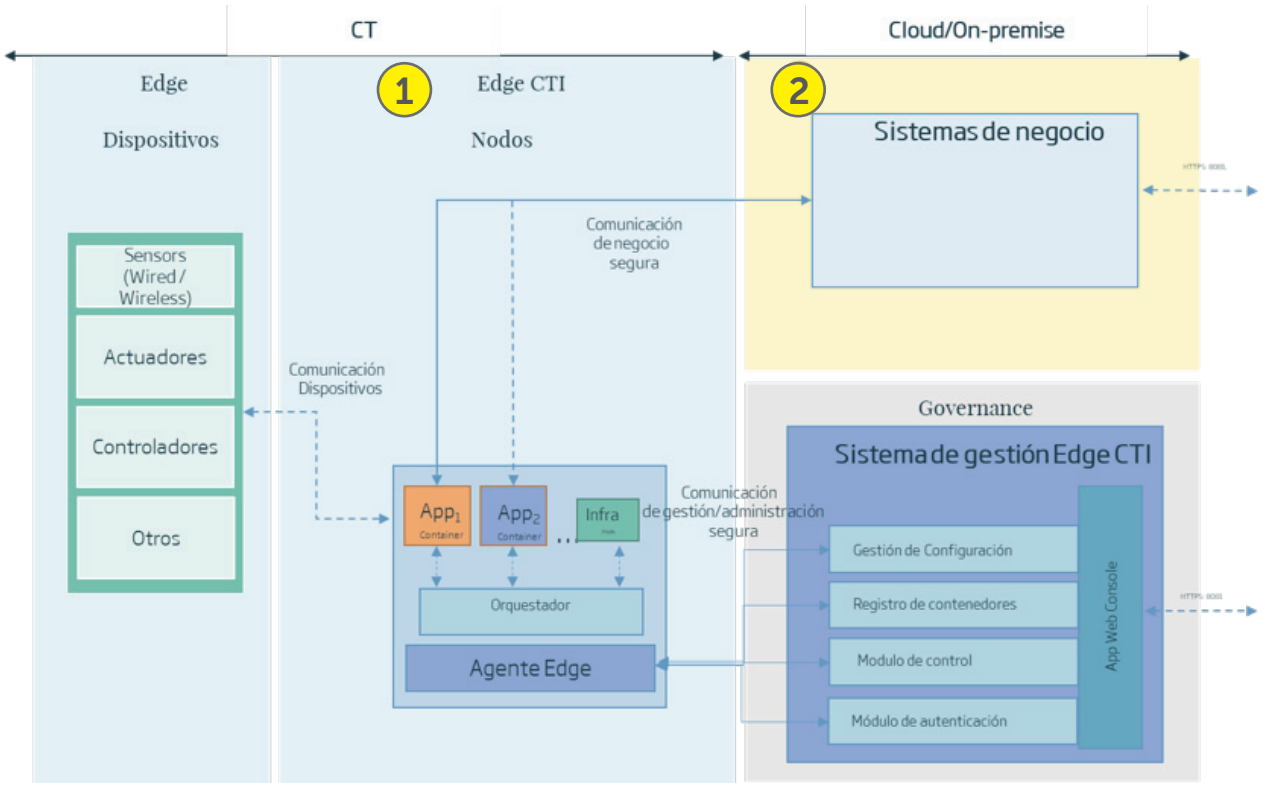


Figura 60: Arquitectura SW de alto nivel del SASCTI.

La arquitectura del SASCTI se desarrolla en dos niveles de gestión Edge:

1. **Edge SASCTI,** instalado en el CT Inteligente gestionando el flujo de información y control con los dispositivos en el ámbito del CT y habilitando un espacio virtual (puntos 3 y 4 del esquema de la figura 67) basado en contenedores para el procesamiento, análisis y automatización local estandarizado.

2. **Sistema central de gestión Edge,** sistema central instalado en zona de sistemas OT de la Utility desde el que se monitoriza y gestiona el parque completo de nodos Edge SASCTI, y el contenido de aplicaciones desplegado.

5.2. Requerimientos arquitectura SW SASCTI

Los siguientes apartados recogen los requerimientos para los principales componentes SW que configuran la arquitectura del SASCTI.

Con el objetivo de explotar experiencias previas en otros ámbitos y acelerar la especificación del SASCTI algunos de los requerimientos identificados en este apartado podrán recomendar en base a estas experiencias el uso de algunas tecnologías entrando en un plano de especificación de arquitectura.

Una vez completado el análisis de casos de uso estas recomendaciones deberán ser revisadas para verificar su adecuación a los requerimientos funcionales detallados resultado de este ejercicio de análisis.

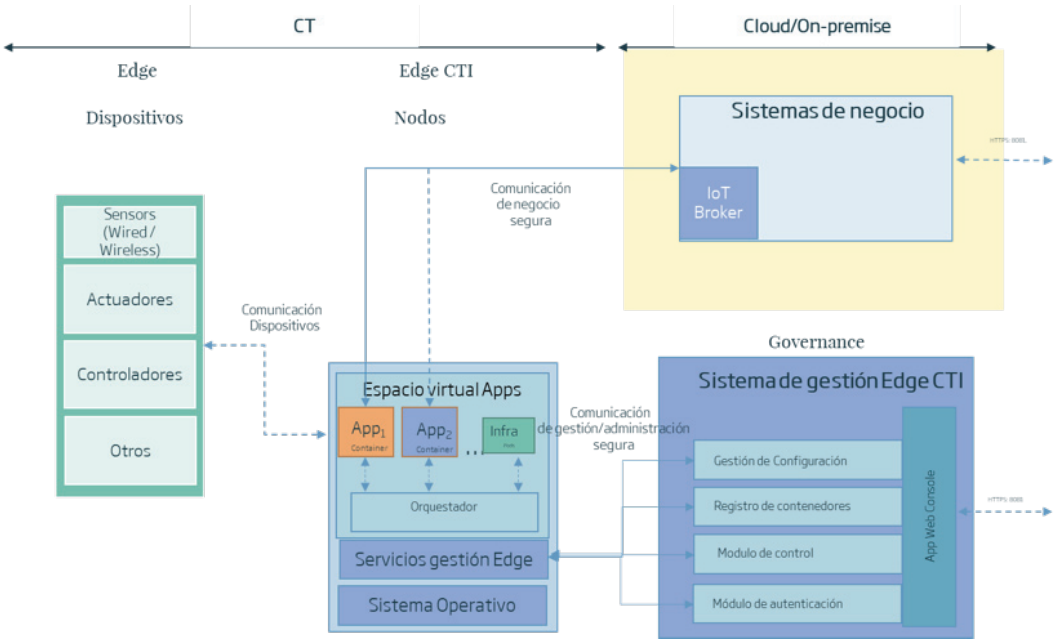


Figura 61: Arquitectura SW por componentes del SASCTI.

5.2.1. Servicios core de gestión/ administración Edge.

El SASCTI en su componente Edge debe de contar con una capa de servicios core de gestión y Administración que se ha identificado como **Agente Edge** instalado en el Nodo Edge que esté continuamente en ejecución.

Este Agente Edge puede ser un único ejecutable o varios directamente compilados sobre el sistema operativo y corriendo como Administrador.

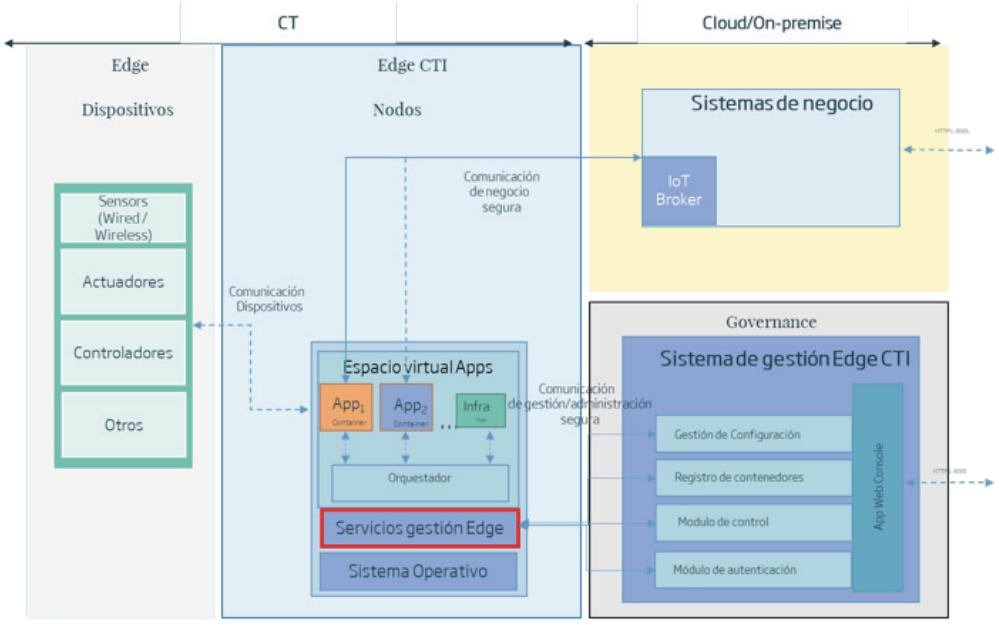


Figura 62: Servicios de Gestión Edge o Agente Edge en la arquitectura SW del SASCTI.

Requerimiento	Al menos uno de esos	Recomendado
Seguridad	SELinux, Seccomp, Apparmor, Container Security, Managed Firewalls (L3/L4)	Managed Firewalls, SELinux, Container Security policy.
Comunicaciones	Linux bridges, OVS, IOVisor, other CNIs	Linux bridges
Almacenamiento	Any format supported as Container Storage Interface (CSI).	
Ceph, Gluster, Local SSD, RAID, iSCSI, USB, NFS.	Local SSD with overlay2	
Backup e instantaneas	**Snapshot - live, snapshot-paused**	**Snapshot – live**
Monitorización de servicios	**Systemd restart, container restart**	**Systemd restart, container restart**
Monitorización de recursos	**Built-in, 3rd party integrated**	**Built-in (e.g. Prometheus or Telegraf)**

5.2.2. Virtualización y Encapsulamiento de funciones

Uno de los aspectos fundamentales a los que una arquitectura Edge debe de dar respuesta es al encapsulamiento, gestión y distribución de la funcionalidad de negocio en cientos o miles de dispositivos Edge.

El objetivo de este documento es dar pautas para el diseño de nuevos CT, buscando su versatilidad funcional, escalabilidad y eficiencia en costes. A lo largo de otros apartados del documento, se describen en detalle las funcionalidades o casos de uso de mayor interés para las distribuidoras.

A modo de resumen, estos son los bloques funcionales que se contemplan:

- Concentrador de datos
- Supervisión avanzada de BT
- Descubrimiento de red eléctrica
- Gestión de activos
- Supervisión de red
- Analítica de red
- Control de red
- Gestión de la energía – flexibilidad
- Movilidad, operación y mantenimiento de red
- Ciberseguridad
- Seguridad

Todos ellos requerirán de implementaciones más o menos complejas en los SASCTI. Así pues, y tal como se menciona en el estado del arte de este mismo documento, se considera que la virtualización, el encapsulamiento y las funciones en modo de microservicios deben ser las tecnologías elegidas para el despliegue de las funciones requeridas en los nuevos SASCTI.

Este encapsulamiento funcional del SASCTI deberá de cumplir con los siguientes requerimientos para lograr los objetivos identificados: versatilidad funcional, escalabilidad y eficiencia en costes.

5.2.2.1. Requerimientos generales para el encapsulamiento de aplicaciones SASCTI

a) El mecanismo de encapsulamiento debe de ser abierto y basado en iniciativas de open source de adopción mayoritaria evitando dependencia con plataformas propietarias que limiten la competencia y encarezcan su coste.

b) Debe de ser acorde con arquitectura de microservicios, una unidad de encapsulamiento. por cada microservicio.

c) El acceso a los recursos de infraestructura y apertura de puertos de comunicaciones no puede ser gestionado directamente por las aplicaciones para evitar dependencias con la infraestructura HW y riesgos de ciberseguridad.

Todo el acceso a recursos HW de las aplicaciones deberá ser gestionado de forma unificada dentro del nodo Edge.

d) La tecnología de encapsulamiento debe de optimizar el uso de recursos en el nodo Edge SASCTI, optimizando el uso de memoria y CPU, y facilitando el despliegue de nuevas aplicaciones en entornos con comunicaciones limitadas. Para ello el tamaño medio de las aplicaciones en ejecución y sus imágenes no debería de superar los 400 Mb.

e) Soporte flexible a un rango amplio de lenguajes de programación y librerías necesarias, que permita desplegar tanto aplicaciones de tiempo real como HMIs, gestores de reglas, aplicaciones analíticas complejas, y aplicaciones de control.

f) Todas las aplicaciones incluirán un fichero de configuración gestionable por el gestor Edge, que permita particularizar su funcionamiento a cada SASCTI.

g) Las aplicaciones deberán habilitar mecanismos para exponer interfaces web de monitorización y gestión remota de la aplicación.

h) Las aplicaciones podrán habilitar interfases API rest en caso de requerir comunicaciones en modo petición/respuesta de otras aplicaciones.

5.2.2.2. Espacio de aplicaciones SASCTI

Todas las aplicaciones ejecutadas en el SASCTI se deberán desarrollar y virtualizar en un mismo entorno para asegurar un mejor aprovechamiento de los recursos Edge.:

- Sistema de ficheros único por defecto, mejorando la velocidad y la gestión.
- Funciones generales de monitorización y resolución de seguridad y vulnerabilidades.
- Simplificar el proceso de certificación.
- Homogeneidad en las herramientas, flujos de compilación y utilización de recursos de entorno.

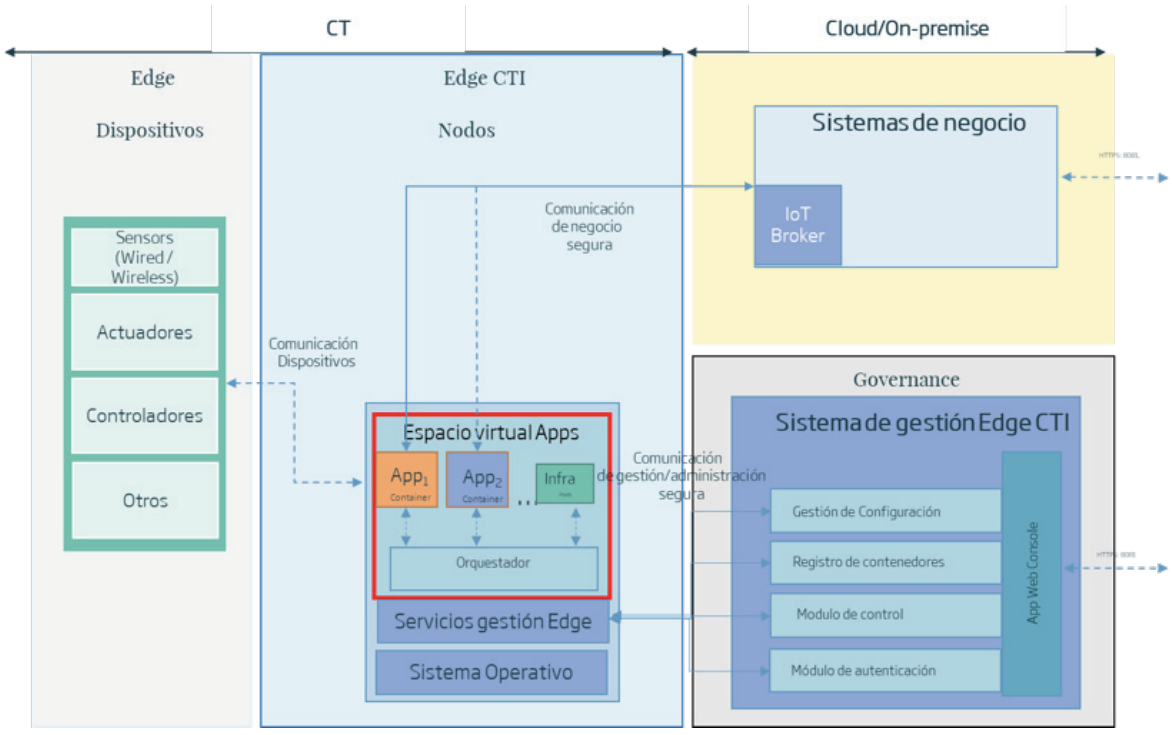


Figura 63: Espacio virtual de aplicaciones SASCTI en la arquitectura SW del SASCTI.

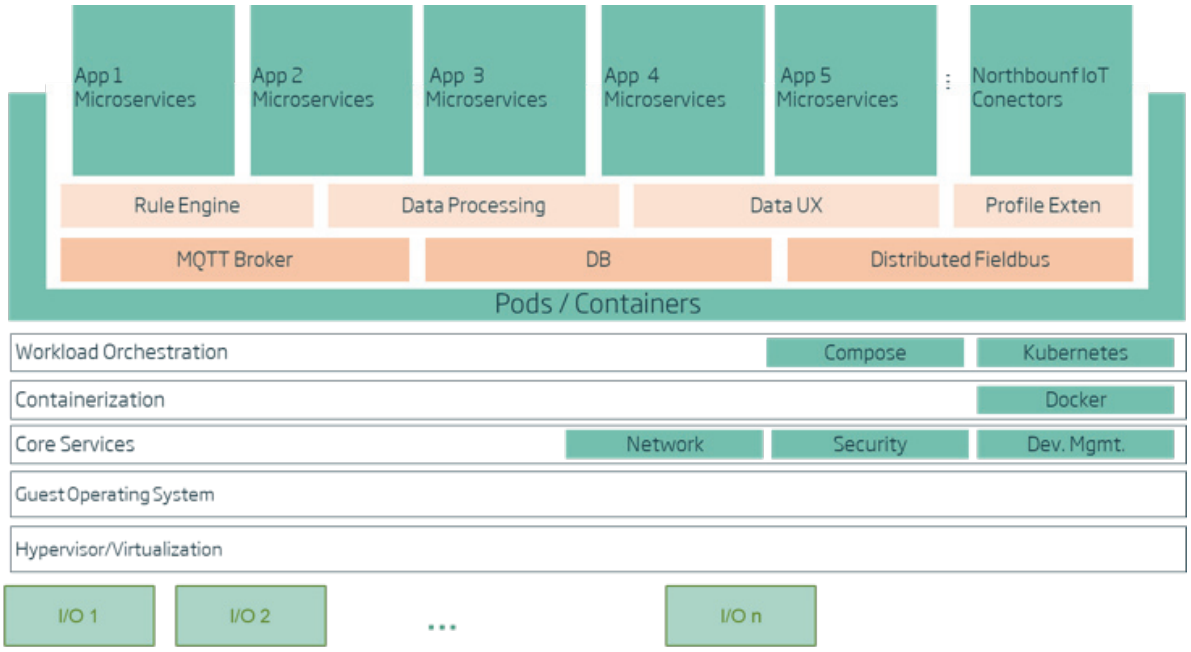


Figura 64: Catálogo general de servicios en el espacio virtual de aplicaciones Edge.

El SASCTI deberá de habilitar los siguientes servicios básicos en forma de aplicaciones:

a) Bus interno de comunicaciones que gestione el intercambio de información entre aplicaciones y estandarice el modelo de información interno del nodo Edge. Independientemente de la configuración de dispositivos en el SASCTI. Este bus debe de cumplir los siguientes requerimientos básicos:
   - Minimizar el uso de recursos.
   - Basarse en mecanismos de publicación/subscripción.
   - Optimizado para intercambio de mensajes pequeños con alta frecuencia.
   - Flexible en el formato y composición de los mensajes a intercambiar.

b) Base de datos local de trabajo.
   - Ligera.
   - Almacenamiento configurable de mensajes publicados en el bus interno de comunicaciones.
   - Orientada al almacenamiento de datos de trabajo de las aplicaciones y búfer de datos salientes ante perdidas temporales de comunicaciones.

c) Gestores de comunicación con dispositivos OT. Deben tener acceso a puertos de comunicaciones con los dispositivos, y soportar los protocolos de comunicaciones que se definan para el ámbito OT:

d) Gestores comunicaciones IoT/IT. Gestión de las comunicaciones con sistemas de control y operación centrales.

e) Gestores de reglas que permitan automatizar de forma flexible y rápida reglas de procesamiento sobre los flujos de información circulando en el bus interno: Alarmas de umbral, cálculo de agregados, protecciones.

f) Interface HMI, que permita de forma local o visualizar/controlar de forma remota la información fluyendo por el bus interno.

g) Aplicaciones de control, que permitan implantar lógicas de control de dispositivos.

h) Aplicaciones analíticas, para el diagnóstico o control experto de del SASCTI.

5.2.2.2.1. Gestión de configuraciones y almacenamiento de datos de las aplicaciones.

Los archivos de almacenamiento en un contenedor son efímeros, el contenedor comienza con un estado limpio y, a menudo, es necesario aplicar una configuración específica o

compartir archivos entre esos contenedores. La abstracción de volumen de Kubernetes resuelve ambos problemas con los volúmenes persistentes, es decir, el almacenamiento que tiene un ciclo de vida independiente de cualquier Pod individual.

La plataforma SW pondrá a disposición 2 tipos de almacenamiento para las aplicaciones:

- Acceso a un sistema de archivos independiente para registros y otro para almacenamiento de archivos. Este espacio será de acceso único para la aplicación
- Acceso al conjunto de servicios de base de datos relacional y de series temporales. El sistema proporcionará un usuario específico para que la aplicación pueda administrar su propia base de datos de forma independiente.

La plataforma se asegurará del cumplimiento de los límites asignados en el uso de las BBDD.

5.2.2.2.2. Seguridad de aplicaciones.

Se podrán utilizar los dispositivos TPM / HSM presentes para realizar operaciones de Secure Boot y establecimiento de una raíz de confianza (Root of Trust). Estos son capaces de autenticar tanto la distribución o el SO a través de una clave pública (PK) establecida. El firmware firmado y autenticado a través del módulo de seguridad puede contener claves públicas adicionales (Key exchange Keys o KEK) que comprueben la validez de las aplicaciones o contenedores instalados. Estas bases de datos de claves públicas soportarán también un almacén de claves prohibidas (o listas de revocación). De este modo cualquier ejecutable que se pretenda lanzar dentro del nodo tendrá que pasar la fase de comprobación de firma, denegándose la ejecución de aplicaciones que no sean de confianza.

5.2.2.2.3. Comunicaciones entre aplicaciones dentro del Nodo Edge Computing

La arquitectura de comunicaciones entre aplicaciones del NEC permitirá los siguientes mecanismos:

- Publicación/Subscripción (Publish/Subscribe)
- Petición/Respuesta (Request/Response)

  Las comunicaciones entre los componentes de software dentro del SASCTI están reguladas por el Modelo de Comunicación Interna (ICM). Dentro de este modelo de comunicación, cada componente de software empaquetado como un contenedor (o Pod de Kubernetes, si la proporción entre ellos es 1: 1 se considera un Servicio (o una Aplicación).

  El modelo de comunicaciones del SASCTI contempla cuatro tipos de intercambios (o flujos) de información entre los componentes de software implementados dentro de la subestación basados en estos dos esquemas de comunicación.

- **Tipo de mensaje.1**.- Bajo demanda y síncrono. Servicio (o un App1) requiere información de otro Servicio2 (o App2), esta solicitud debe ser respondida inmediatamente vía HTTP/REST al solicitante y in paralelo al tópico de MQTT correspondiente.
- **Tipo de mensaje.2**.- Bajo demanda y asíncrono. Servicio (o un App1) requiere información de otro Servicio2 (o App2), esta solicitud debe ser validada inmediatamente con un "ack" al solicitante via HTTP/REST y respondida cuando se tenga la información vía el tópico de MQTT correspondiente.
- **Tipo de mensaje.3**.- Programado. Un Servicio1 (o App1) requiere información de otro Servicio1 (o App1), debido a la duración de las tareas informáticas necesarias para generar la respuesta completa, la tarea debe programarse. El peticionario recibe una respuesta con la URL necesaria para consumir la información una vez completada.
- **Tipo de mensaje.4**.- Espontáneo. Un Servicio1 (o un App1)) quiere suscribirse para recibir periódicamente algunos datos de otro Servicio2 (o App2). Este Service2 proporciona los datos de forma espontánea.

En base a la amplia experiencia acumulada en la aplicación de estas tecnologías se propone el uso de los siguientes protocolos de comunicaciones para soportar los cuatro tipos de mensajes anteriores:

(i) Servicio web usando HTTP, siguiendo el estilo API REST, y

(ii) MQTT.v.5 o superior,

Se propone utilizar ambos junto con el estándar Web of Things Architecture (WOT-A) patrocinado por W3C (W3C, n.d.).

El uso de WOT-A proporciona al SASCTI una forma simple de interoperabilidad entre los servicios (o aplicaciones) implementados en el SASCTI.

El Anexo II de este documento desarrolla una primera propuesta de especificación para la aplicación de este estándar para dotar al SASCTI de un marco flexible que permita al autodescubrimiento de aplicaciones y su interoperabilidad a través de los tres modos de comunicación requeridos:

Tipo	Modo	Protocolo de petición	Protocolo de respuesta
1	Bajo demanda	HTTP/REST	HTTP/REST y/o MQTT
2	Bajo demanda	HTTP/REST	HTTP/REST (ACK) y/o MQTT
3	Planificado	N/A	MQTT
4	Espontaneo	N/A	MQTT

Tabla 2: Modos de comunicación entre aplicaciones.

La adecuación de estas tecnologías y estándar al ámbito SASCTI deberá ser objeto de verificación tras la compleción del análisis de casos de uso del SASCTI.

5.2.2.2.3.1. Modelo publicación/subscripción:

El modelo publicación/subscripción proporciona un marco flexible y escalable para el intercambio de mensajes entre aplicaciones. Este modelo implica que el editor y el suscriptor dependen de un agente de mensajes o broker que transmite mensajes del editor a los suscriptores. El editor publica mensajes (eventos) en un canal en el que los suscriptores pueden registrarse.

Típicamente, los mensajes generados por las entidades emisoras son enviados a una entidad denominada bróker. Los subscriptores se registran en dicho bróker y es éste quien realiza las labores de filtrado y redireccionamiento de los mensajes, en función de las preferencias de cada subscriptor en base al tipo de mensaje que desea recibir.

Las ventajas que este modelo de comunicaciones aporta al SASCTI son las siguientes:

- Integración transparente de entidades. Los emisores y subscriptores se integran de forma transparente, sin necesidad de conocer la existencia de otros ni la topología del sistema. Cada uno puede funcionar de forma autónoma independientemente del estado del otro. También es posible que editores envíen información aun cuando los subscriptores no estén activos, o que subscriptores se registren a mensajes de editores no activos, siendo el bróker del sistema el que garantizará, si es necesario, la entrega de la información.
- Escalabilidad. Este modelo de comunicaciones es altamente escalable, especialmente en entornos donde cada aplicación reside en máquinas físicas diferentes. La integración de un nuevo subscriptor o editor, como se ha dicho antes, es totalmente transparente y no requiere la adaptación de ninguna entidad del sistema. A nivel de NEC, la principal ventaja de modelo residirá en que cada aplicación será independiente del resto aunque haya establecido un flujo de comunicaciones entre ellas (siempre que el modelo de datos esté claramente definido).

Un ejemplo de este tipo de protocolos es MQTT (Message Queuing Telemetry Transport). Este protocolo fue originalmente diseñado para sistemas de bajo consumo y con redes de comunicaciones inestables, y sería válido para el intercambio de información ligera y frecuente dentro del SASCTI.

5.2.2.2.3.2. Modelo petición/respuesta:

El modelo petición/respuesta, también conocido como cliente/servidor, se basa en la existencia de una entidad (servidor) a la que es posible realizar peticiones de información por parte de otra entidad (cliente), al estilo de los servidores web tradicionales. Los servidores exponen o publican los métodos a los que son capaces de responder, que serán utilizados por los clientes para obtener la información que desean.

Este tipo de arquitectura resulta más rígida que el modelo publish/subscribe, ya que requiere que los clientes conozcan la existencia

de los diferentes servidores para obtener los datos, y también que los servidores se encuentren activos en el momento de la búsqueda de la información.

Sin embargo, este modelo presenta algunas características que serán necesarias según la funcionalidad que se quiera conseguir:

- **Peticiones bajo demanda.** En ocasiones puede ser necesario obtener información seleccionada en función de parámetros de entrada como fechas, filtros,... Los métodos publicados permitirán añadir parámetros de diferentes tipos para generar una respuesta adecuada a las necesidades del cliente.
- **Peticiones síncronas.** En otras ocasiones es posible que se necesite obtener información inmediata. Los protocolos publish/subscribe no garantizan el sincronismo de los mensajes.

Una implementación típica del modelo cliente/servidor sería la llamada API Rest, que con un funcionamiento similar a los servidores web utilizada json como lenguaje de codificación y expone mediante URLs los servicios ofrecidos.

5.2.2.3. Catálogo general de aplicaciones SASCTI

El SASCTI deberá de habilitar los siguientes servicios básicos en forma de aplicaciones:

a) Bus interno de comunicaciones que gestione el intercambio de información entre aplicaciones y estandarice el modelo de información interno del nodo Edge. Independientemente de la configuración de dispositivos en el SASCTI. Este bus debe de cumplir los siguientes requerimientos básicos:
   - Minimizar el uso de recursos.
   - Basarse en mecanismos de publicación/subscripción.
   - Optimizado para intercambio de mensajes pequeños con alta frecuencia.
   - Flexible en el formato y composición de los mensajes a intercambiar.

b) Base de datos local de trabajo.
   - Ligera.
   - Almacenamiento configurable de mensajes publicados en el bus interno de comunicaciones.
   - Orientada al almacenamiento de datos de trabajo de las aplicaciones y búfer de datos salientes ante perdidas temporales de comunicaciones.

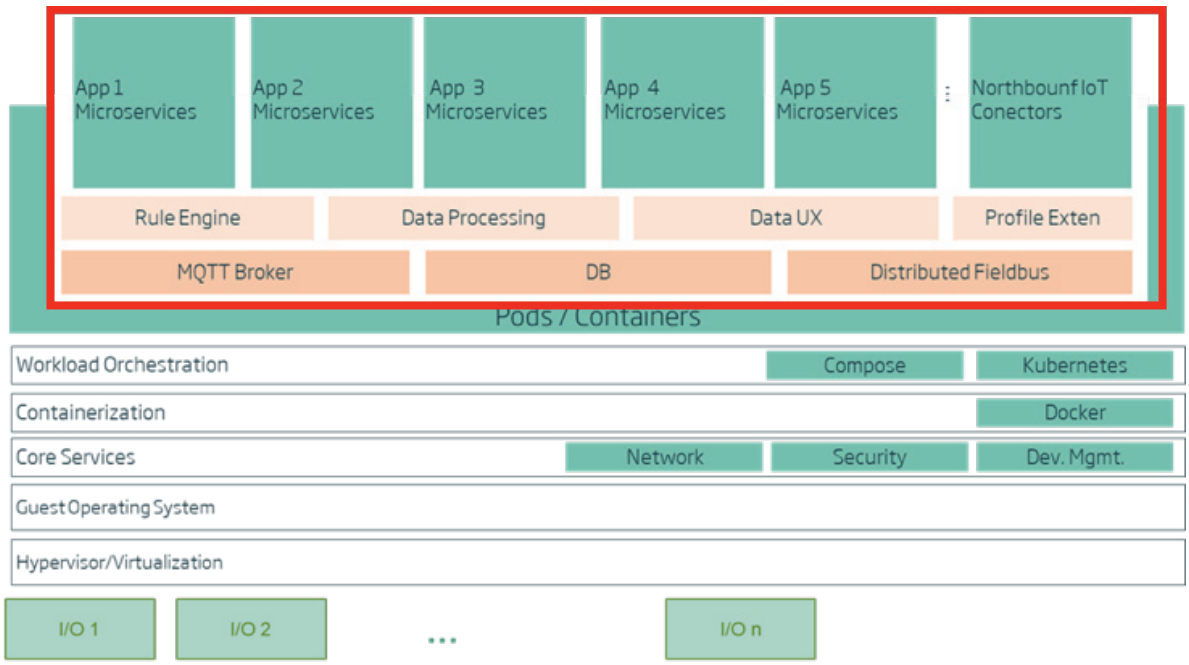


Figura 65: Esquema posible de encapsulamiento de microservicios.

c) Gestores de comunicación con dispositivos OT. Deben tener acceso a puertos de comunicaciones con los dispositivos, y soportar los protocolos de comunicaciones que se definan para el ámbito OT:

d) Gestores comunicaciones IoT/IT. Gestión de las comunicaciones con sistemas de control y operación centrales.

e) Gestores de Reglas que permitan automatizar de forma flexible y rápida reglas de procesamiento sobre los flujos de información circulando en el bus interno: Alarmas de umbral, cálculo de agregados, protecciones.

f) Interface HMI, que permita de forma local o visualizar/controlar de forma remota la información fluyendo por el bus interno.

g) Aplicaciones de control, que permitan implantar lógicas de control de dispositivos.

h) Aplicaciones analíticas, para el diagnóstico o control experto de del SASCTI.

5.2.2.3.1. Base de datos

La plataforma SASCTI proporcionará acceso a dos tipos de bases de datos en cada nodo Edge:

- Base de datos de relaciones.
- Bases de datos de series temporales.

Por norma general las aplicaciones deberán de hacer uso de las bases de datos comunes de la plataforma, en lugar de crear instancias privadas para dicha base de datos dentro de sus propios contenedores de aplicaciones. La plataforma garantizará la reducción de recursos, la reserva de recursos con aislamiento de datos, protección y seguridad con RBAC.

Sin embargo, si la aplicación requiere un tipo diferente de base de datos para su aplicación (por ejemplo, sqlite), pueden optar por implementar su propia base de datos de aplicaciones dentro de su contenedor, pero este debería ser el último recurso.

Requerimiento	Al menos uno de esos	Recomendado
Base de datos relacional	Postgres,KxDB	Postgres
Base de datos de series temporales	InfluxDB, KxDB	InfluxDB

Tabla 3: Requerimientos base de datos.

5.2.2.3.1.1. Base de datos relacional

Base de datos relacional que permita a las distintas aplicaciones almacenar estructuras de datos privadas, estado de la aplicación y / o configuración del usuario.

- El acceso a la base de datos se realizará a través del conocido puerto 8080 utilizando las API Restful estándar de la BBDD.
- La aplicación puede elegir su propio modelo de datos para almacenar los datos, esto mantiene a cada aplicación en control de sus propias tablas privadas.
- Los datos guardados en esta base de datos están destinados principalmente para uso privado (escritor único / usuario único), no se recomienda el uso secundario para la comunicación entre aplicaciones directamente sobre esta base de datos. La aplicación debe proporcionar API para acceder a su base de datos, si estos datos deben exponerse a aplicaciones adicionales.
- La plataforma limitará el uso de cada aplicación a la base de datos de Postgres (lectura / escritura) para proporcionar una participación justa para que otras aplicaciones tengan acceso a esta instancia de base de datos compartida.
- La plataforma admitirá la reducción de recursos por aplicación según la configuración de la plataforma / aplicación.

5.2.2.3.1.2. Bases de datos para series temporales (InfluxDB)

La plataforma proporcionará una base de datos de series temporales para que las aplicaciones almacenen datos de sensores recopilados (medidores, alimentadores, etc.) para funciones de historial, visualización y análisis.

Una vez que los datos se publican en la TSDB desde las aplicaciones del productor, los servicios de BBDD como:

- Visualización.
- El análisis en línea (streaming) y por lotes Edge.
- La exportación de datos a otros BBDD centrales.
- Y la distribución (Brokerage) de datos a otras aplicaciones pueden ser facilitados por este servicio central de series temporales.

El acceso de escritura de la base de datos se realizada a través de del bus interno de publicación (MQTT u otro equivalente).

Un servicio específico de la BBDD consumiría los datos publicados sobre ciertos topics (topics configurados por el usuario del sistema) y los almacenaría en la TSDB.

Los requerimientos generales que deberá cumplir este servicio TSDB son los siguientes:

- La plataforma admitirá la fragmentación de datos para un acceso más rápido y fiable (prevención de pérdida de datos) en situaciones de fallo del nodo Edge.
- La plataforma admitirá políticas de retención de datos para depurar datos más antiguos (descartar automáticamente después de cierto período).
- Los datos almacenados en la TSDB utilizan cifrado TLS y secretos de autenticación por nodo.
- La plataforma limitará el uso de cada aplicación a la base de datos (lectura / escritura) para asegurar un reparto equitativo entre aplicaciones.
- Los datos almacenados en la TSDB se pueden utilizar para:
  - o Visualización de datos enriquecidos mediante cuadros de mando personalizables por usuario.
  - o Visualización de datos localmente en el nodo Edge o remotamente desde el fogSM centralizado con RBAC completo.
  - o Streaming Analytics en datos ingeridos para derivar notificaciones de Insights y Alarmas.
  - o La notificación de alarmas se puede publicar por correo electrónico, servicio de buscapersonas o una simple notificación http.
  - o Limpieza de datos, transformación de datos o análisis de datos utilizando la función de canalización de datos de la plataforma.
  - o Exportación a datalakes externos con RBAC.

5.2.3. Gestión y Administración

Uno de los principales retos del SASCTI está relacionado con la gestión y administración de cientos de miles de nodos Edge distribuidos a lo largo de las redes de distribución del país.

Esta gestión y administración contempla todas las tareas necesarias para desplegar y posteriormente mantener y actualizar estos nuevos elementos de procesamiento distribuido con el mínimo coste posible de operación y mantenimiento asegurando en todo momento su operación segura y fiable.

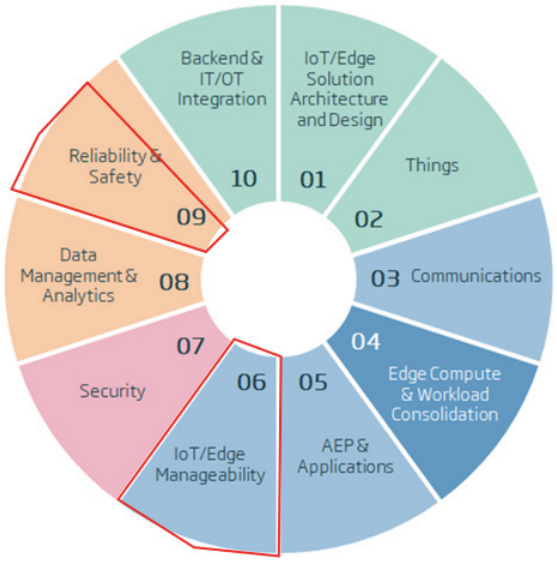


Figura 66: Bloque se requerimientos a abordar por el SASCTI desde el punto de vista de gestión y administración.

Desde el punto de vista de gestión y administración de la arquitectura SASCTI se identifican tres elementos básicos que deberán de estar presentes en cualquier despliegue con el objeto de garantizar su gestión y administración:

1. **Agente Edge.** Responsable de la gestión administración del nodo Edge SASCTI.
2. **Sistema de gestión Edge.** Sistema central que monitoriza, administra y gestiona todo el portfolio desplegado de CTIs.
3. **Orquestador.** Gestor de la ejecución de aplicaciones SASCTI.

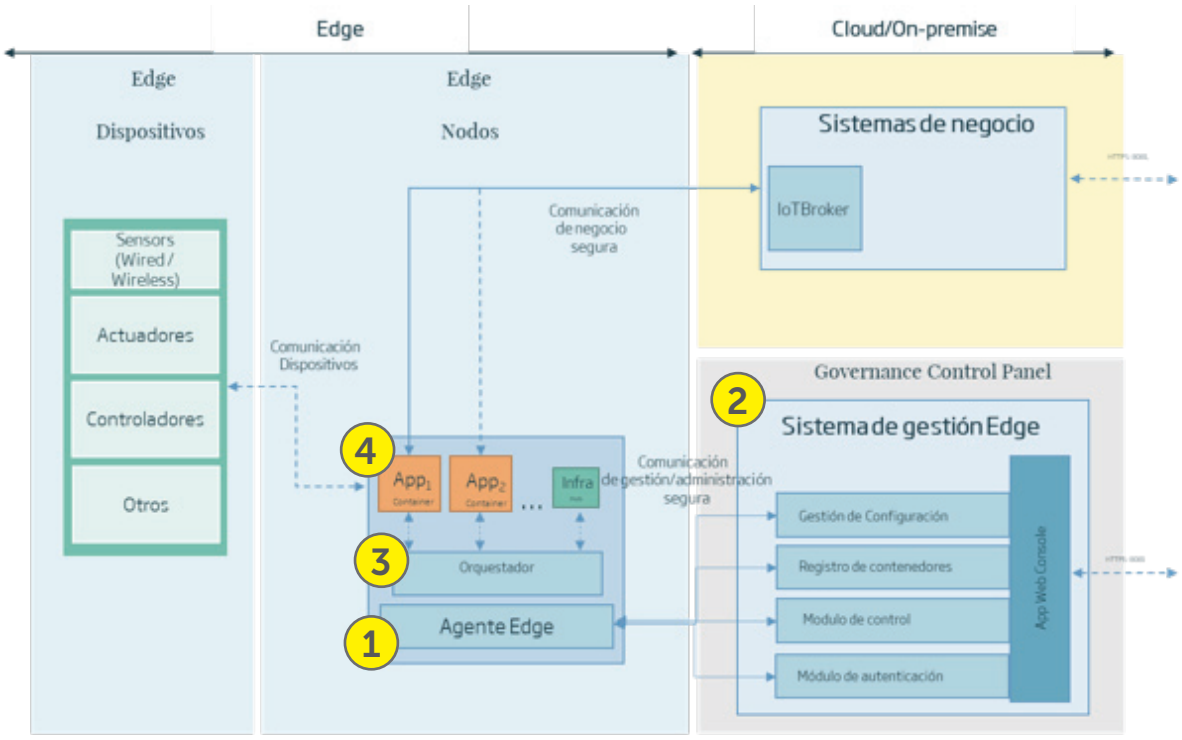


Figura 67: Identificación de componentes involucrados en la administración y gestión del SASCTI.

Se identifican a continuación para cada una de las fases del ciclo de vida del SASCTI los requerimientos básicos a cumplir para garantizar la gestión y administración eficiente de despliegues masivos de SASCTI.

5.2.3.1. Gestión y administración básica en el Edge.

Todos y cada uno de los nodos Edge del SASCTI deben de contar al menos con:

1. **Agente Edge** instalado que esté continuamente en ejecución y que permita:
   a) Autentificar y verificar cualquier acceso a los recursos HW del nodo tanto locales como remotos, rechazando accesos que no estén debidamente autorizados.
   b) Monitorizar el uso de recursos de la infraestructura física del nodo Edge SASCTI: RAM, CPU, almacenamiento y puertos de comunicaciones físicos.
   c) Generación de alarmas y automatización de acciones cuando se alcancen porcentajes determinados de los recursos disponibles o se detecten accesos no autorizados de puertos de comunicaciones.
   d) Comunicación segura con el sistema de gestión central.
   e) Verificación y descarga segura de nuevas versiones de aplicaciones verificadas disponibles en el Gestor Central.
   f) Redireccionamiento seguro a HMI y servicios de configuración y gestión ofrecidos por las aplicaciones.
2. **Orquestador**.
   a) Asignación de recursos a aplicaciones de acuerdo con datos de configuración.
   b) Dar acceso a las aplicaciones a recursos físicos de acuerdo con configuración.
   c) Gestión de configuraciones.
   d) Monitorización del uso de los recursos y funcionamiento de las aplicaciones en ejecución en el nodo.
   e) Control de ejecución de aplicaciones. En caso de caída de aplicaciones o necesidades de recursos cerca del límite asignado, reinicio y reasignación de recursos según configuración.
   f) Gestión y despliegue de nuevas aplicaciones. Confirmación de éxito o fallo de despliegues.

g) Verificación y actualización de nuevas versiones de aplicaciones disponibles en el Gestor Central.

Tanto el agente como el orquestador debe de consumir los mínimos recursos posibles.

5.2.3.2. Gestión y administración central de despliegues SASCTI.

La red de CTIs debe de contar con un sistema central que permita la gestión unificada y remota de despliegues masivos de nodos Edge SASCTI.

Este sistema debe de cumplir los siguientes requerimientos:

a) Gestión del Inventario completo de todos los nodos Edge SASCTI desplegados: parámetros, configuraciones, versiones de SW desplegadas.

b) Gestión agrupada de nodos Edge SASCTI por tipos de SASCTI.

c) Registro de los nodos Edge gestionados por cada uno de los nodos Edge SASCTI. Monitorización y gestión unificada de estado de funcionamiento de los nodos Edge SASCTI con visión general del parque y detalle por instalación: Uso de recursos total, uso de recursos por aplicación desplegada, alarmas y eventos.

d) Acceso a herramientas de administración y gestión de bajo nivel de los nodos y dispositivos que lo habiliten: SSH, portales web de dispositivos...

e) Gestión y registro de aplicaciones desplegados Edge.

f) Entono DevOps para el despliegue y verificación de apps (detalle requerimientos apartado 5.2.3.2.1)

g) Gestión masiva de configuraciones y aplicaciones de forma centralizada sobre familias de nodos Edge SASCTI.

h) Detección automática de anomalías en nodos Edge y soporte a reglas automáticas de reinicio de nodo Edge y contenedores.

5.2.3.2.1. DevOps

El sistema de gestión y administración central, deberá de contar con herramientas que implementen la metodología DevOps con el objetivo de acelerar y optimizar el proceso de desarrollo, validación y despliegue de nuevas funcionalidades en cientos de miles de centros de transformación agrupados en distintas familias de configuraciones.

Para ello el sistema de gestión y administración central de despliegues SASCTI deberá de habilitar un entorno DevOps con las siguientes capacidades:

a) Los equipos responsables del desarrollo de nuevas funcionalidades deben de contar con un **sistema Integración y entrega continuas (CI/CD)** como pueda ser Git/Jenkins que permita construir/modificar, y probar automáticamente nuevas funcionalidades/proyectos para el SASCTI incluido su encapsulamiento en forma de contenedores.

b) **Repositorio de contenedores**

El sistema debe de contar con un repositorio unificado que gestione todas las versiones de contenedores/máquinas virtuales desplegadas en los CTIs. Este repositorio debe de permitir diferenciar los distintos estados de los contenedores: Obsoleto, en pruebas, en producción.

c) El **Repositorio de configuraciones** (Infraestructura como código) almacena los parámetros básicos de configuración y de asignación de recursos del sistema necesarios para las distintas configuraciones de SASCTI. El repositorio debe de permitir gestionar distintas versiones de las configuraciones SASCTI.

d) **Entorno virtual SASCTI de pruebas**

El sistema debe de contar o ser capaz de generar una réplica virtual actualizada de las distintas familias de configuraciones SASCTI.

Estas réplicas deben de incluir la última versión de los contenedores y configuraciones de un entorno SASCTI tipo, así como herramientas que permitan similar las entradas de tal forma que permita verificar el funcionamiento de nuevos contenedores integrado en el ecosistema SASCTI.

5.2.3.2.2. Orquestación SASCTI

La orquestación es la configuración, gestión y coordinación automatizadas de sistemas, aplicaciones y servicios informáticos.

La relación entre virtualización, encapsulamiento y orquestación es muy estrecha. La orquestación se puede utilizar para aprovisionar o implementar servidores, asignar capacidad de almacenamiento, crear máquinas virtuales y administrar redes, entre otras tareas. También se puede utilizar para administrar contenedores, y es donde nos centraremos en los siguientes párrafos, dado que es una tecnología a tener muy en cuenta para su implementación en los SASCTI.

La combinación de muchos microservicios y una mayor frecuencia de publicación se traduce en una mayor cantidad de implementaciones, lo que puede suponer varios retos operativos. Para ello, las prácticas de DevOps como la integración y la entrega continuas se encargan de resolver estos problemas y permitir que se realicen entregas rápidas, seguras y fiables.

Los equipos de TO/TI deben administrar muchos servidores y aplicaciones, pero hacerlo manualmente no es aconsejable especialmente en la arquitectura distribuida del SASCTI con potenciales miles de CTIs a gestionar. Cuanto más complejo sea un sistema más complejo puede resultar la gestión de todas las partes. Aumenta la necesidad de combinar múltiples tareas automatizadas y sus configuraciones en grupos de sistemas o máquinas. Ahí es donde la orquestación puede ayudar.

Para administrar esta funcionalidad encapsulada en microservicios/contenedores, es necesario un buen framework. Los contenedores suelen tener ciclos de vida cortos, y a la hora de hacer una buena orquestación, es necesario tener en cuenta los siguientes aspectos:

- Conectividad de red.
- Alta disponibilidad.
- Facilidad de despliegue.

Tal como se comentó en el apartado 4 de estado del arte, existen diferentes herramientas para realizar una buena orquestación de contenedores.

Corresponderá a cada distribuidora optar por una herramienta u otra, en función de sus necesidades, recursos, sinergias, despliegues realizados hasta el momento, etc.

5.2.3.2.2.1. Resumen requerimientos orquestación

Requerimiento	Al menos uno de esos	Recomendado
Container Runtime	Dockers, Podman, Moby, LXC, CRI-O	
Imágenes de contenedores	Dockers images, OCI	Imágenes Docker
Especificación de despliegue de contenedores	Compose, Kubernetes Especificaciones declarativas basadas en YAML o JSON que sean al menos compatibles con o Kubernetes	Compose YAML
Arquitectura de orquestador	K8s, K3s, Otros orquestadores edge ligeros	
Maesro de orquestación	Openshift, Tanzu, Rancher, Master autogestionado	Master autogestionado (Maduro y con capacidad d customización)

Tabla 4: Resumen requerimientos de orquestación.

5.2.4. Ciberseguridad

Debido a la gran complejidad de los sistemas actuales, y de manera más justificada, en los sistemas distribuidos, se recomienda seguir una metodología de desarrollo segura que nos permita (p.e. SDL[35])

(1) hacer un análisis para identificar los recursos y sus necesidades de interacción,

(2) diseñar el diagrama de flujo de datos,

(3) identificar las amenazas y su mitigación,

(4) su implantación y

(5) su supervisión.

El modelado de amenazas (p.e. STRIDE o DREAD)[36] es un proceso que nos ayuda durante la fase de diseño a elegir qué mecanismos

[35]https://www.microsoft.com/en-us/securityengineering/sdl

[36]https://owasp.org/www-pdf-archive/AdvancedThreatModeling.pdf

deberíamos implantar. En un sistema distribuido; algunos de los mecanismos necesarios para poder implementar una plataforma ciberseguridad son los que se mencionan a continuación.

5.2.4.1. Identidad de dispositivos

En entornos distribuidos, es esencial conocer las identidades de los dispositivos para poder diferenciar los dispositivos legítimos de los ilegítimos dentro de la red. Este es el primer paso antes de conceder acceso a la red, a los datos, a otros dispositivos, etc. Existen diferentes estrategias para controlar estas identidades; entre las más relevantes están las basadas en criptografía simétrica y las arquitecturas PKI (Public Key Infrastructure).

Basado en criptografía simétrica. La criptografía simétrica (misma clave de cifrado y descifrado) es más ligera que la criptografía asimétrica (distinta clave para cifrar y descifrar), y por lo tanto permite un cifrado más rápido. Su principal problema es la gestión de las claves, las cuales deben generarse y distribuirse para cada dispositivo de manera segura.

Arquitecturas PKI. Esta estrategia se basa en el uso de criptografía asimétrica mediante el uso de pares de clave pública y clave privada. En una PKI, cada dispositivo tiene asignada una clave privada (idealmente única) que le identifica dentro de la red. Por otra parte, expone al resto de dispositivos su clave pública, de manera que los dispositivos pueden usar esta clave para cifrar cualquier información para que sea legible únicamente por este dispositivo. De esta manera se puede asegurar la confidencialidad de esta información. Por otra parte, invirtiendo el proceso es posible asegurar la integridad de la información. Esto es posible cifrando la información mediante la clave privada. De esta manera cualquier otro dispositivo es capaz de leer la información enviada usando la clave pública y asegurar que el contenido no ha sido alterado ya que si este no hubiera sido cifrado con la respectiva clave privada no hubiera sido posible descifrarlo.

5.2.4.2. Identidad de clientes

La forma más básica de autenticación es la de solicitar al usuario el nombre y contraseña (Single Factor Authentication), y al ser comprobados correctos por el servidor de autenticación, conceder el acceso al recurso solicitado.

El proceso de comprobar si el usuario y contraseña es correcto, comúnmente lo lleva a cabo un servidor de autenticación. Actualmente hay disponibles soluciones tanto propietarias (Okta[37], WSO2[38]) como Open-Source (Keycloak). Estos servidores, son un punto central de gestión de usuarios, roles, así como de gestión de los permisos de los usuarios dados de alta a los diferentes recursos disponibles. Se despliegan como servidores independientes y son fácilmente integrables por las aplicaciones a securizar (aplicaciones Web, o APIs REST).

Debido a que esta forma de autenticación (par nombre-contraseña) es fácilmente hackeable, en los últimos tiempos se han venido desarrollando procesos y formas de autenticación más robustas, que en vez de solicitar al usuario un único factor (como el par usuario-contraseña), solicitan varios factores adicionales (Multiple Factor Authentication) tales como un código aleatorio temporal (TOTP) que se generan mediante las aplicaciones móviles como FreeOTP[39], Google Authenticator[40] o Authenticator de Microsoft[41] en el propio teléfono móvil del usuario legítimo, o el uso de llaves security keys, como Yubikey[42]. Mediante el uso de MFA, solo si todos los factores son correctos, el usuario tendrá finalmente acceso a los recursos solicitados (en el caso del ejemplo, la aplicación web). De esta manera conseguimos que, mediante la combinación de distintos factores de autenticación, minimizar las intrusiones.

5.2.4.3. Actualizaciones remotas

Tan pronto como se descubre una vulnerabilidad en un dispositivo IoT, o porque se desea añadir nuevas funcionalidades; la actualización de estos dispositivos se convierte en

[37]https://www.okta.com/

[38]https://wso2.com/

[39]https://freeotp.github.io/

[40]https://apps.apple.com/es/app/google-authenticator/id388497605

[41]https://support.microsoft.com/es-es/help/4026727/microsoft-account-how-to-use-the-microsoft-authenticator-app

[42]https://www.yubico.com/?lang=es

un reto debido a su gran cantidad y dispersión geográfica. Por lo tanto, para realizar estas actualizaciones de manera eficiente, es necesario realizarlas de manera automatizada y remota; aprovechando el canal de comunicaciones que se usa para telemetría / control. Pero las actualizaciones remotas (también conocidas como OTA, Over-The-Air), abren una posibilidad a los hackers, ya que les podría permitir violar la integridad de los dispositivos si consiguen que se actualicen con el contenido que ellos deseen. Para ello es esencial garantizar la integridad (p.e. mediante mecanismos de firma digital) y confidencialidad (p.e. mediante encriptado) de la actualización.

Debido a la gran heterogeneidad en los dispositivos IoT (gran variabilidad en los recursos de CPU/Memoria/Red), no existe ninguna solución comercial o estándar de facto reutilizable para realizar esta tarea. Por otro lado, si analizamos la manera de cómo esta implementado en diferentes dispositivos comerciales, todos ellos comparten las siguientes características.

Integridad. Es necesario que el dispositivo que va a realizar la actualización se asegure que lo que va a instalar es de confianza. Para ello, se suele utilizar el mecanismo de firma digital. El dispositivo IoT sale de fábrica con un firmware y el certificado (clave pública del fabricante). Cuando el fabricante quiere distribuir una nueva actualización, la firma con su clave privada y la distribuye. De esta manera los dispositivos son capaces de verificar la procedencia antes de actualizarse. En este caso se recomienda delegar la custodia de la clave privada del fabricante a un HSM (hardware security module).

Para asegurar una integridad completa, se recomienda que tanto la clave de fabricante como el proceso de arranque del dispositivo no sea actualizable en el dispositivo (p.e. en una ROM) para asegurar la cadena de arranque.

Cifrado. En este caso, el cifrado del firmware se realiza ya que su transmisión se suele realizar mediante canales no seguros (redes compartidas, Internet, etc.). De este modo se protege la propiedad intelectual del software (impidiendo su decompilación) y elimina la posibilidad de poder analizar el software el busca de bugs que permitan comprometer los dispositivos.

5.2.4.4. Monitorización del comportamiento

Debido al posible gran número de dispositivos y a su naturaleza distribuida, se convierte en algo necesario poder monitorizar la seguridad de la infraestructura en sí misma. Para poder realizar dicha monitorización, existen los sistemas SIEM. Un SIEM (Security Information and Event Management) es un software que combina las capacidades de un SIM (Security Information Management) y un SEM (Security Event Management). Mediante la adquisición de información, ofrece un servicio de alertas en tiempo real sobre la infraestructura monitorizada. Esta información proviene de diferentes dispositivos de red o equipos con software específico instalado en ellos.

Las principales ventajas de usar un SIEM son por una parte una mejor gestión del tiempo de trabajo del equipo al tener centralizada la información y, por otra parte, una significativa reducción en los tiempos de respuesta frente a incidentes de seguridad. Este segundo aspecto puede suponer una diferencia clave a la hora de evitar un ataque o evitar que se extienda el control del atacante por la red.

Clasificación de SIEMs. Existen múltiples características que diferencian las múltiples soluciones disponibles en el mercado de los SIEM. Cada producto suele caracterizarse por esas diferencias en el servicio y utilidades prestadas. Dentro de las soluciones comerciales existe una evaluación anual sobre el rendimiento de estas. El diagrama Gartner (ver Figura) muestra la posición de las soluciones más relevantes del mercado de los SIEMs comerciales:

Por otra parte, en el Mercado de los SIEM de Código abierto, nos encontramos con un panorama bastante diferente. En este caso si nos ponemos a analizar las estructuras podemos ver que la gran mayoría hacen uso de ELK para tanto el almacenamiento (elastic) como las interfaces (kibana) mostradas en sus soluciones. Las soluciones más utilizadas actualmente son

Figura 68: Gartner de SIEMs.

las siguientes: Wazuh[43], MozDef[44], AlientVault OSSIM[45], SIEMonster[46] y Apache Metron[47].

Debido a esta infraestructura común sus mayores fuerzas y flaquezas residen en la compatibilidad con otras utilidades que les diferencien, así como en las propias capacidades del SIEM.

5.2.5. Sistema Operativo

Con el objeto de cumplir el rango de funciones identificado para el SASCTI, se utilizarán sistemas operativos Linux embebidos con capacidad de gestionar tareas en tiempo real.

La selección de la distribución Linux a emplear debe de ser acorde con los siguientes criterios:

- Sistema operativo de 64 bits
- No utilice mucha memoria, con el objeto de optimizar el aprovechamiento de los recursos HW necesarios en el nodo Edge.
- Posibilidad de asociar tareas a cualquier evento en la capa física del dispositivo Edge.
- Multi-arquitectura capaz de soportar cualquier arquitectura de CPU o al menos las más extendidas (ARM, Intel), con el objeto de asegurar la disponibilidad de un amplio rango de HW edge.
- Predictibilidad en los tiempos de respuesta para eventos.
- Fiabilidad y tolerancia a fallos.

[43]https://wazuh.com/
[44]https://github.com/mozilla/MozDef
[45]https://cybersecurity.att.com/products/ossim
[46]https://siemonster.com/
[47]https://metron.apache.org/

Teniendo en cuenta estos requisitos y la experiencia de los distintos miembros del grupo de trabajo de Futured se recomienda el uso sistemas operativos basados en 64 Linux OS o superiores.

Requerimiento	Al menos uno de esos	Recomendado
Sistema Operativo	64 Linux OS	RHEL
Virtualización	Contenedores/ Pods	Contenedores/ Pods
aBoot Loader	UEFI, BIOS	UEFI (to support secure boot)
Soporte a Tiempo Real	1 ms-10ms o superior con garantía de carga de trabajo determinista,	1ms con garantía de carga de trabajo determinista,

Tabla 5: Resumen requerimientos sistema operativo.

6. METODOLOGÍA DE DEFINICION DE CASOS DE USO E INTEGRACIÓN

En este capítulo se describe la metodología para la elaboración de la especificación técnica del sistema SASCTI inicial, también para incorporar funcionalidades al sistema. El núcleo de la metodología está basado en el estándar IEC 62559 (Use Case Methodology) y los trabajos a nivel europeo (CEN, CENELEC y ETSI) del Expert Group 1 (EG1) dentro del Smart Grid Task Force (SGTF). A ellos nos referenciaremos a lo largo de este capítulo.

El propósito de esta metodología es expresar los requisitos de manera estructurada o formal ayudando a identificar los aspectos clave del diseño la solución y mejorando las comunicaciones con las partes involucradas, que pueden comprender fácilmente cuál es el objetivo de la solución y qué sistemas, dispositivos, aplicaciones y personas participan en ella.

Un Caso de Uso describe las funciones de un sistema de manera neutral respecto a la tecnología. Identifica actores participantes que pueden ser, por ejemplo, otros sistemas o actores humanos que desempeñan un rol en un Caso de Uso. Los Casos de Uso se pueden especificar en diferentes niveles de granularidad. Profundizaremos en esto en las próximas secciones.

Es pertinente en este punto pararnos para situar en el contexto del documento el papel que juega la metodología. En pocas palabras, la metodología de Casos de Uso recoge requisitos básicos del sistema SASCTI (capítulo 5: computación distribuida, gestión, comunicaciones, entorno, etc.) y funcionalidades a implementar sobre el sistema SASCTI (capítulo 7) y describe una forma de cómo generar especificaciones técnicas a partir de estas informaciones de entrada. En este camino, se definirá una Arquitectura de Referencia, un Caso de Uso Base y un método de cómo realizar Casos de Uso (CU) que incorporen funcionalidades al sistema SASCTI (Caso de Uso Funcional, CUF). Todos los Casos de Uso generarán requisitos formales para la selección (o en su caso especificación) de estándares y de rendimiento del sistema (capítulo 4), materia prima de una especificación técnica.

6.1. El proceso

La siguiente figura [69] representa las etapas que se han de cubrir desde la concepción misma del sistema (el SASCTI) hasta la elaboración de la especificación técnica paso previo al desarrollo/fabricación del sistema (software y hardware).

El objetivo de usar esta metodología es, por tanto, generar especificaciones técnicas que

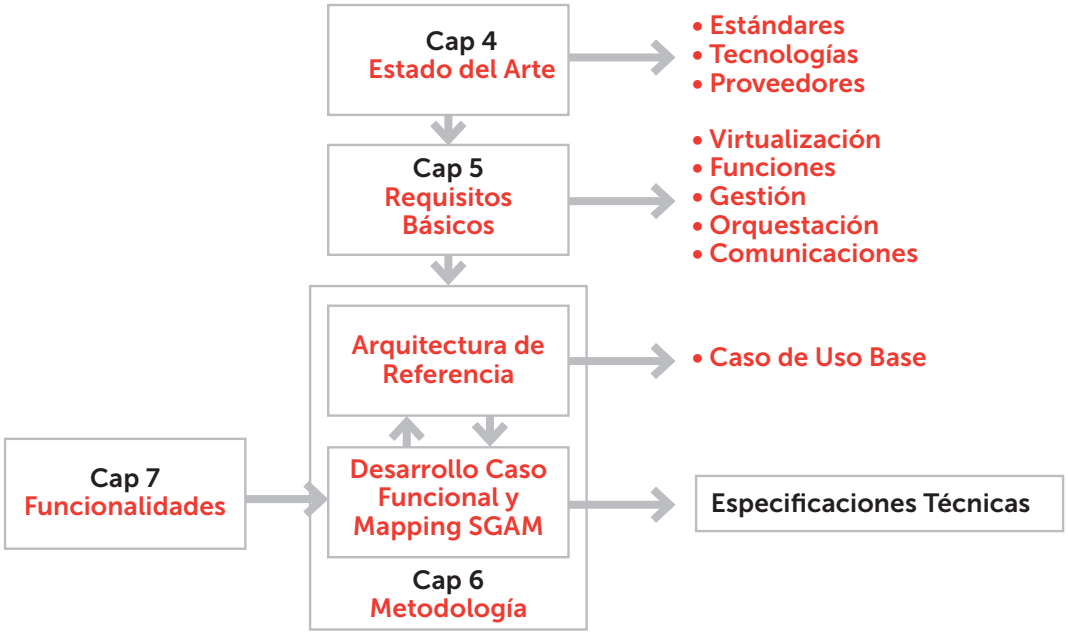


Figura 69: Esquema guía especificación casos de uso.

puedan ser recogidas por los fabricantes. El núcleo de esta metodología es el desarrollo de los Casos de Uso (CUs), de cómo realizar esta actividad se dedicará un capítulo más adelante. Esta metodología se centrará en Casos de Uso orientados a sistemas (el cómo) que no son otra cosa que el paso siguiente a los Casos de Uso orientados a negocio (el qué), se entenderá que esta última actividad es una etapa realizada. Adicionalmente, los requerimientos formales generados por los casos de uso se contrastan con los estándares con el objetivo de ser incluidos en la especificación. Los siguientes puntos describen cada una de las etapas del proceso:

- **Fase 2:** Expertos en el dominio (en nuestro caso, expertos en computación distribuida y en el dominio eléctrico) describen requisitos básicos (capítulo 5 de este documento) derivados del CU de negocio y son los inputs de los CUs de sistemas que hacen un análisis de las funcionalidades. Se desarrollan los CUs de funcionalidades que se quieren implementar, estos CUs generan requisitos más específicos tanto funcionales como de rendimiento (no funcionales).
- **Fase 3**: Los ingenieros de proyectos y los especialistas en TI evalúan la aplicabilidad al proyecto de los estándares, tecnologías

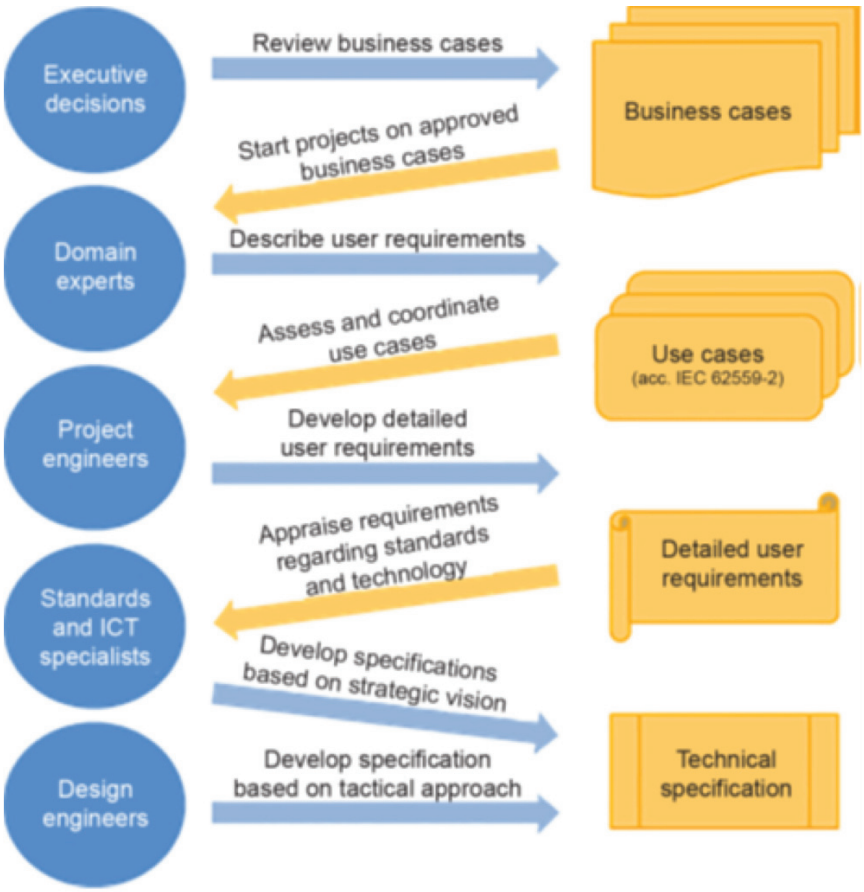


Figura 70: Fases del proceso de especificación técnica (IEC).

- **Fase 1:** Aprobación de los CUs de negocio (el qué, en nuestro caso el sistema SASCTI) que desencadenan el proceso de especificación.

y mejores prácticas. Esta fase coincide con el mapeo del CU en el modelo SGAM para cada uno de los planos de interoperabilidad.

- **Fase 4:** Los ingenieros de diseño desarrollan especificaciones técnicas basadas en la visión estratégica, el enfoque táctico y los estándares

Nos centraremos en estos capítulos dedicados a la metodología en las fases 2 y 3, con especial foco en la primera de ellas en donde se desarrollan los CUs. Estas dos fases las podemos identificar muy bien en la figura [71], en la fase 2 definimos el sistema y sus componentes para desarrollar los CUs que incorporen funcionalidades sobre el sistema definido. El principal objetivo de los CUs es la generación de requisitos formales. En la fase 3 se realiza el mapeo en modelo SGAM y se identifican estándares y tecnologías (por ejemplo, IoT) aplicables, descritas en el capítulo 4 de este documento (Estado del Arte).

sistema multipropósito abierto a la incorporación de nuevos CUs. Para poder representar esta situación nos vamos a apoyar en el concepto Arquitectura de Referencia (desarrollado en la siguiente sección). La Arquitectura de Referencia (AR) es también un Caso de Uso (CU) al que llamaremos "Caso de Uso Base" (CUB). Los CUs que se derivan de las funcionalidades (por ejemplo, el concentrador) se apoyarán en este Caso de Uso Base (en ocasiones llamamos a esto mapeo) y se denominarán Casos de Uso Funcionales (CUF). Observamos aquí una jerarquía en los CUs que representa en la figura.

Esta multiplicidad de CUs relacionados de forma jerárquica hace imprescindible una gestión adecuada del proceso, lo que se detalla en el documento IEC 62559-1:2019 en la referencia

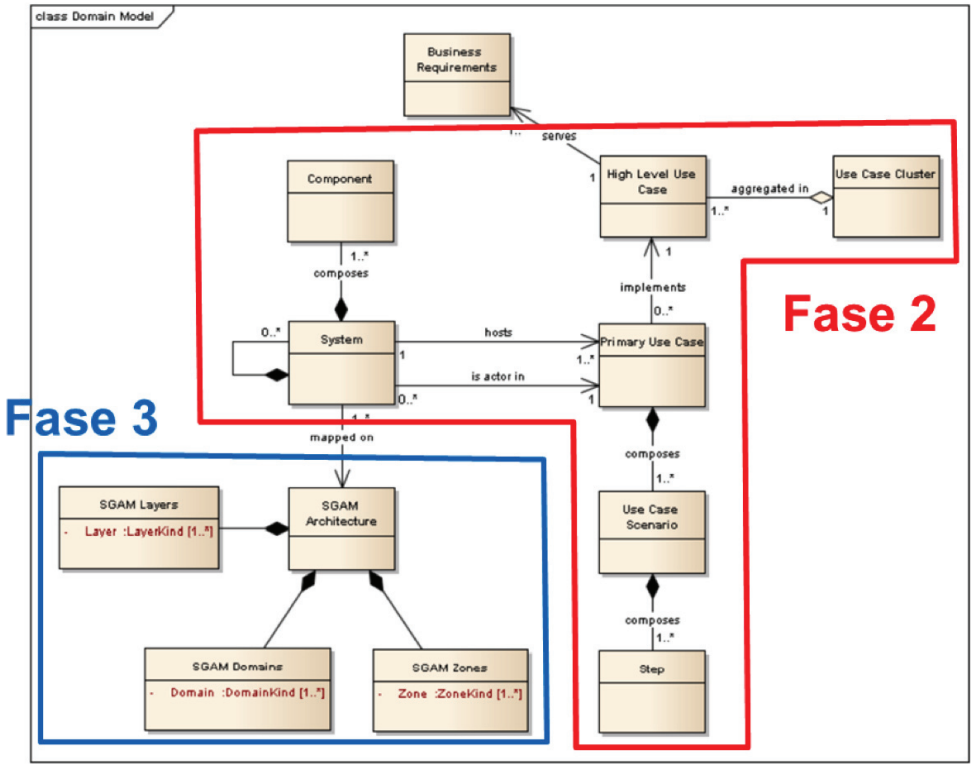


Figura 71: Casos de uso y mapeo en modelo SGAM (CEN-CENELEC-ETSI).

Una de las características básicas del sistema SASCTI es la capacidad de albergar múltiples CUs, aunque no tengan que estar todos desarrollados inicialmente, pues pueden ser incorporados en el futuro. Se trata, pues, de un

[4]. El elemento central de este proceso es el Use Case Management Repository (UCMR). Este proceso nos ayuda a identificar componentes (o funciones) que son utilizados por varios CUs y

por tanto candidatos a ser incorporados a la AR y el CUB. Además, lo veremos en la sección de metodología, nos proporciona un listado de actores, funciones y requisitos que son los elementos básicos para el desarrollo de los CUFs.

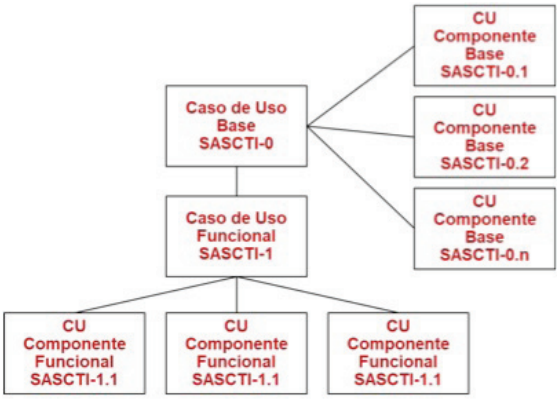


Figura 72: Jerarquía de Casos de Uso.

Los CUs realizados en la fase 2 generan requisitos funcionales y no funcionales. En los primeros, cabe destacar por su importancia los requisitos informacionales, en los cuales se describe la información necesaria que intercambian los diferentes actores para poder realizar una función. En la fase 3 se especifica el modelo de datos, es decir, el modelo semántico que es capaz de cumplir con los requisitos de información.

En el mundo eléctrico existen 3 grandes familias de estándares que especifican los modelos de datos dependiendo de su ubicación en el plano Smart grid (ver modelo SGAM, capítulo 5.1): COSEM, IEC61850 y CIM. En general es buena práctica acudir a estándares del mundo eléctrico, no obstante, y por la naturaleza del sistema SASCTI (no nos olvidemos, hablamos de digitalización de la red eléctrica), en ocasiones es aconsejable acudir a nuevos estándares que se generan en otros ámbitos y que proceden del mundo IT como por ejemplo IoT (o IIoT, o WoT) menos pesados en el desarrollo y con infinidad de productos, librerías y herramientas en el entorno open source. Esto se ve más claramente en los protocolos de comunicaciones y mensajería. Ya no se duda del uso de TCP/IP y de protocolos de

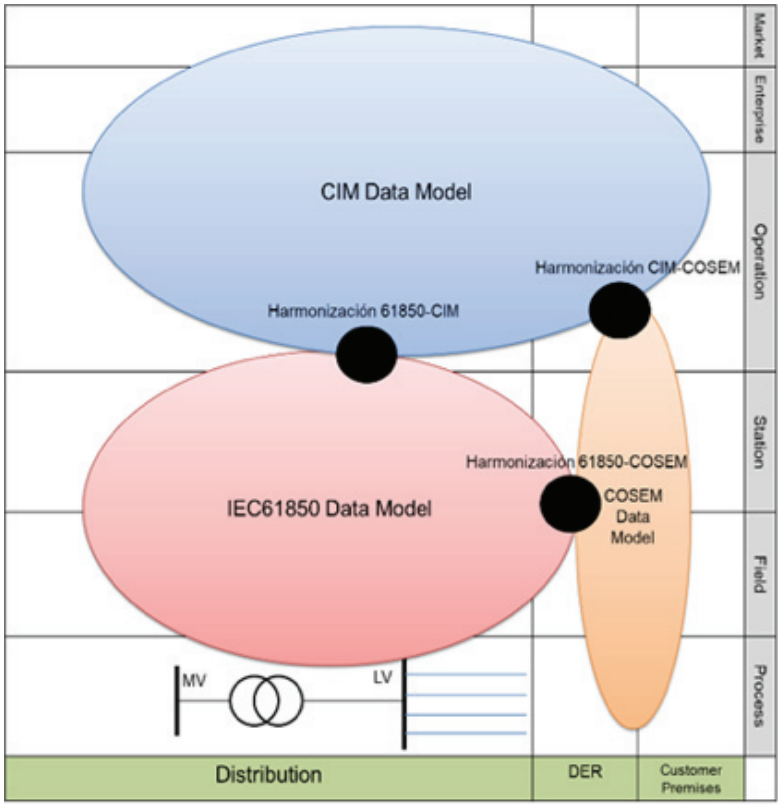


Figura 73: Modelos de datos en el plano Smart Grid.

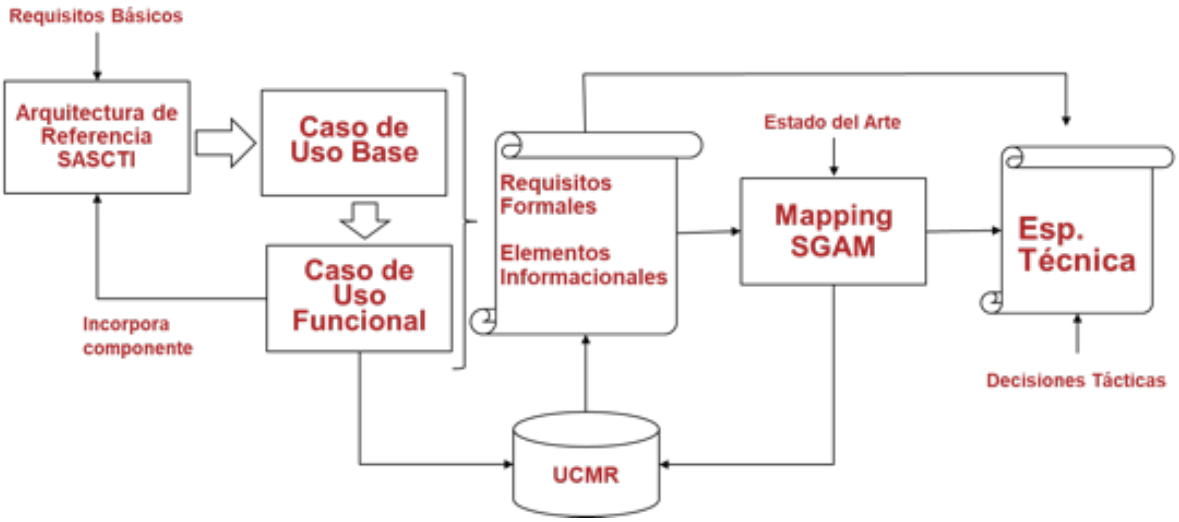


Figura 74: Diagrama del proceso de especificación técnica.

comunicaciones del tipo "pub/sub" como el MQTT, así como el uso de JSON como forma de serializar los datos, estos protocolos son el núcleo de los sistemas IoT.

Para terminar este apartado, se ofrece en el siguiente diagrama el proceso completo de cómo desde unos requisitos básicos alcanzamos una especificación técnica del sistema SASCTI. Las siguientes secciones profundizarán en cada una de las "cajas" de la figura.

6.2. Arquitectura de Referencia (AR)

La Arquitectura de Referencia es la descripción de un sistema con sus tipos de elementos y sus estructuras, así como sus tipos de interacciones entre ellos y el entorno. A través de la abstracción de los detalles individuales, la arquitectura de referencia es universalmente válida dentro de un dominio específico [6]

Dada esta definición, dentro de esta sección desarrollaremos los dos puntos siguientes:

- Definición del sistema SASCTI.
- Especificación de los tipos de elementos y relaciones entre ellos desde un punto de vista Funcional.

6.2.1. Nuestro Sistema: SASCTI

Los principales elementos de la ingeniería de sistemas son el modelado y la descripción de funciones. En sistemas complejos se necesita una representación simplificada del sistema, que sea capaz de describir las partes principales del sistema, sus interacciones y estructura. Un modelo también beneficia enormemente el entendimiento común de todas las partes interesadas. Describir lo que hace el sistema proviene del análisis de las funciones o, como se les suele llamar, los CUs que se contemplan en el diseño del sistema. Además, es necesaria una lista de actores para identificar quién o qué está realizando o utilizando las funciones. Estos elementos - sistema, modelo (arquitectura), CUs y actores - juegan un papel vital [5]. Dado que estos conceptos son muy importantes para el enfoque sistemático, a continuación, se describen con más detalle.

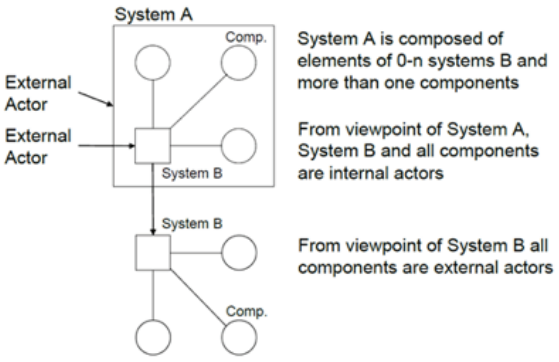


Figura 75: Sistemas, componentes y actores (CEN-CENELEC-ETSI).

Un sistema representa una disposición típica de componentes y sistemas, basada en una arquitectura única, que sirve a un conjunto específico de CUs (en nuestro caso los caos de uso sobre el SASCTI). Es importante señalar que los sistemas pueden estar compuestos de 0 a n sistemas y/o componentes y que los componentes se diferencian de los sistemas por no tener relaciones con actores externos. Todo sistema tiene interacciones con actores

La sección 5 de este documento nos proporciona la información necesaria en forma de requisitos básicos para poder definir el sistema SASCTI:

- Información de tipo arquitectónico.
- información de tipo funcional.
- información de comunicaciones

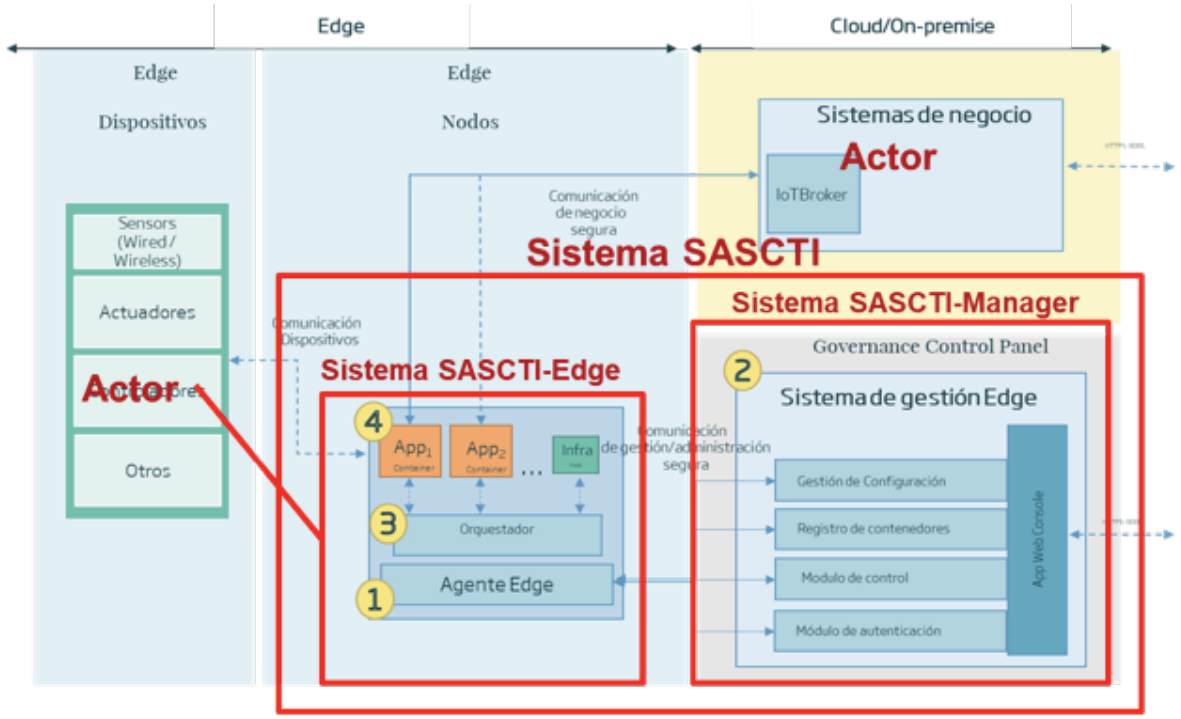


Figura 76: Identificación de sistemas en los requisitos básicos del SASCTI.

externos. Los actores externos también pueden ser del tipo "sistema", es decir, cuando interactúan con otros sistemas. Para fines de modelado, los elementos del sistema pueden aparecer como actores internos del sistema. El diagrama adjunto muestra con más detalle la definición y su uso en el ámbito de las Smart Grids.

Un sistema aloja un conjunto de CUs. Estos CUs describen la interacción dentro del sistema y con actores externos. El sistema es una implementación de un CU primario (en nuestro caso el Caso de Uso Base, CUB). Al mapear el sistema y el conjunto de CUs en el modelo SGAM se puede hacer una investigación de la disponibilidad de estándares para la implementación de del sistema.

Según se ha comentado en el mismo (punto 5.1.2) el sistema SASCTI está compuesto por dos subsistemas:

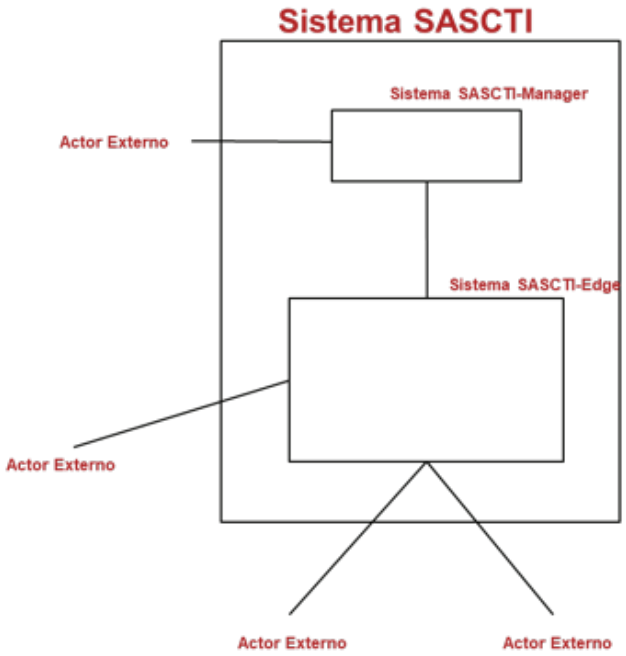


Figura 77: Sistema SASCTI

- Subsistema SASCTI-Manager (SASCTI-M), encargado de las funciones de gestión remota de los sistemas SASCTI-Edge y de las aplicaciones que este alberga. Los roles de los actores relacionados con este subsistema pueden ser diversos, desde operación hasta recogida de información. La ubicación de este subsistema es centralizada y se relaciona (a través del intercambio de información) con el sistema SASCTI-Manager.
- Subsistema SASCTI-Edge (SASCTI-E), encargado de albergar las funciones necesarias para la implementación de los CUs. Los actores en este caso pueden ser dispositivos y otros sistemas accediendo a las funciones (o CU) incorporadas. La ubicación es en el CT y se relaciona con el subsistema SASCTI-M para poder ser gestionado desde un punto central.

Nos centraremos a partir de aquí en el subsistema SASCTI-E, dado que los CUFs se implementan en este subsistema. Para ello, a efectos prácticos, vamos a considerarlo nuestro sistema principal.

En este sistema SASCTI-E distinguimos los siguientes elementos:

- Subsistema SASCTI- Process/Network Manager, cuya misión es proporcionar funciones útiles (mensajería, orquestación, etc) a los componentes de nuestro sistema. Se relaciona con subsistemas y componentes dentro de nuestro sistema. Eventualmente actores externos pueden relacionarse con este subsistema
- Subsistemas SASCTI-Acceso Externo, proporciona funciones para el acceso de actores externos a las funciones proporcionadas por los componentes del sistema.
- Componentes funcionales. Elementos funcionales que conforman los CUs.

La siguiente sección analiza los elementos que componen el sistema SASCTI-E desde un punto funcional y los clasifica para su reutilización en CUs que se analicen sobre el SASCTI

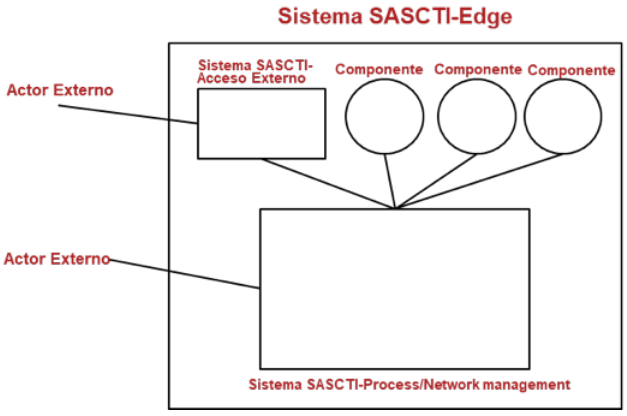


Figura 78: Subsistema SASCTI-Edge.

6.2.2. Elementos y relaciones desde un punto de vista Funcional

Los elementos del sistema (componentes y subsistemas) aportan funcionalidad al sistema SASCTI-E. La figura representa un mapa

funcional del sistema SASCTI-E, las funciones residen en los componentes y subsistemas definidos en la sección anterior. Además, pretende clasificar las distintas funciones de nuestro sistema y establecer una relación entre ellas, la relación es básicamente de visibilidad, es decir, elementos funcionales de capas superiores tienen visibilidad, y por tanto pueden hacer uso de elementos funcionales de capas inferiores.

para los actores o contenedores. Los CUs se plantean desde aquí, por tanto, los contenedores son actores. A nivel de intercambio de información nos ofrece las siguientes funciones de nivel inferior y útiles para el desarrollo de los CUs:

- **Syn Request:** son peticiones de información que hace un contenedor a otro y espera ser contestada en la misma sesión

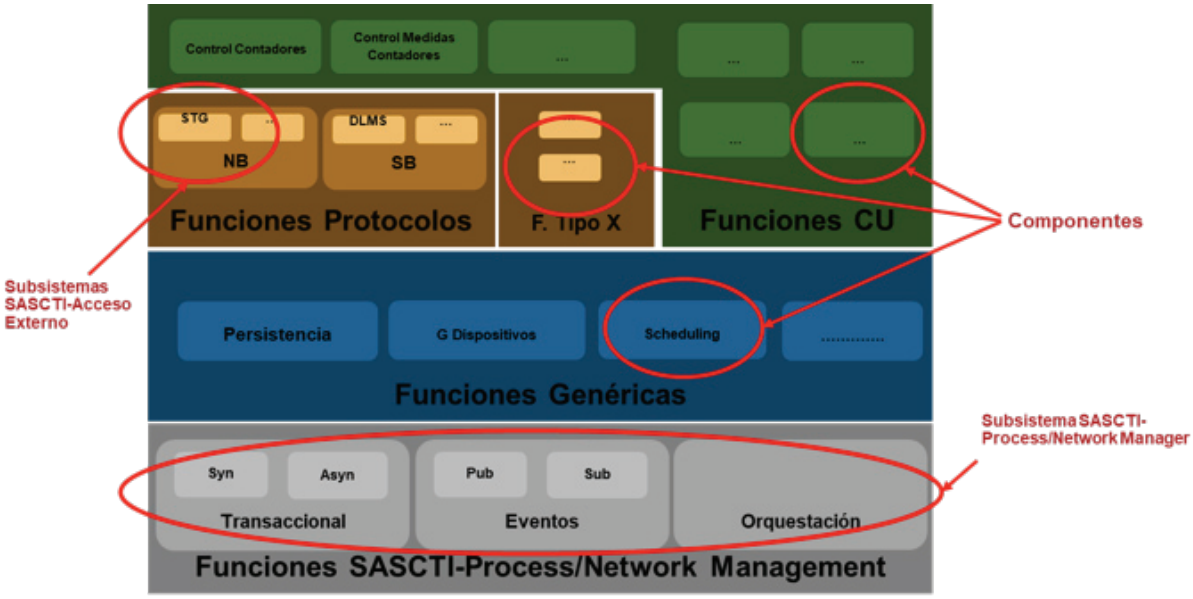


Figura 79: Arquitectura funcional SASCTI.

Si nos posicionamos en la capa inferior "Process/Network management" y miramos hacia arriba lo que vemos son actores aportando funciones. Lo siguiente es una clasificación de estos actores atendiendo al tipo de función que aportan al sistema. Componentes, actores, contenedores o microservicios se emplean en este entorno indistintamente y vienen a representar (en relación con capítulos anteriores), a los elementos funcionales (o componentes) virtualizados en el sistema SASCTI-E.

Destacaremos aquí los siguientes tipos de elementos (componentes/sistemas) atendiendo a la función que aportan:

- **Process/network management SASCTI (sistema):** aquí implementemos el CU, metafóricamente podemos verlo como el terreno de juego donde los actores desarrollan una jugada en forma de CU. Nos aporta las funciones básicas (de infraestructura) (transacción). Tanto la petición como la respuesta está orientada a conexión entre pares.
  - **Asyn Request:** son peticiones de información que hace un contenedor a otro, la respuesta será notificada una vez se realice la petición. La petición está orientada a conexión, la repuesta no.
  - **Pub Event:** son informaciones enviadas a contenedores que se han suscrito y que se derivan de eventos (espontáneos o programados).

Otras funciones más allá del intercambio de información son:

- Monitorización del uso de recursos de la infraestructura física del SASCTI-E.
- Descubrimiento de funciones de otros actores/contenedores.

- Gestión de las configuraciones de los actores/contenedores.
- Gestión de actualizaciones de los actores/contenedores.
- Control de la ejecución de los actores/contenedores.

– Esterotipado de los componentes (o contenedores/microservicios). La figura muestra una posible arquitectura general del componente (según el proyecto RIAPS de Energy Linux Fundation), en este caso la caracterización viene determinada por el módulo "exec". Los caracterizamos por la función que desempeñan dentro del sistema.

los siguientes (seguramente aparecerán más en la elaboración de los CUs y haya que completar este documento):

- Persistencia (SASCTI-CG-Per).
- Gestión de dispositivos (SASCTI-CG-GD).
- Scheduler (SASCTI-CG-Sch).
- Contenedor Funcional (SASCTI-CF). Añade funcionalidades (como se verá será parte fundamental del Caso de Uso Funcional) al Sistema SASCTI haciendo uso de los contenedores de protocolo y genéricos.

Para finalizar este capítulo relacionado con la arquitectura de referencia, el sistema SASCTI-E

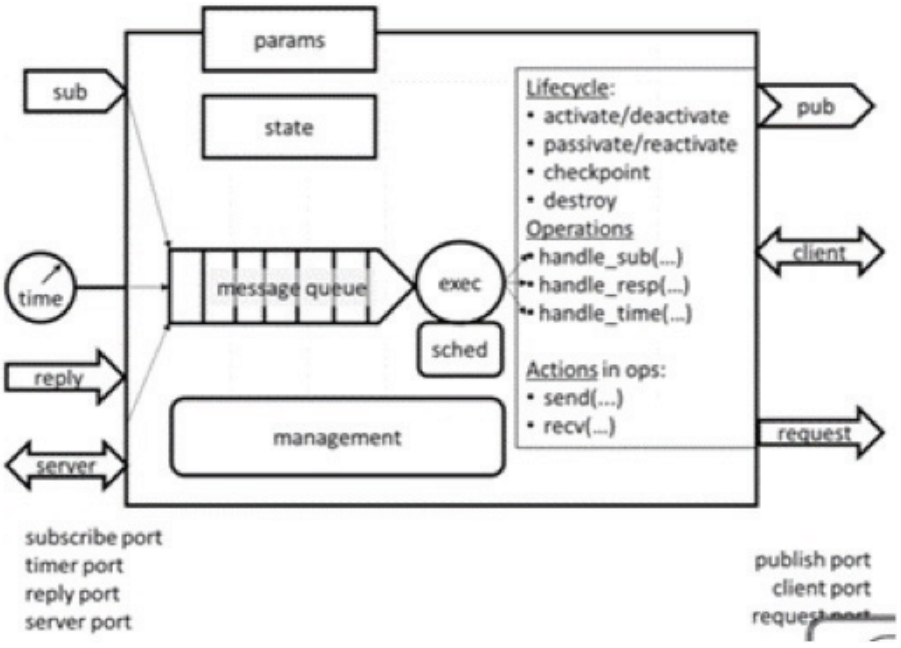


Figura 80: Arquitectura contenedor proyecto RIAPS (Linux Fundation).

- Contenedor de Protocolo (SASCTI-CP). Es la puerta al exterior del Sistema SASCTI. Aquí se realiza el mapeo de funciones y modelos informacionales entre sistemas externos y el SASCTI. Los contenedores de protocolo pueden ser hacia el Centro de Control (NB) o hacia dispositivos (SB).
- Contenedor Genérico (SASCTI-CG). Son funciones comunes a muchos CUs, hasta el momento presente se han identificado

lo representamos a través de un CU que se ha denominado "Caso de Uso Base", este CU será el fundamento arquitectónico para la elaboración de todos los CUs del sistema SASCTI, en ocasiones se llamará "mapeo" el adecuar un CU a la Arquitectura de Referencia.

6.2.3. Caso de Uso Base (CUB)

El CUB representa la Arquitectura de Referencia y nos proporciona una guía para el desarrollo de cualquier Caso de Uso Funcional (que añade funcionalidad adicional al CUB) en el sistema SASCTI. En esta sección se desarrolla el CUB (para más información consultar el CU SASCTI-0 en el repositorio).

Tal y como muestra la figura, el propio sistema, definido en la sección anterior, actúa como actor en el CU y como receptor de las funciones que integran el CU.

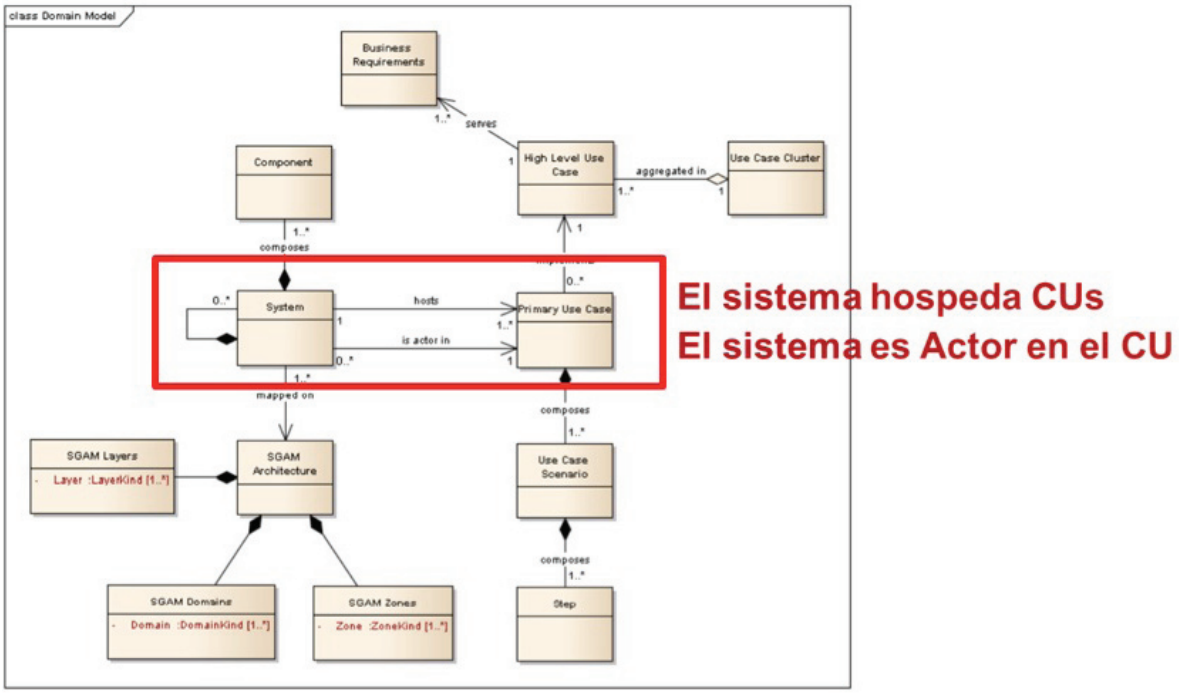


Figura 81: Rol del SASCTI.

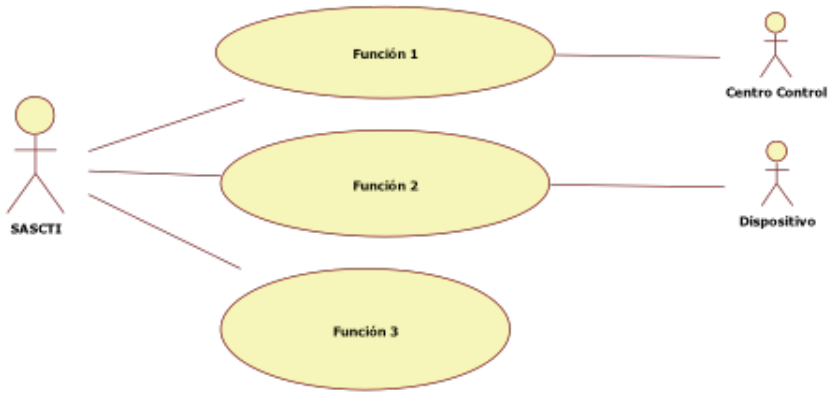


Figura 82: El SASCTI como actor y receptor de funciones.

Esto lo podemos representar de la siguiente forma: el SASCTI se relaciona a través de funciones con otros actores (centro control, dispositivos), otras funciones relacionadas con el SASCTI son internas (en la imagen la función 3). Esta forma de representación general del SASCTI, siendo válida, no nos proporciona visibilidad de la propia estructura del sistema que se ha desarrollado en el capítulo anterior, la Arquitectura de Referencia. En particular será muy útil considerar los componentes y subsistemas internos al SASCTI como los actores en donde se van a depositar los elementos funcionales. Todos menos el subsistema "Process/Network Management" que representa todas aquellas subfunciones que hacen que los contenedores puedan funcionar correctamente: comunicaciones entre ellos, asignación de recursos, etc.

Teniendo en cuenta todo lo anterior, el CUB se representa en la siguiente figura en donde vemos actores añadiendo funciones al subsistema "Process/Network Management". Los CUFs utilizarán las funciones del CUB añadiendo nuevos actores (contenedores o microservicios, SASCTI-X y SASCTI-Y en la figura) que incorporarán nuevas funciones (X, Y en la figura).

6.3. Casos de uso funcionales (CUFs) sobre el sistema SASCTI

La realización de CUFs, ayudarán en el diseño de funciones útilies (funcionalidades, en el capítulo 7 de este documento, entendiendo este término como el conjunto de características que hace que algo sea útil) en el sistema SASCTI. Es parte nuclear de la metodología y como resultado de su realización obtenemos requisitos formales del sistema, así como los elementos informacionales intercambiados. En esta sección se describe cómo realizar el CU de una forma metódica.

Antes, veamos la definición de algunos de los elementos que entran en juego:

- Funciones. Las funciones son acciones del sistema para realizar una funcionalidad (o una parte de esta) y que pueden ser descritas independientemente de los actores, las funciones se describen independientemente de la implementación tecnológica.
- Actores. Los actores interaccionan (se relacionan) con los sistemas desde el exterior de estos. Pueden se roles (ej: operador de la red, planning, personal mantenimiento), sistemas (SASCTI, Scada, DMS, MDM, concentrador, RTU) incluso elementos físicos (ej: sensores, red BT). Los actores se relacionan con los sistemas y dentro de estos con las funciones de diferentes formas, por ejemplo, aportando información, consumiendo

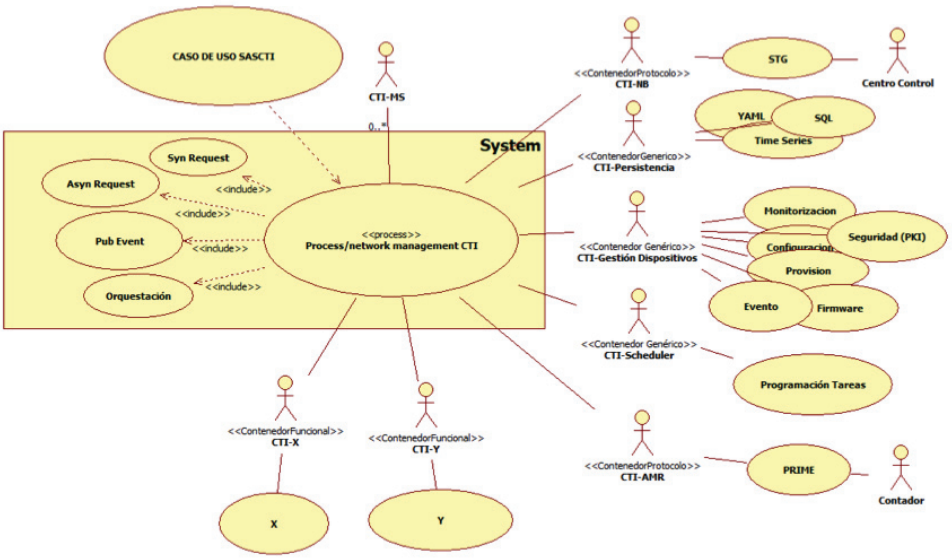


Figura 83: Caso de uso Base.

información, procesando esta información. Lógicamente, el tipo de relación tienen que ver con el tipo de actor.

- Escenarios. Plantean casos concretos de cómo se realiza una o varias funciones en términos de intercambio de información entre los actores involucrados.

Los CUFs son subsidiarios del CUB y heredan de éste funciones y actores, estos últimos solo si son necesarios:

- Actores (contenedores/microservicios) genéricos, como las funciones de persistencia
- Actores de protocolo, para la comunicación con el exterior.
- Sistema process/network management, funciones básicas o de infraestructura del sistema.

Un CUF está orientado al análisis de nuevas funciones que se desea incorporar al sistema SASCTI teniendo en cuenta el CUB y las funciones y actores que este incorpora. Estas nuevas funciones pueden ser incorporadas a uno o más contenedores (como actores) dependiendo del análisis funcional que se realice. Además, algunas de ellas pueden ser incorporadas al CUB si es que encajan dentro de la taxonomía definida en este y el carácter general, es decir, que pueden ser utilizadas en otros CUs.

En general para la realización de los CUs se acude a plantillas donde se representan todos los bloques mediante tablas y gráficos. Existen varias plantillas confeccionadas por organizaciones como EPRI o IEC, todas ellas son similares. En nuestro caso, se ha decidido utilizar la plantilla realizada en el proyecto DISCERN (Distributed Intelligence for Cost-Effective and Reliable Distribution Network Operation, proyecto colaborativo en el ámbito europeo) que puede ser consultada en el Anexo I.

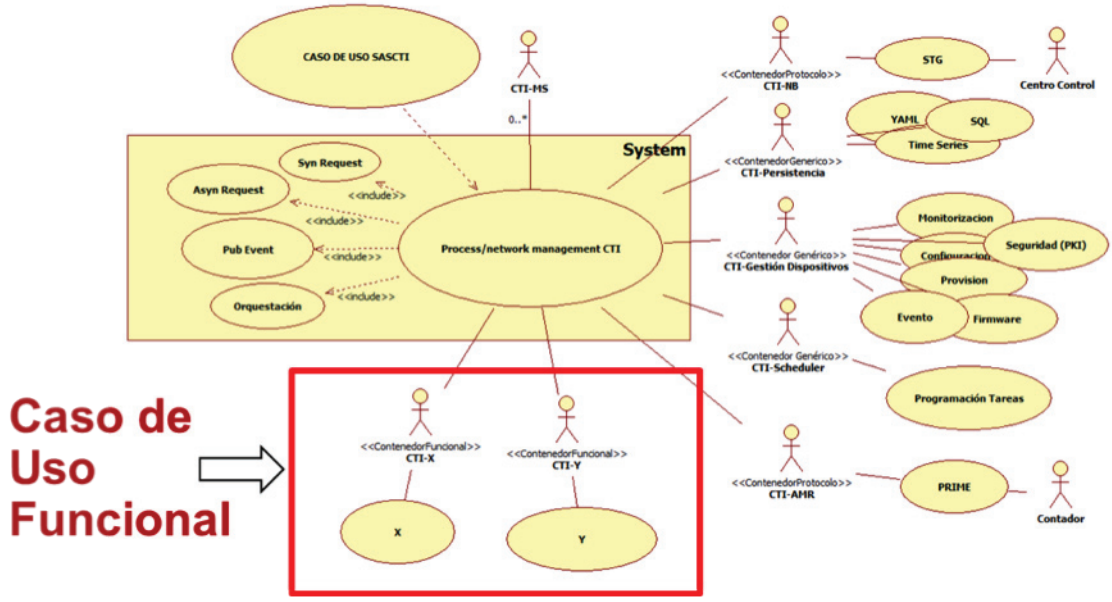


Figura 84: Caso de Uso Funcional.

La figura representa los bloques que comprenden la realización del CU y que forman parte de la plantilla a la que nos hemos referido. Aquí se describen a grandes rasgos estos bloques, si desea más detalles de las secciones y como cumplimentarlas se puede acudir a la referencia [7]:

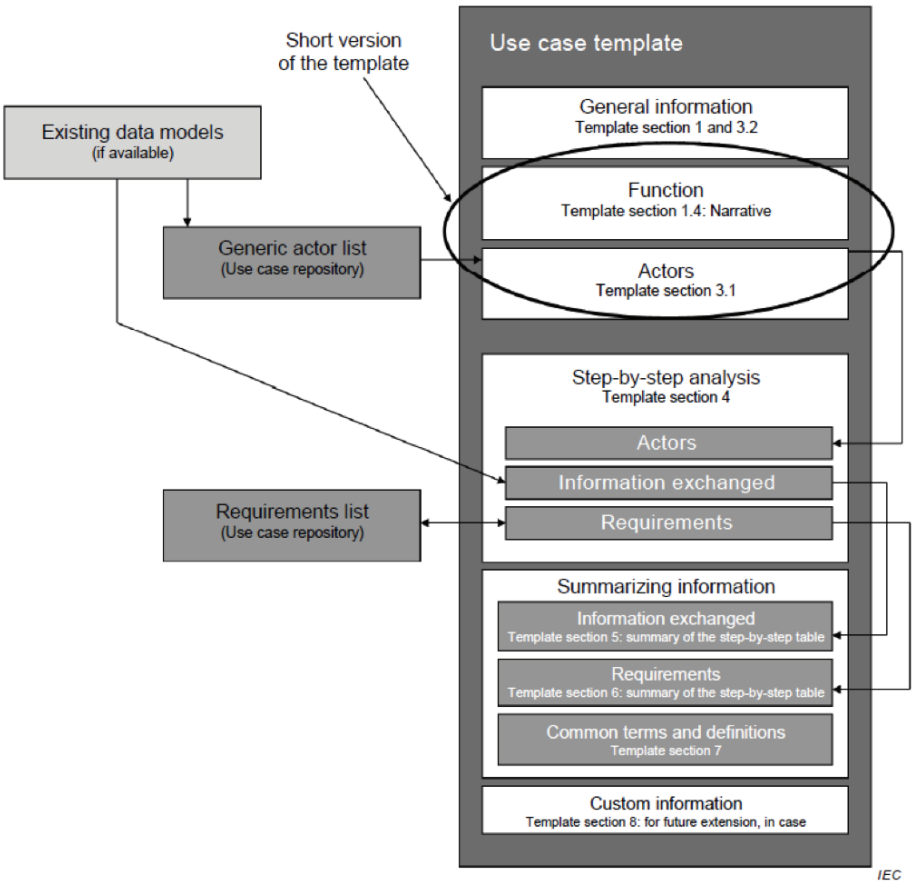


Figura 85: Bloques del Caso de Uso (IEC).

- Información General:
  - o Use Case Identification.
  - o Versionado.
  - o Alcance y objetivos del Caso de Uso.
  - o Descripción corta
  - o Descripción completa
- Actores, listado y características de los actores involucrados en el CU. Importante en este punto incorporar actores del CUB en el caso de que sea necesario (Repositorio de actores del UCMR). Una vez realizado este punto se puede confeccionar el diagrama del CU con los actores, funciones y las relaciones entre ellos. Se detallarán al menos las siguientes características:
  - o Nombre de Actor.
  - o Tipo de Actor.
  - o Descripción.
  - o Agrupación de actores.
- Función, narrativa del CU. Hay que tener muy en mente el CUB que nos aporta funciones. Por ejemplo, la función "Process/ Network Management" heredada del CUB no hace falta describirla se entiende que está incluida, esta concretamente siempre será necesaria.
- Escenarios, en este apartado se listan los escenarios y se desarrollan, es decir se analizan paso a paso con especial interés de ir

rescatando que informaciones se intercambian los actores y los requisitos que debe cumplir el sistema en cada uno de los casos.

En el listado de los escenarios habrá que especificar los siguientes aparados:

- Actor Primario.
- Triggering Event.
- Pre-condición.
- Post-condición.

Los escenarios identificados se desarrollan en tablas donde se analiza cada uno de los pasos del escenario, este análisis se representa frecuentemente a través de diagramas de flujo:

- Nombre de la actividad.
- Descripción de la actividad.
- Evento.
- Servicio (CREATE, GET, SHOW, CHANGE, etc).
- Productor de la información.
- Receptor de la información
- Información intercambiada.
- Requerimientos.

- Listado formal de información intercambiada y requerimientos, se expresan estos conceptos extraídos del apartado anterior de un modo formal, se codifican y son incluidos en el repositorio (UCMR)

La plantilla confeccionada en el proyecto DISCERN contiene algunos apartados adicionales (ver Anexo I) algunos de ellos interesantes dependiendo del CU, no obstante, los descritos aquí son los básicos y por tanto su realización es obligada.

6.4. Mapeo en el Modelo SGAM

El modelo SGAM proporciona una forma coherente y amplia de representar las funcionalidades relacionadas con Smart Grid con un enfoque especial en la interoperabilidad entre sistemas y la identificación de ausencias ("gaps") de estandarización. Es ampliamente adoptado en publicaciones relacionadas con Smart Grid y actividades relacionadas con la estandarización. El mapeo en el modelo SGAM nos permite extraer del CU especificaciones técnicas del sistema SASCTI desde un punto de vista estratégico. Nos permite ubicar en el plano Smart Grid (ver capítulo 5.1) los componentes o elementos físicos, las funciones (asociadas a componentes) y finalmente cómo interaccionan (intercambiando información) las funciones entre ellas, seleccionando para ello modelos de datos y protocolos de comunicaciones que los puedan transportar.

La metodología en esta fase incluye el mapeo del CU en cada una de las capas de interoperabilidad que se definen en el modelo SGAM. En este documento nos basaremos en el documento "Architecture templates and guidelines", entregable 1.3 del proyecto DISCERN

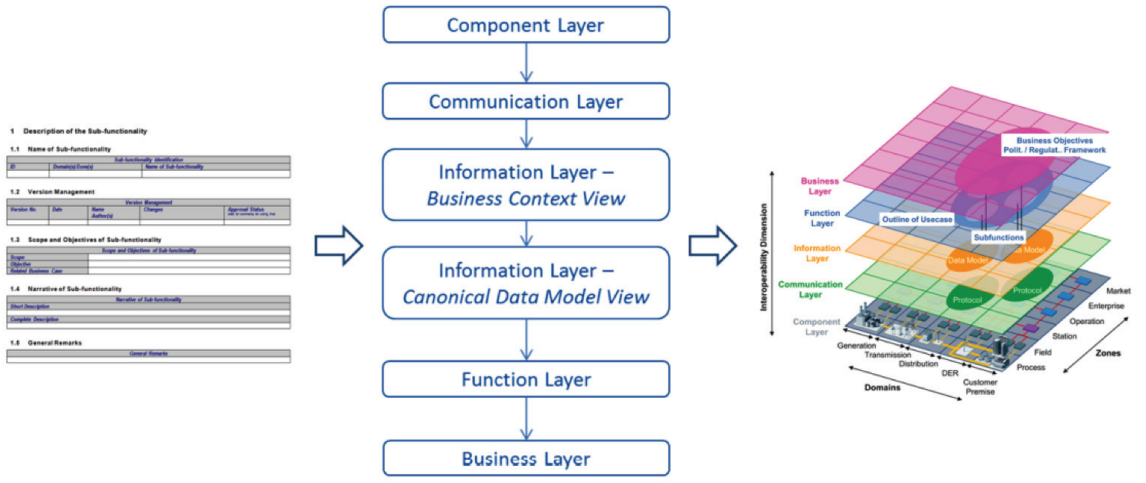


Figura 86: Del Caso de Uso al mapeo en SGAM (DISCERN).

también documento de referencia en la sección anterior [7].

El orden en el cual se realiza el mapeo para cada una de las capas depende de los CUs que se están considerando. El enfoque ascendente (como el de la figura) es adecuado, por ejemplo, si ya se están diseñando nuevos componentes, pero el alcance y caso de negocio o la interacción con otras partes del sistema y las funciones resultantes aún no se conocen ni se especifican por completo. Este es el caso del SASCTI en donde ya desde el inicio, como requisito básico, se está considerando un nuevo dispositivo en los centros de transformación y de lo que se trata es de dotar a este dispositivo de funcionalidad, fundamentalmente por el hecho de estar ubicado en la periferia de los sistemas de la distribuidora cerca de los activos eléctricos.

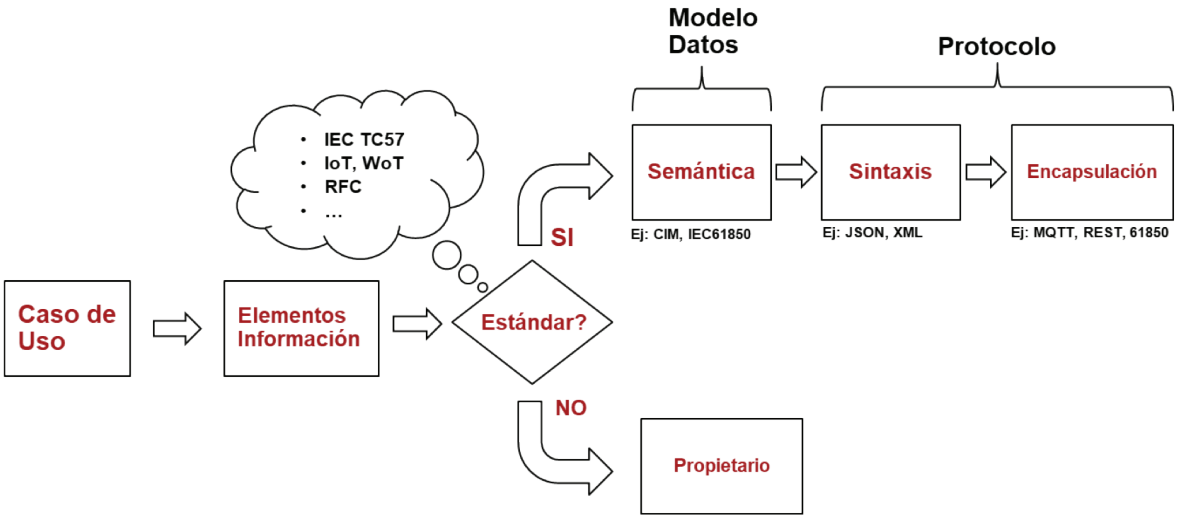


Figura 87: Selección de modelo de datos y protocolo.

En este punto es interesante detenernos brevemente en el concepto de información intercambiada al cual se alude en este capítulo y que era el resultado del análisis realizado en un CU en el bloque de escenarios. En esta fase de mapeo en el modelo SGAM, el objetivo es identificar los estándares más adecuados a los CUs que estamos realizando, es decir, identificar los modelos de datos y los protocolos más adecuados. Para ello nos puede servir como guía los estándares (y arquitecturas) definidos en el IEC TC57 (capítulo 4.6.6.1) (básicamente CIM y IEC61850) y todos los relativos a las tecnologías IoT (capítulo 4.6.7) en sus muchas variantes, novedosas y que impulsan la digitalización a los puntos más remotos de los sistemas. No podemos olvidar que estas tecnologías han proporcionado a los sistemas M2M tradicionales un salto cuantitativo y cualitativo.

A continuación, se describe el mapeo de cada una de las capas de interoperabilidad y como ejemplo en los gráficos se ilustra este mapeo para el CUB descrito en el capítulo anterior:

- **Capa de componentes:** representa la distribución física de todos los componentes participantes en el contexto de un CU. Esto incluye el equipo del sistema de potencia (normalmente localizados a nivel de proceso y de campo), dispositivos de protección y telecontrol, infraestructura de red (conexiones de comunicación alámbricas/inalámbricas, enrutadores, conmutadores, servidores) y cualquier tipo de ordenadores o sistemas computacionales incluida la nube. En la plantilla, la capa de componentes se utiliza como fondo para todas las demás capas, excepto la capa empresarial.

Interesará aquí considerar los contenedores definidos en el CUB como "dispositivos", la razón es poder analizar los elementos informacionales y los estándares que los soportan internos al SASCTI también en el modelo SGAM.

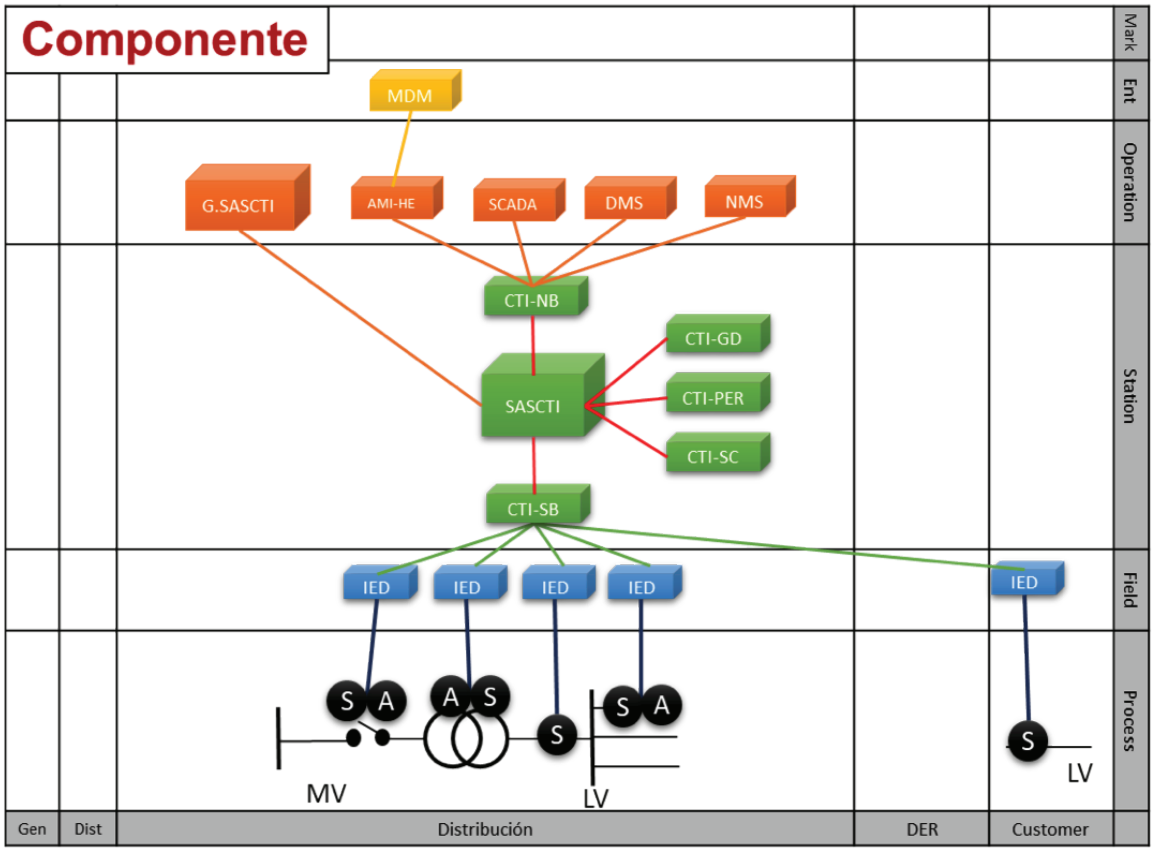


Figura 88: Mapeo capa Componente.

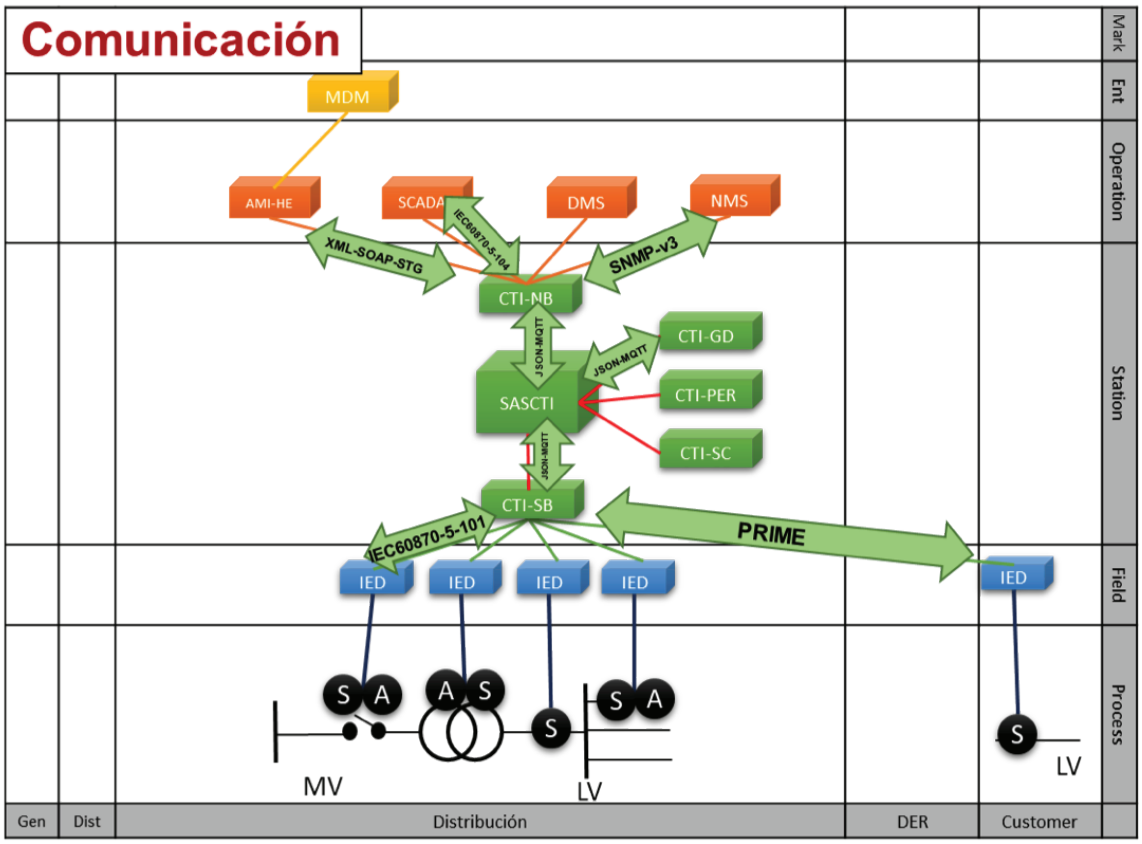


Figura 89: Mapeo capa Comunicación.

- **Capa de comunicación:** la capa de comunicación se utiliza para proporcionar información sobre los protocolos de comunicación empleados para soportar el intercambio de información entre componentes. Representa protocolos y mecanismos para el intercambio interoperable de información entre componentes en el contexto del CU subyacente, función o servicio y objetos de información o modelos de datos.
- **Capa de información - Vista del modelo de datos canónicos:** representa el modelo de datos canónicos estándar que se utiliza para representar los objetos de información en el contexto de un CU. En esta capa se identifican los estándares (si es que existen) que modelan los elementos/objetos informacionales identificados en el CU (en el bloque de escenarios). Aquí aparecen los estándares CIM, IEC61850 y COSEM utilizados ampliamente en el mundo eléctrico. El estándar CIM en concreto admite el uso de subconjuntos (perfiles) y de extensiones en el caso de que algún elemento informacional no pueda ser representado. El IEC TC57 nos proporciona una guía de dónde utilizar estos modelos dependiendo de la ubicación en el plano Smart Grid.

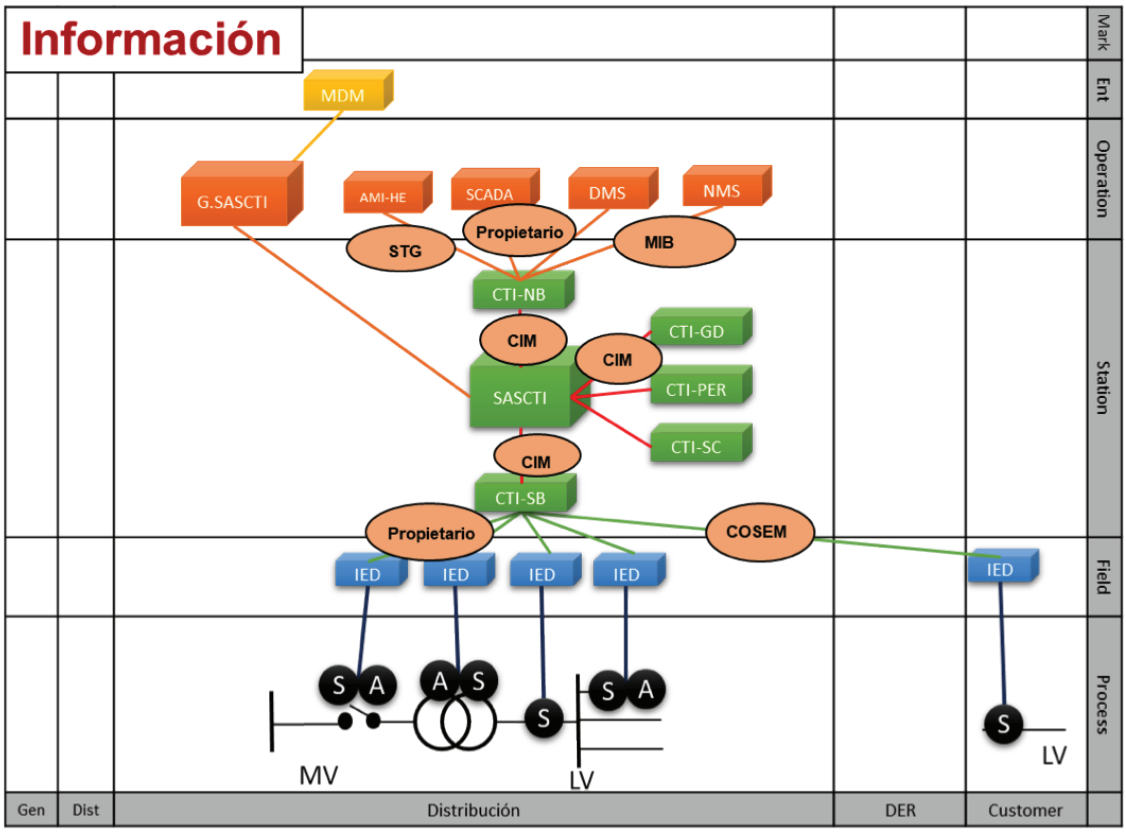


Figura 90: Mapeo capa Información.

- **Capa de información - Vista de contexto empresarial:** representa los objetos de información que se intercambian en el contexto de un CU. Son los elementos/objetos informacionales identificados en el bloque de escenarios del CU mapeados en el modelo SGAM. Esta vista no es imprescindible representarla.

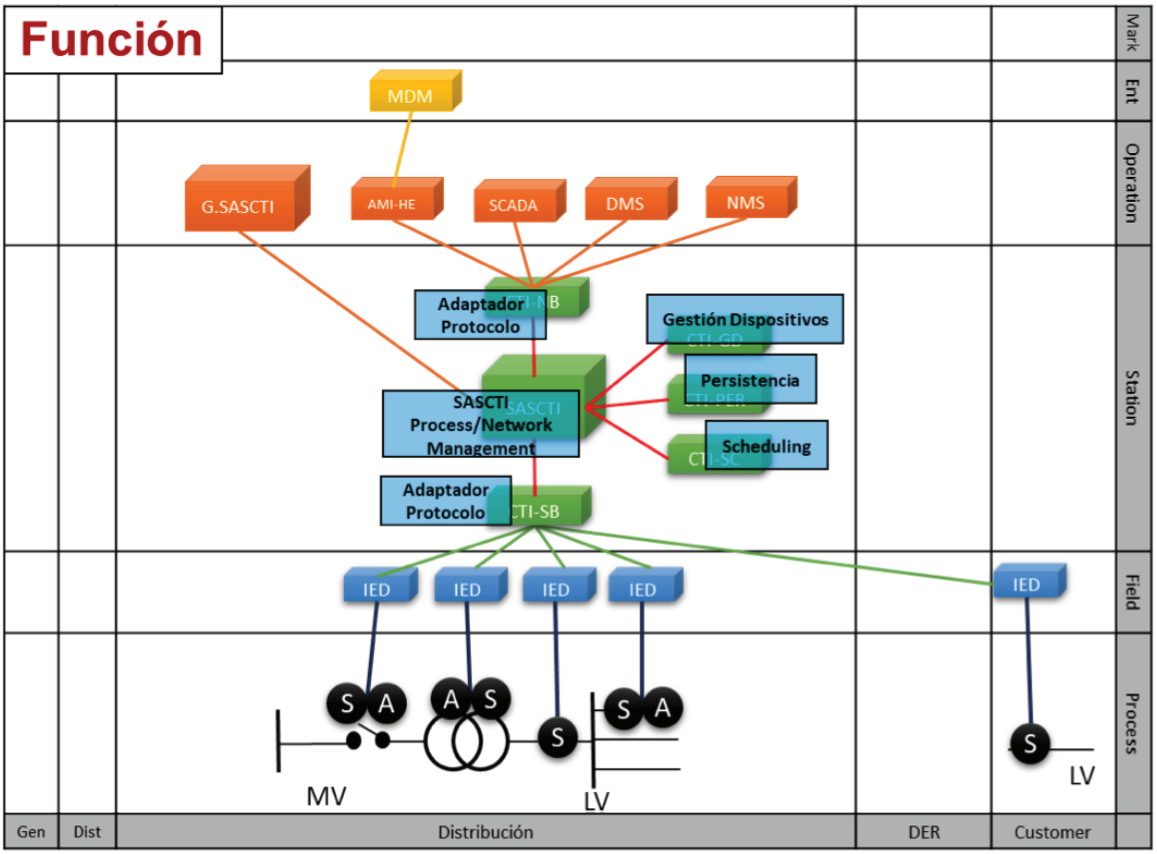


Figura 91: Mapeo capa Función.

- **Capa de función:** representa las funciones que realizan los dispositivos físicos o sistemas de información incluyendo interacciones entre funciones. En la figura se representan las funciones identificadas en el CU base.
- **Capa empresarial:** representa conceptos relacionados con la arquitectura empresarial de un CUF. Esto incluye, por ejemplo, actores, roles, procesos y objetivos en contexto del CU. En este documento no es necesaria.

7. FUNCIONALIDADES

7.1. Introducción

La distribución de energía eléctrica deberá adaptarse al nuevo entorno en constante evolución del sector, que requerirá implementar nuevas funcionalidades que se han identificado inicialmente y que se pretende sea el punto de partida que de visibilidad de las posibilidades que pueden implementarse en este marco de procesamiento distribuido. La creatividad e imaginación de la comunidad de desarrolladores supondrá el único límite real a lo que esta tecnología puede ofrecer.

De esta manera a continuación se enumerarán y se realizará una breve descripción de alto nivel de las posibles y potenciales funcionalidades que o bien ya existen desarrolladas en los CTs actuales y que deberían integrarse en el futuro SASCTI, así como su coexistencia con nuevas funcionalidades que aunque actualmente no estén desplegadas en este entorno de procesamiento distribuido, su incorporación permitirá adaptarse a las nuevas necesidades del proceso de transformación que sufre la sociedad en general y que cada vez afectará más al sector eléctrico, con la integración de:

- Generación distribuida (DER).
- Cargas distribuidas (VE, bombas de calor).
- Almacenamiento distribuido (microredes, agregadores, etc...).
- Mecanismos de flexibilidad distribuida.

Y, cómo no, va a requerir procesamiento distribuido que acerque al origen (redes de BT y clientes) la capacidad de reacción y actuación en casi tiempo real, además estas nuevas funcionalidades aportarán mejoras en mantenimiento predictivo, mejoras en la operación y calidad de suministro, mejora en el uso de los recursos disponibles y extensión de su vida útil, etc.... que proporcionará las herramientas que las distribuidoras requieren para convertirse en DSO.

De esta manera en este capítulo se han agrupado funcionalidades y clasificado según posibles casos de uso comunes:

- Adquisición de datos de los elementos de medida y sensórica (gestión de dispositivos terciarios)
    - **Concentrador de Datos (CD)**
    - **Supervisión Avanzada de Baja Tensión (SABT)**
- **Predicción de red eléctrica:** que será capaz de disponer topológicamente las medidas recibidas (reales) en cada punto de la red y predecir el valor que debería tener los parámetros y puntos no medibles o alcanzables.
- **Gestión de activos:** que mantendrá un inventariado de los activos del CT y aguas abajo en la red de BT, así como el uso que se hace de los mismos, para ser capaz, entre otros, de detectar riesgos por deterioro, pronosticar incidencias y estimar el fin de la vida útil de cada activo tanto digital como físico.
- **Supervisión de Red:** en base a las medidas reales recibidas de todos los elementos de medida y sensores, se mantendrá un resumen de la situación de la red en tiempo cuasi real, que permitirá detectar anomalías y ser notificadas a modo de alarmas.
- **Analítica de Red:** estará compuesto por funcionalidades de analítica avanzada que harán uso de datos históricos almacenados en persistencia que aportará un gran ahorro en uso de ancho de banda y capacidad central de procesamiento.
- **Control de Red:** permitiendo realizar actuación autónoma de los elementos de maniobra disponibles como cambio de toma en transformador OLTC, apertura y cierre de interruptores en el cuadro automatizado, reconectadores, etc. siempre basado en los estados monitorizados por la Supervisión de Red y predicciones de las funcionalidades de Predicción de Red.
- **Gestión de la energía – flexibilidad:** en este apartado se encuentran todas las funcionalidades que permitirán la gestión de la capacidad de la red en cada momento, permitiendo interactuar con consumidores activos sobre los que se permita actuar reduciendo potencia, cortando consumo (mediante gestión de la demanda), admitiendo vertido a la red en los autogeneradores (DER), etc. Permitiendo interactuar con puntos de almacenamiento, agregadores (integradores DER), microredes... de manera

que doten de flexibilidad tanto en el consumo como en la generación distribuida que evitará el sobredimensionamiento del sistema para convertirlo en un sistema energéticamente eficiente.

- **Movilidad, operación y mantenimiento de Red:** que integrará funcionalidades que facilite el reconocimiento local de los dispositivos para confirmar y registrar actuaciones de mantenimiento y operación, no solo de equipos electrónicos, sino de elementos de maniobra no telecontrolados, de manera que queden registrado localmente cada maniobra y se dote al operador de las ayudas necesarias.
- **Ciberseguridad:** contendrá aplicaciones que no solo velarán por el cumplimiento de criterios de ciberseguridad (protocolos seguros, confidencialidad, integridad, disponibilidad, encriptación, etc...) sino que añadirán una capa de procesamiento para evaluar el estado del sistema, detección de anomalías en la ejecución de aplicativos, excesos de consumo (CPU, memoria...) de manera remota y notificarán ante cualquier anomalía detectada.
- **Seguridad y Sostenibilidad:** en esta agrupación se incluyen funcionalidades de control de la seguridad física y ambiental, así como control inteligente de acceso al CT, confirmación de uso de EPIs por el personal que accede al CT... y monitorización ambiental: humos, incendio, fugas, control de puntos calientes, etc...

7.1.1. Metodología de desarrollo de casos de uso

Se entiende funcionalidades como el conjunto de características o funciones que hace que algo sea útil, ese "algo", en el contexto de este documento, es el sistema SASCTI.

La incorporación de funcionalidades al SASCTI generará requisitos y por tanto afectará a la especificación técnica del sistema.

El capítulo 6 de este documento describe la metodología de cómo desde unos requisitos básicos y unas funcionalidades, podemos generar un listado de requisitos formales y, por tanto, unas especificaciones técnicas.

Este capítulo describe las funcionalidades del sistema SASCTI y es un input que junto con el CUB (que representa la AR, es decir los requisitos base, descritos en el capítulo anterior) nos permitirá especificar el SASCTI.

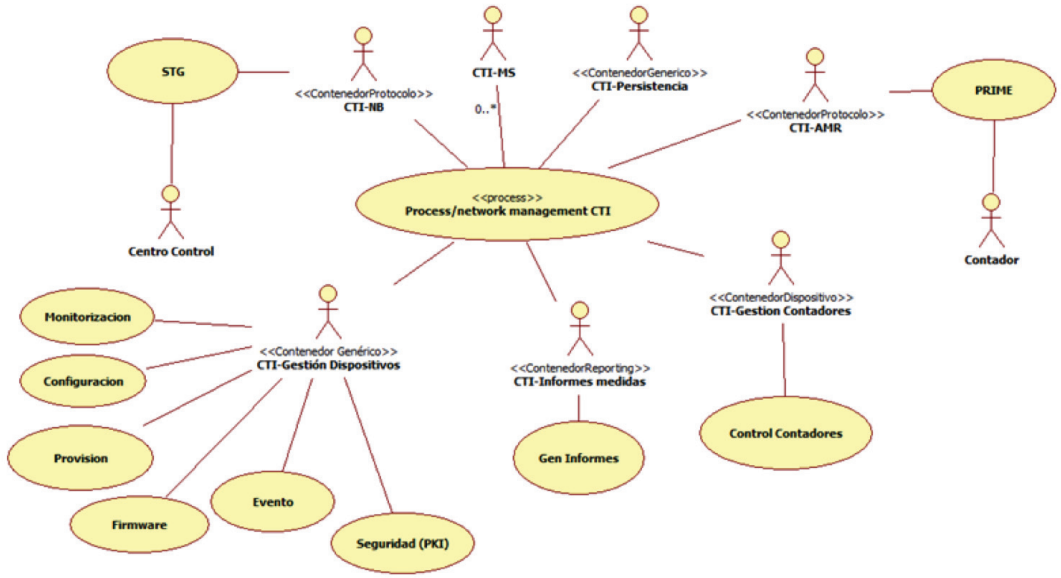


Figura 92: Ejemplo de Caso de Uso Funcional.

Las funcionalidades se analizan en CUFs (capítulo 6.3). Fundamentalmente, se trata de descomponer las funcionalidades en funciones básicas e identificar los actores y las relaciones entre ellos. Todo ello, apoyado en el CUB y las funciones y actores que este aporta. Sirva solo como ejemplo meramente ilustrativo, el gráfico que representa el CUF Concentrador en donde se identifican contenedores de protocolo: STG y DLMS hacia el centro de control y los contadores respectivamente, adicionalmente se identifican contenedores funcionales relacionados con la gestión de contadores y los informes que se generan. El capítulo 6.3 nos describe en detalle cómo realizar esta tarea en forma de plantilla.

Una funcionalidad se puede dividir en varios CUs (como en el caso del concentrador) y son componentes del CU principal como se indicó en el capítulo de metodología, esto en general es una buena práctica y nos ayudará a identificar componentes de uso general que se pueden elevar al CUB.

Cada uno de los CUFs derivados de una funcionalidad se mapean en el modelo SGAM (capítulo 6.4) y todo ello se registra en el repositorio UCMR

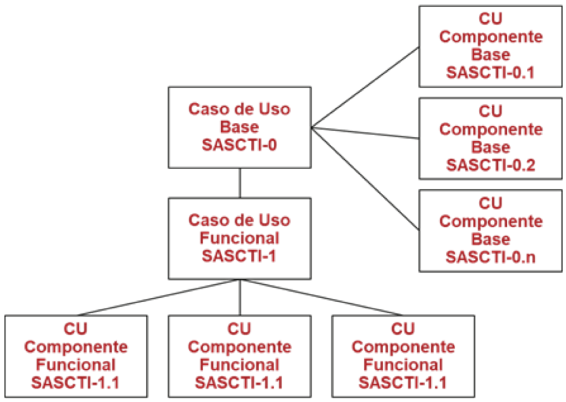


Figura 93: Jerarquía Casos de Uso Funcionales.

7.2. Concentrador de datos

Esta funcionalidad se ha reconocido como parte fundamental del sistema y, la que ha ayudado a definir una primera aproximación al CUB, sobre el que el resto de funcionalidades podrán hacer uso y solicitar sus servicios. Se entiende que es fundamental para el SASCTI establecer una metodología para la adquisición de datos de los diferentes dispositivos de medida y sensórica, y en el caso del Concentrador de Datos (CD) se requerirá de una Gestión de Dispositivos (Contadores Inteligentes = CNs), sobre los que se solicitarán datos y se registrarán en informes funcionales, mediante un acceso ordenado y periódico que será controlado por un gestor de tareas (Scheduler), esos datos adquiridos serán almacenados en una base de datos de persistencia en el propio sistema y/o serán enviados a un sistemas central.

En el SASCTI coexistirán otras aplicaciones o funcionalidades, unas que requerirán de los datos adquiridos y almacenados por el CD, para realizar diferentes procesos analíticos (datos históricos de la base de datos de persistencia) y otras que demandarán datos instantáneos para lo que solicitarán al módulo correspondiente del CD (gestión de informes + gestión de dispositivos) y por esa razón el CD se concibe como una descomposición de diferentes funcionalidades o módulos que formarán parte del CUB y serán reutilizadas por otras funcionalidades como la que se describe en el siguiente punto (Supervisión Avanzada de BT), que comparte misma filosofía y concepto de adquisición de datos de manera periódica o a demanda, almacenando o enviando esos datos y gestionando dispositivos terciarios que contiene la sensórica. Cada uno de los módulos que compone el CD se especificará como CU independiente: Gestión de informes, Gestión de dispositivos (CNs), Gestión de tareas (Scheduler), Persistencia y Protocolos de comunicaciones: Northbound (STG-CD) y Southbound (DLMS-COSEM sobre PRIME).

La función principal del concentrador de datos es realizar interrogaciones periódicas a los equipos de medida (CNs) que se encuentran conectados en el mismo SASCTI. Los datos obtenidos de los equipos de medida tanto por interrogantes como la obtenida a través de los

eventos espontáneos, se almacenan en persistencia para que pueda ser enviados al sistema de gestión remoto o consumidos por otra funcionalidad. Se distinguen diferentes modos de acceso a los datos y su adquisición, dependiendo el uso que tengan:

- **Acceso asíncrono:** se realiza mediante tareas periódicas o a demanda y los datos son enviados a repositorios históricos que alimentan a funcionalidades o casos de uso que no requieran monitorización o acción en tiempo real.
- **Acceso síncrono:** se realiza mediante petición a demanda de datos o medidas instantáneas que deben devolverse directamente al sistema o función que lo consume. Este tipo de acceso es utilizado por funcionalidades o casos de uso que requieran monitorización para actuación en tiempo real.
- **Eventos:** se distinguirán entre espontáneos que serán enviados inmediatamente tras su generación por los elementos de medida (CNs) y deberán ser notificados de manera síncrona al sistema central o funcionalidades de monitorización de eventos en tiempo real. O también eventos NO espontáneos que se van almacenando en el histórico de los dispositivos y podrán ser adquiridos de manera asíncrona.

Las actividades que debe llevar a cabo el concentrador de datos relacionadas con la red de baja tensión son:

- Gestión de equipos de medida (estados, lecturas y configuración de CNs).
- Gestión de estrategia de adquisición de datos y construcción de informes funcionales.
- Almacenamiento o envío de los informes al sistema o aplicación que lo requiera.

Para poder realizar estas actividades, el CD debe contar con las siguientes funcionalidades:

- Verificación de conexión y sincronización (gestión de estados de CNs).
  - o Comisionado y securización comunicación del CN.
  - o Detección de fase de contador.
  - o Autodescubrimiento de CNs.
  - o Registro y control de topología.
- Inventariado y configuración de parametrización de CNs.
  - o Lectura/configuración de parámetros de CNs.
  - o Actualización de firmware de CNs.
- Programación de tarifas y potencias contratada.
- Adquisición de valores instantáneos de medida: medios, máximos, mínimos.
- Adquisición de registros para facturación.
  - o Generación de fichero de curva de medida.
  - o Generación de fichero de curva de carga.
  - o Generación de fichero de resúmenes diarios y cierres mensuales.
  - o Generación de ficheros con potencias contratadas.
- Monitorización de eventos espontáneos.
- Generación de informes predefinidos y/o definidos a medida con datos obtenidos de los CNs (el supervisor de secundario de trafo se considera como CN trifásico)

7.3. Supervisión Avanzada de Baja Tensión

La Supervisión Avanzada de Baja Tensión (SABT) se encarga de realizar la supervisión y monitorización desagregada de las líneas a la salida de los cuadros de BT (CBTs) así como de la medida en la entrada de cada CBT y de su corriente de fugas a tierra; permitiendo obtener información en tiempo real del estado de la red eléctrica, detección de incidencias de calidad de suministro, detección de fugas a tierra, detección de conectividad de los suministros y detección de fraudes.

La supervisión avanzada de Baja Tensión incluirá la posibilidad de operar interruptores en las salidas de BT, en tiempo real. En aquellos casos en los que la protección de las salidas de BT del cuadro se realice con interruptor automático, en lugar del fusible (nombraremos iCBT), los datos colectados por la supervisión avanzada permitirán operar este elemento sin intervención desde un centro de control.

Se diferencian, por lo tanto, dos tipos de funcionalidades. Aquellas en las que no es necesaria una información de la BT en tiempo real, (Telegestión, balances, fraude, información de calidad de red para mantenimiento predictivo) y aquellas en las que es necesaria una información de la BT en tiempo real, para mantenimiento correctivo y operación.

La remota de SABT se encarga de recoger los datos provenientes de las tarjetas (considerados como dispositivos terciarios a gestionar por este módulo) a través del protocolo DLMS/COSEM sobre HDLC o Ethernet. Estos dispositivos también almacenan estos datos en persistencia del propio equipo y/o los envía mediante Web Services y/o ficheros. A continuación, se describen algunas de sus funcionalidades:

- La RTU SABT proporciona las siguientes alarmas por salida y fase:
  - Fusible fundido.
  - Sobrecargas.
  - Sobretensión, Tensión mínima.
  - Desequilibrio de cargas entre fases.
  - Dirección de la corriente.
- Entre otras funcionalidades, la SABT gestionará la monitorización y supervisión de cada secundario de transformador y/o entrada de cada CBT realizando la siguiente medición de parámetros de calidad:
  - Frecuencia industrial.
  - Amplitud de tensión y Flicker.
  - Desequilibrio de la tensión de suministro.
  - Armónicos de tensión.
  - Variaciones rápidas de tensión.
  - Eventos de calidad de suministro. Por ejemplo: interrupciones, sobretenciones temporales y huecos de tensión.
  - Monitorización ante anomalías: Oscilografías.

Al igual que el concentrador y como se ha comentado, comparten funcionalidades comunes que se definirán en CUB como:

- **Gestión de dispositivos:** en el caso de SABT gestionará tarjetas de medida en cada línea, que a todas formas serán gestionados de la misma manera que los CNs por el concentrador (reutilizará mismo módulo descrito en CUB).
- **Gestión de tareas periódicas:** compartirán el módulo Scheduler donde se programarán las acciones periódicas (colecta de datos de tarjetas, medidas en la entrada CBT y fugas a tierra) así como otras acciones de gestión de los dispositivos (sincronización, eventos, estados, etc.).
- **Gestión de informes:** modulo que se encargará de construir informes bien predefinidos o a medida, a modo de funcionalidades que responderá a la demanda del gestor de tareas, del sistema central u otro aplicativo/funcionalidad interna al SASCTI.
- **Gestión de las comunicaciones**: compartirá mismo módulo de comunicación con el sistema central de telegestión (STG) que el CD y atenderá a peticiones del sistema central. Y establecerá la comunicación con los dispositivos mediante mismo intérprete de protocolo DLMS (comunicación DLMS sobre HDLC o Ethernet) que el CD.

7.4. Predicción de red eléctrica

Inicialmente se dispondrá de una primera aproximación topológica de la red de BT (Grafo Topológico), con formato normalizado tipo CIM o modelo que se defina, basada en los datos de inventario de elementos disponible en el GIS de cada distribuidora, estableciendo las relaciones padre-hijo entre cada elemento, de manera que será posible disponer de un diagrama de árbol tipo grafo, con la topología de la red de BT, recogiendo cada elemento y sus relaciones sin necesidad de disponer de coordenadas geográficas pero si datos de longitud, tipo de cable, etc..., como ejemplo: posición de trafo – secundario de trafo – CBT – LBT – segmento – CGP – CN..., que se considerará como información de partida, siendo las funciones que a continuación se describen las responsables de enriquecer y corregir con datos de medidas reales y estimaciones de cada punto o elemento de la red, dando posibilidad de detección de anomalías.

Los algoritmos normalmente utilizados para la predicción se basan en modelos de Machine Learning que, en este caso al permitir ejecutar-

se de manera local, habilita a los dispositivos no solo reaccionar en tiempo casi real sino también ir aprendiendo patrones para tomar decisiones más inteligentes en el futuro.

7.4.1. Simulación flujos de carga y estimación de estados

Las redes de baja tensión están adquiriendo una mayor relevancia progresivamente debido a la proactividad que el consumidor puede tener en dichas redes mediante el uso de DERs (fotovoltaica, baterías, vehículo eléctrico, etc.)

Los algoritmos de flujo de carga (Power Flow) son esenciales en estas redes para así conocer el efecto en la calidad de suministro que estos DERs pueden provocar: sobre o subtensiones, sobrecargas ciertas secciones de cable, desbalanceos entre fases, etc. Uno de los algoritmos más usado es el método de Netwon-Raphson, ejecutándose en este caso para redes no equilibradas.

Para ejecutar estos algoritmos, es necesario conocer una serie de características y datos de la red de distribución de baja tensión:

- Tensiones en bornas de baja tensión del centro de transformación.
- Consumos de cada uno de los puntos de suministro
- Localización (terminal y fase en la que está conectado el punto de suministro)
- Topología de la red de baja tensión: tipo de cable, longitudes, localización, etc. (Grafo topológico)

Tanto las tensiones del transformador como los consumos de cada punto de suministro provienen del concentrador a través de tareas de colecta de valores instantáneos.

Como resultado de la ejecución de este algoritmo, se conocerán las tensiones teóricas que cada terminal ha de tener, así como la saturación de los cables y otros parámetros como ángulo de la tensión respecto a la intensidad, consumo a través del punto frontera, etc.

Estos resultados pueden alimentar a otra serie de algoritmos como localización de fraude, optimización de las cargas de la red de baja tensión, cálculo de pérdidas técnicas, etc.

Será necesario diferenciar entre la información BT que se necesita para los flujos de carga, (no en tiempo real y destinada al sistema de telegestión de contadores) de aquella información de BT necesaria en tiempo real para la operación BT.

Como alternativa o complemento a los Flujos de Carga (FC) se podría utilizar la Estimación de Estado (EE) siempre que exista una redundancia en la medida adecuada en la red de BT.

Un EE se encarga de determinar a partir del conjunto de estados, topología y medidas disponibles cuales son los que definen el estado de la red más probable y eléctricamente correcto (modelado eléctrico de componentes y leyes eléctricas) en cada instante (ver referencia [32]). La EE permitiría tener en cuenta la incertidumbre de medida de los sensores y detectar errores de medida de los mismos mediante la aplicación de una metodología estadística (a diferencia del enfoque determinístico/probabilístico de los FC). El problema del FC es obtener las tensiones en todos los nudos y flujos de potencia por todos los elementos, sin embargo, la EE admite todo tipo de medidas, tanto presentes (con más dificultades para obtener) como futuras, en proceso de definición sobre las nuevas versiones de contadores.

Para obtener mejores resultados tanto en la predicción de la EE como los FC, serán necesario también tener en cuenta y disponer de datos y parámetros no eléctricos como: temperatura, laboralidad, insolación, movilidad eléctrica, eventos especiales. La detección y control de situaciones especiales por CT es fundamental: ferias, fiestas, eventos sociales, suministros significativos...

7.4.2. Balances de pérdidas técnicas y no técnicas

Toda red de baja tensión asociada a un centro de transformación en un momento dado tiene una serie de parámetros que la hace singular frente al conjunto de todas las demás. Sin duda el reparto de sus suministros, las secciones y longitudes de sus conductores las hacen únicas.

Teniendo los datos de la topología de la red de BT y las medidas horarias de todos los suministros del centro de transformación por medio del concentrador, o a través de los equipos no telegestionados, se podría realizar el cálculo de las pérdidas técnicas teóricas de la red de BT asociada a un centro de transformación en función de las distintas curvas de consumo que pueden darse cada hora entre los n suministros asociados.

En la diferencia existente entre el sumatorio desde los consumos de cliente medidos y las pérdidas técnicas calculadas para cada una de las redes en cada uno de los momentos, se obtendría la base de referencia que debe compararse con las medidas del SABT y así determinar la existencia o no de pérdidas no técnicas, cuantificarlo tanto en % como en kWh incluso extraer los patrones de consumo de dichas pérdidas no técnicas que facilitarían su búsqueda.

Adicionalmente, conociendo el consumo en cada una de las líneas de salida del cuadro de baja tensión a través del SABT mediante sus informes de curva de carga total y por fases por cada línea del CBT, además del consumo de los contadores en cada línea a través de su correspondiente curva de carga (colectada con periodicidad diaria y con periodo de integración actual de 1 hora), se puede determinar tanto el % o la energía en kWh perdida en cada una de las líneas de baja tensión, así como las horas en las que se produce dicho fraude y aproximar el valor, útil para la campaña de eliminación de fraude en campo.

7.4.3. Saturación del transformador

Con respecto a la saturación del transformador (considerado como un índice de la medida de salud del transformador y no el concepto de saturación del núcleo magnético) debemos de verlo con una doble temporalidad, la inmediatez y la analítica para el cálculo de envejecimiento.

Como datos necesarios de entrada al algoritmo de cálculo de saturación de transformador se requerirán idealmente la Intensidad de las salidas de BT, tensión, potencias (en VAs), temperatura del aceite del transformador, humedad y temperatura del ambiente (si hay estación metereológica) o del propio transformador. Con estas medidas y disponiendo de los datos y características del transformador , será capaz de calcular el estado de saturación, permitiendo activar una alarma notificando al sistema central correspondiente cuando se sobrepase un umbral establecido, durante un cierto tiempo establecido.

Teniendo en cuenta tanto el histórico de maniobras (cambios de tomas), alarmas de saturación y los históricos de la sensórica, se podrá calcular el envejecimiento equivalente (por días), que usará el módulo de gestión de activos.

Esta monitorización no eliminaría el sistema de protección actual, en el que la sonda se lleva a la bobina de disparo del ruptofusible.

7.4.4. Análisis de capacidad de red

Detección y cálculos de los límites de la red basados en las condiciones de operación:

- Control de tensión. Disponible para control de tomas del transformador (previsión de tensiones fuera de límites).
- Control de capacidad. Disponible para control de sobrecarga a nivel de cabecera de LBT (previsión de sobrecargas).
- Funciones avanzadas: restricciones en segmentos aguas abajo de la red de BT. Necesidad de disponibilidad de datos topológicos y flujo de cargas.

7.4.5. Mapa de tensiones

Disponer de un mapa de tensiones no es un caso de uso en sí mismo, sino una herramienta que será utilizada por otras funcionalidades, como la regulación de transformador, cálculo de toma óptima, el simulador de flujos de carga o estimador de estados, algoritmos de detección de anomalías, de detección de fraude y de localización de ruidos PRIME, etc.

Esta funcionalidad se encargará de mantener actualizado y enriquecer el grafo topológico con los últimos valores de tensiones medidos en cada elemento de la red con sensórica y un histórico de valores anteriores.

7.4.6. Equilibrado de fases en una línea de BT

El equilibrado de fases es una de las funcionalidades necesarias para la mejora de la eficiencia en la gestión de la red de BT, ahorrando

pérdidas y disminuyendo la saturación, mediante el equilibrado de las fases de cada línea de BT.

El objetivo inicial es generar un informe de desequilibrios a nivel de LBT y CT siguiendo estos pasos:

- Garantizar la disponibilidad de los datos de tensiones e intensidades por fase de la SABT y la puesta en servicio de la conectividad por línea y fase para garantizar la fiabilidad del grafo topológico.
- Utilizar los datos de red históricos para identificar situaciones de la red de BT con una explotación alejada del óptimo por encima de un umbral de equilibrado de las cargas.

El objetivo es la mejora de la protección del conductor de neutro, la caída de tensión en las líneas de BT, las pérdidas técnicas y/o del nivel de saturación en las líneas de baja tensión (LBT) que tengan sus fases desequilibradas por encima de un umbral, que justifique la intervención. La información necesaria proviene de la telegestión, de la supervisión avanzada, junto con los datos técnicos y de inventario de la línea, como el grado de saturación y las pérdidas en valor absoluto relacionadas con la energía y la longitud de la línea.

Un sistema de equilibrado de mayor eficacia sería el equilibrado en tiempo real si se dispusiera de una capacidad de conmutar cargas entre las fases de una LBT.

Se identificarán en el grafo topológico los elementos que se han detectado con desequilibrios, que serán enviados al sistema central, al igual que eventos o alarmas cuando se superen los umbrales máximos de desequilibrio definidos durante los tiempos definidos.

7.5. Gestión de activos

En un negocio regulado, donde cada vez es más importante disponer información de todos sus activos así como la maximización de su vida útil, la gestión de activos supone uno de los puntos clave, que redundará en una mejora en su mantenimiento y reducción de costes operacionales.

Uno de los principales retos en el CT, es la sensorización de los activos físicos a partir de los activos digitales, de manera que se disponga de un control e histórico de todos los parámetros medibles, información que alimentará a procesos analíticos avanzados, que aportarán predicción de averías y capacidad de reacción para lograr la máxima disponibilidad en la red.

7.5.1. Inventariado y estimación de vida útil

En el CT ya se dispone de activos digitales que aportan medidas, tales como el concentrador de datos que monitoriza las variables eléctricas en el secundario de cada transformador , o la SABT que supervisa la entrada y salidas de línea de cada CBT. Además de otras nuevas sensóricas que permitirán monitorizar variables ambientales y de activos físicos como el transformador (presión, temperatura, nivel de aceite, control de toma, etc..). Si además la distribuidora es capaz de registrar las operaciones manuales realizadas en la red (conteo de maniobras realizadas) así como relacionarlos con los parámetros suministrados por el fabricante de cada activo, toda esta información es muy útil para estimar el envejecimiento de cada elemento de la red.

Del mismo modo que se trata la "saturación del transformador " donde una de sus salidas es el envejecimiento o vida útil remanente, el caso de interruptores debería abordarse de un mismo modo, con la complicidad de los fabricantes de los interruptores que deberían aportar su propio criterio y algoritmo de cálculo de "vida útil de interruptor" basado en datos de maniobras realizadas, así como medidas de la intensidad que estaba pasando en el caso de apertura y cierre, además de consultar el DPF para consultar la Icc en el caso de estar activo. Otros datos de interés deben ser la temperatura y humedad ambiente.

El problema principal para esta gestión radica en disponer el control de las maniobras realizadas de un modo manual, con lo que la gestión de operación (apartado movilidad, operación y mantenimiento de la red) es un punto muy relevante que debe tenerse en cuenta.

7.5.2. Autodiagnóstico

En este escenario, cada aplicación distribuida se debería poder considerar como activo digital, así como el resto de activos digitales,

de manera que existe la necesidad de monitorización y confirmación de estado de vida (KeepAlive) de todos estos activos.

De cara al correcto funcionamiento de un sistema tan complejo como el SASCTI, surge la necesidad de plantear un componente que valide a todos los bloques funcionales. Para ello, la arquitectura definida deberá contar con un módulo de autodiagnóstico, capaz de gestionar el control de todos los test funcionales. Este módulo de autodiagnóstico deberá verificar que su funcionamiento es correcto en los siguientes casos:

- En el arranque del equipo.
- Bajo demanda de petición.
- Bloque funcional no responde a través del bus.
- Instalación de un bloque funcional.

A tales efectos, todos los despliegues funcionales de software deben tener estandarizados los siguientes servicios:

- Reboot {start | stop}.
  - o Respuesta: OK, Error - Log.
- Autodiagnosis.
  - o Respuesta: OK, Error – Log.

Una vez validadas todas las funcionalidades, este módulo ha de ser el encargado de dar el "OK" al arranque del equipo, o enviar las órdenes de reinicio a los distintos módulos. Asimismo, contará con la capacidad de enviar logs con los fallos localizados. Para ello, deberá contar las funcionalidades denominadas "reboot module" y "notify error".

En el caso de recibir arranques con error, deberá notificar a los sistemas de gestión central de la red Edge los errores encontrados a través de "notifyerror" y deberá aplicar la siguiente política para el rearranque:

- Reinicio del bloque funcional: N intentos (parametrizable) en base al servicio "autodiagnosis".
- Reinicio de comunicaciones internas: En caso de que el log reportado fuera asociado al bus de comunicaciones.
- Reinicio de comunicaciones upstream: En caso de que se detectasen errores en el envío de datos hacia el exterior del nodo.
- Reinicio del nodo Edge: En caso de que el comportamiento de arranque o verificación fuera errático.

7.5.3. Reinício remoto equipos

Aumento de disponibilidad de equipos digitales, por medio de la consulta periódica al router y remotas, realizando reseteo selectivo de los mismos en el caso que su funcionamiento esté comprometido. Se mantendrá una monitorización de disponibilidad y rendimiento de todos los activos digitales.

Entre los fallos principales existentes en la telemetría de los equipos o en la telegestión de los mismos están las indisponibilidades de los principales equipos que aportan valor en dicha digitalización, siendo el reinicio siempre una de las principales acciones que recuperan a los equipos del estado de bloqueo.

Por un lado, está la remota (RTU) que digitaliza las señales o viceversa para hacer de traductor entre el mundo analógico y el mundo digital. Sin su traducción sería complicado tener los datos de campo de un modo remoto ni poder realizar las operaciones oportunas.

Por otro lado, estaría el módulo de comunicaciones (ej. Router) que transfiere información bidireccionalmente con el punto remoto.

Cuando uno de estos equipos se perturba en su funcionamiento y deja de hacer sus funciones se hace necesario reiniciar dichos equipos como primera medida para corregir dicho mal funcionamiento.

Para dicho reinicio existen diversas estrategias:

- Mandar operarios a reiniciar (mayor coste operativo y en tiempo de indisponibilidad).
- Programar reinicios periódicos automáticos (barato y solo aumenta la disponibilidad en caso de problemas discretos y prolongados en el tiempo), son proactivos y no resuelven todos los tipos de bloqueos.
- Visualizar alarmas y reinicio remoto. Útil para el caso de reiniciar la RTU y complicado en el caso de fallo de router salvo que se disponga de segundo canal de comunicación.

El nodo SASCTI podría localmente monitorizar el correcto funcionamiento de cada uno

de los equipos, con las consultas que fuesen oportunas para comprobar los tiempos de respuesta o la coherencia de las mismas y por medio de la Fuente de alimentación aplicando órdenes de reinicio de los equipos concretos, reiniciando selectivamente los distintos equipos o el reinicio no selectivo de la totalidad de los equipos conectados a DC.

Igualmente, la estrategia puede ser reinicios programados recurrentemente.

Se garantizará que el reinicio en cualquier componente del sistema no suponga en ningún caso la apertura intempestiva de interruptores automáticos de BT, el cambio de tomas en la regulación del transformador en su caso, ni de cualquier elemento que afecte a la calidad del suministro.

7.6. Supervisión de Red

En base a las medidas reales recibidas de todos los elementos de medida y sensores de los activos digitales, se mantendrá un resumen de la situación de la red de forma conjunta en tiempo cuasi real, que permitirá detectar anomalías y ser notificadas a modo de alarmas

7.6.1. Detección anomalías BT

7.6.1.1. Localización averías BT

El control del CT analizará la información de la SABT y de la Telegestión del CT para la localización de la avería, inclusive, para algunos casos, contrastar la información que gestionan ambos tipos de equipos: supervisor básico (conectado al secundario del transformador) y supervisor avanzado (conectado a la entrada

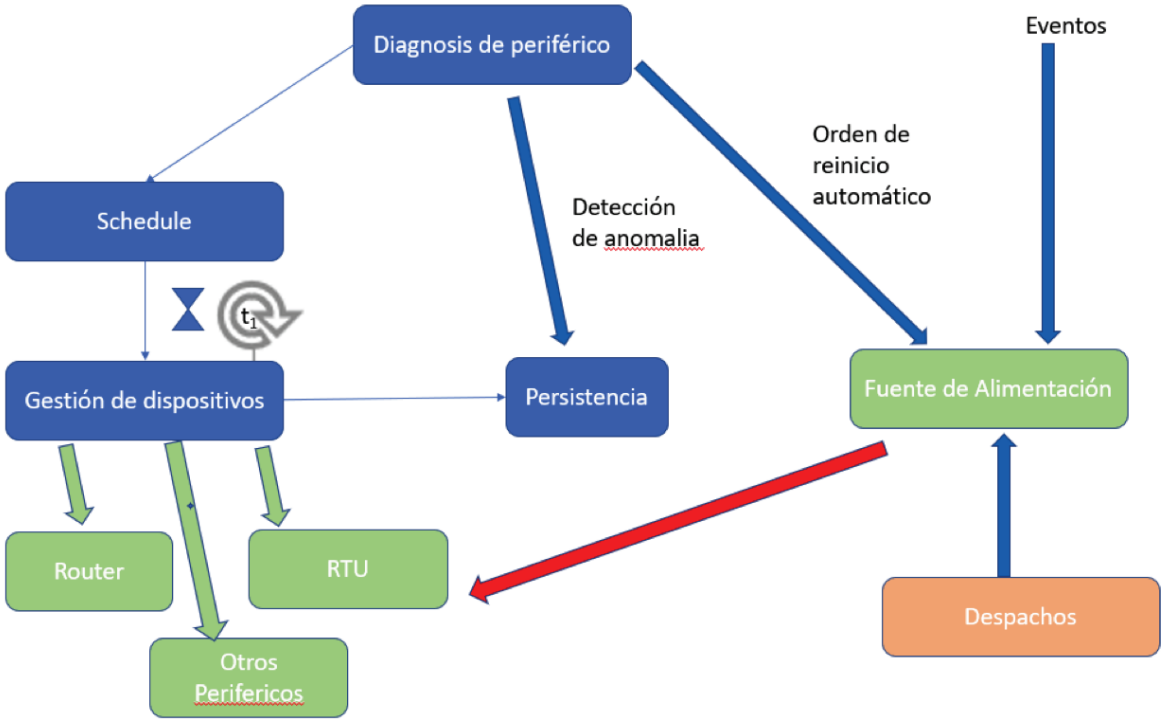


Figura 94: Esquema flujo de reinicio de equipos.

del CBT). El principal objetivo es la localización de la avería (elemento del grafo topológico afectado) y habilitar un mecanismo (si fuera automatizado) o notificación para su rápido restablecimiento.

El objetivo inicial es generar información adicional para la localización de avería en tipología de incidencias de corte de suministro

(corte conductor, fusible en CGP...), sin disparo de fusible en CBT.

- Recibirá los eventos espontáneos de interrupción de la SABT y de los CNs trifásicos. Incluso detectará reducciones de consumo fuera de rango.
- Recibirá las llamadas de incidencia de los clientes (Call Center) OMS.
- Seguirá localmente la lógica de pings a CNs para identificar tramos de LBT con tensión estable y sin tensión: CNs trifásicos de misma CGP, de misma LBT y mismo transformador que los eventos recibidos.
- Proporcionará el tramo de LBT con posible localización de avería.

- Activación 2. Solicitud / captura de informe eventos de tarjetas se la SABT. Evento de detección Fusión de fusible por fase de LBT
- Activación 3. Concentrador. Activación por detección de eventos espontáneos de CNs de tipo calidad de corte de larga duración. En principio sólo de CNs trifásicos para eventos espontáneos.
- Reducción brusca de la demanda del centro superior a un % determinado, ya que la propia avería podría perturbar las comunicaciones con los contadores. Si se detecta una reducción del consumo y una pérdida de comunicaciones que además es acorde dicha reducción del consumo con la suma de los consumos (perdidos) por las comunicaciones,

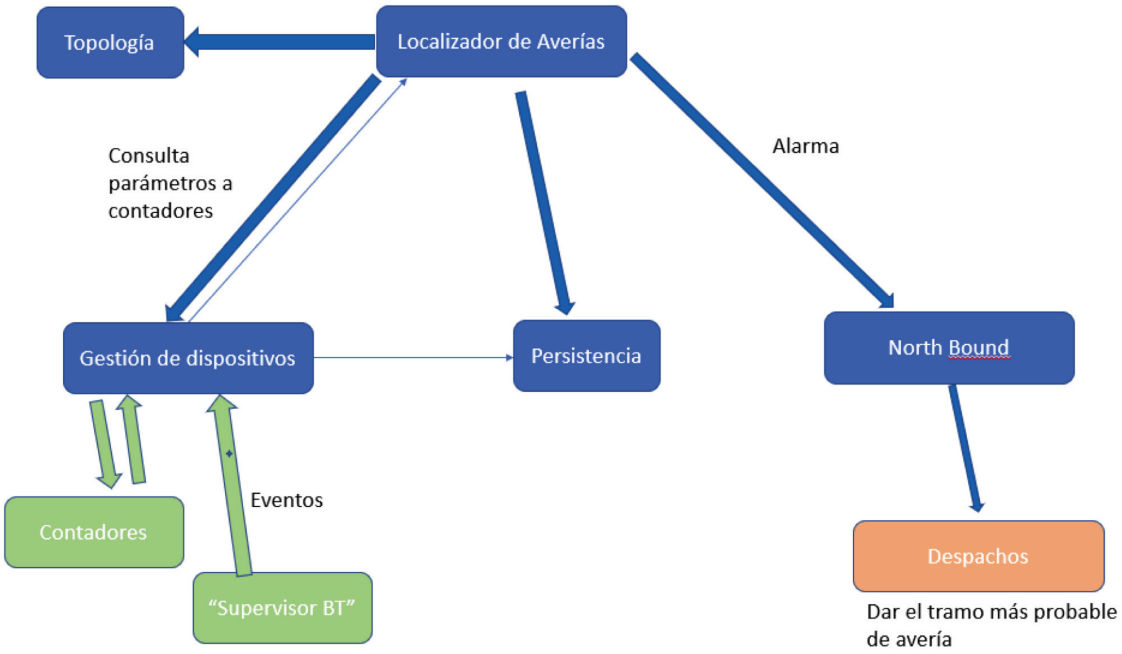


Figura 95: Esquema flujo de localización de averías.

Existirán diferentes mecanismos que activarán el proceso de detección y localización de anomalías;

- Activación 1. Solicitud desde el Sistema central tras recepción de llamada/incidencia en OMS. Información de entrada LBT y CN asociado a punto de suministro con llamada (si sólo uno).

se buscaría en topología el tramo entre el último contador con comunicaciones y el primero sin comunicaciones para focalizar el tramo con mayor probabilidad de avería. Además, se ganaría tiempo por no esperar a la activación por medio de la llamada de los clientes. Esta estrategia permite no depender solo de los contadores trifásicos y sus eventos espontáneos.

Herramientas que servirán para localización de la avería:

- Utilización de la información de conectividad asociada a la LBT con incidencia. Lista de CNs trifásicos.
- Uso de informe de estados y topología PRIME de los CNs que tiene el CD, para detectar los contadores que tienen comunicación activa y poder ir lanzando solicitud de petición de valores instantáneos para confirmar disponibilidad.
- Solicitud al Concentrador de informe reducido de valores instantáneos a la lista de CNs trifásicos, para confirmar disponibilidad y medida de tensión en sus tres fases.

El procesado de los informes de valores instantáneos (tensiones por fase), permitirá:

- Con disponibilidad de la información topológica, permitirá la búsqueda de último CN con las 3 tensiones estables y el primer CN con una o varias tensiones a cero.
- Confirmación caso de fusible fundido. Todos los CNs (asociados a esa fase) con una tensión a cero.
- Confirmación avería cliente. Todos los CNs con las tensiones correctas, incluyendo CN en la misma CGP.
- Confirmación avería CGP. Todos los CNs con las tensiones correctas, excepto CN en la misma CGP.

7.6.1.2. Búsqueda de agrupaciones de sobretensiones como preventivo de la calidad de la conexión del neutro.

En función del % de suministros afectados en el centro de transformación y de su ubicación con respecto al centro de transformación y relativo entre ellos podría darnos la indicación de cambio de toma del transformador si están afectados un % superior al 90% (p.e.). O alejamiento de referencia de neutro si todos pertenecen a una misma fase (la de menor consumo)

Ante la detección de un evento de sobretensión en un suministro (equipo de medida), la aplicación debe compararlo con la tensión de suministro del cuadro de BT.

Si la tensión de suministro del cuadro de BT es menor que el suministro debe compararse con la tensión de suministro de las inyecciones en BT que estén asociadas a dicho concentrador.

Si no hay generaciones la explicación de tener más tensión en el suministro que en el cuadro es la perdida de referencia del neutro en la fase de menor consumo.

Se debe elevar un mensaje para revisión de tierras y corrección de las mismas si procede por el departamento de operaciones que corresponda.

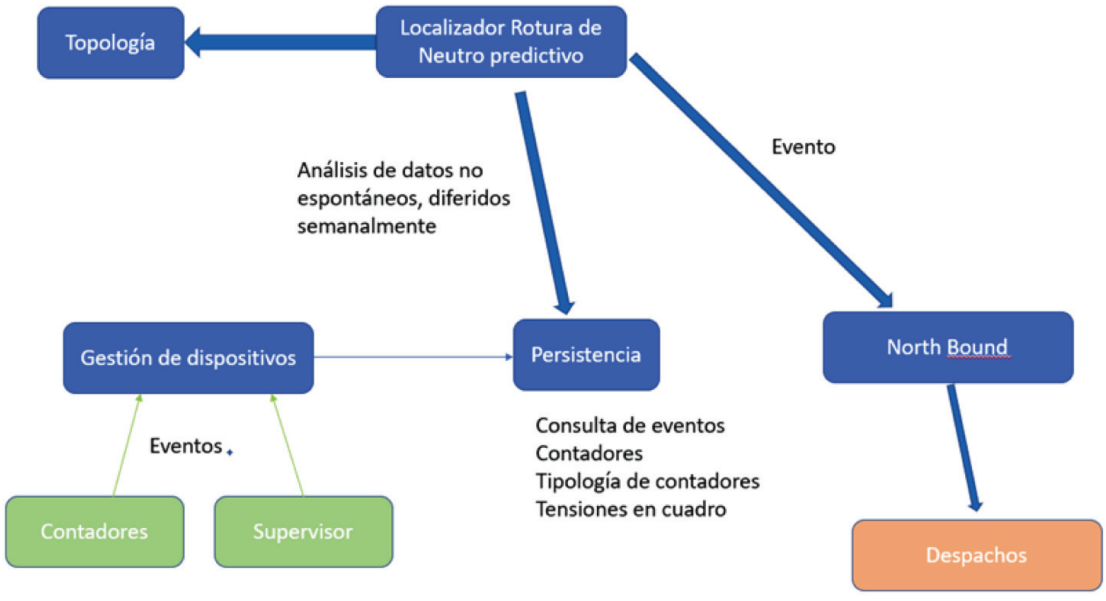


Figura 96: Esquema flujo detección problemas de neutro.

7.6.1.3. Búsqueda de agrupaciones de subtensiones como búsqueda de equilibrados de cargas por fase de la carga

Al igual que las sobretensiones, las subtensiones también nos pueden indicar la necesidad de cambiar la toma del transformador o la necesidad de plantear obras de reordenación de BT o incluso de regulación en un punto intermedio de la red de BT.

Cuando el número de eventos de subtensión en un suministro exceda de la cantidad que se estipule, se compara con los contadores anterior y posterior hasta conseguir agrupar una bolsa de suministros que tengan la misma problemática.

Estos contadores tienen unas coordenadas y por tanto se puede generar un "centro de Gravedad" que debe compararse con el "centro de Gravedad" del centro de transformación

En tanto estas distancias son mayores las soluciones son distintas:

- Una gran distancia suele suponer la necesidad de un centro nuevo o una salida nueva.
- Una distancia media suele suponer una repotenciación de conductores o una reordenación de la red.
- Una distancia pequeña supone un cambio de referencia en las tomas del transformador.

7.6.1.4. Detección de fugas a tierra

El control del CT realizará un análisis de las lecturas obtenidas de manera periódica por el módulo Concentrador a través de la lectura de un Toroidal o VTN. El módulo contará de las siguientes funcionalidades:

- Capacidad de análisis de tendencia de fugas a tierra.
- Configuración de umbrales para el envió de alarma (20A – 60A).

La SABT también dispone de entradas de medida de corrientes conectadas a Transformadores de Intensidad (TIs) colocados en la puesta a tierra del Neutro de los CBTs de cada transformador.

Las fugas a tierra se pueden dar por diferentes motivos: unión de neutros entre transformadores, derivas a tierra, etc y sería posible tipificarlos, incluso localizarlos mediante analítica de datos. La medida de tensión entre Neutro y Tierra de Herrajes confirmaría una fuga a tierra real.

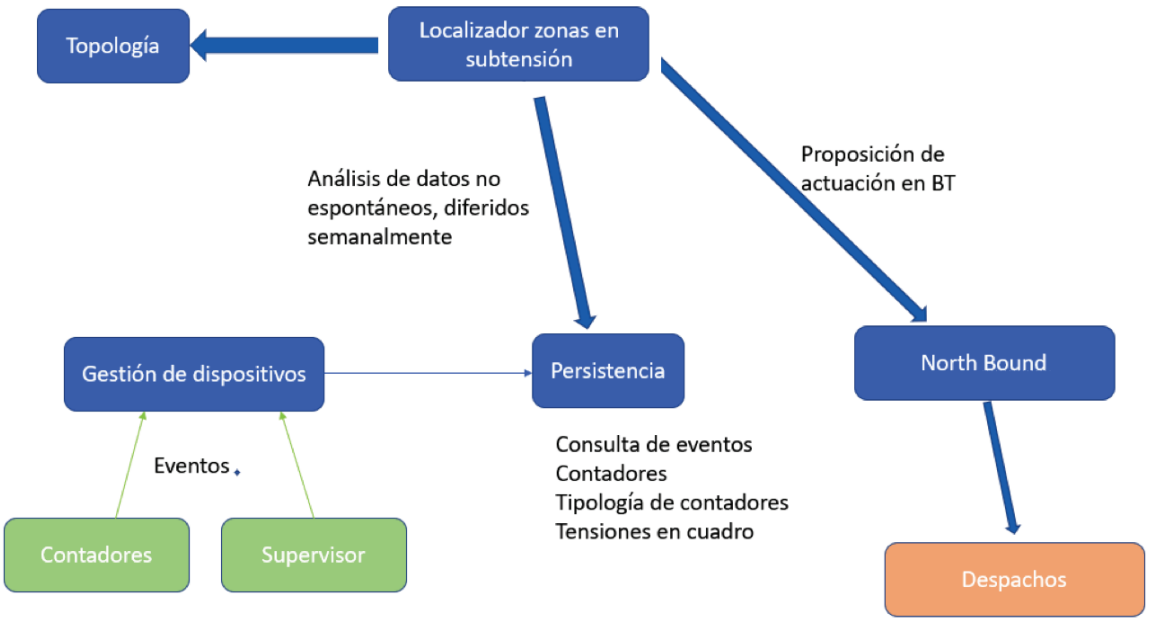


Figura 97: Esquema flujo detección desequilibrios de fase.

7.6.1.5. Detección de rotura de neutro BT y automatización de maniobras para evitar daños a terceros.

En este caso se activa con el evento espontáneo de la rotura de neutro y se mandaría abrir no solo a aquellos contadores o equipos de medida que detectan dicho evento (que se debería hacer en local/contador para proteger al cliente) sino a todos los equipos de medida ubicados eléctricamente alrededor (topología) que presenten una sobretensión superior a la normal pero que no esté dentro del rango reglamentario.

Con la finalización del trabajo de reparación del Neutro se consultaría el listado de suministros interrumpidos previamente por tener sobretensión para recuperar su suministro dado que la red está asegurada.

Dicho listado debería ser remitido a gestión de reclamaciones como un listado de potenciales entradas en los x días posteriores. Asociando las reclamaciones potenciales con la rotura de neutro del vecino y reduciendo los tiempos de gestión de la reclamación.

7.6.2. Listados de SPV sospechosos (anomalías de tensiones o conectividad)

La disponibilidad de medidas de tensiones y corrientes del supervisor, permitirá detectar fallos en la medida del propio equipo o errores de conexión, roturas de TIs, etc..

Ejemplo de anomalías detectables:

- Tensión de referencia incorrecta.
- Inversión (180º) de I en las 3 fases.
- Inversión (180º) de I en 1 o 2 fases.
- Tensiones anómalas.
- Tensiones a 0.
- Intensidades a 0.
- Fases invertidas.

La detección de estas anomalías será notificada al sistema central para ordenar su resolución y deshabilitará todos los algoritmos locales que hagan uso de los datos del supervisor.

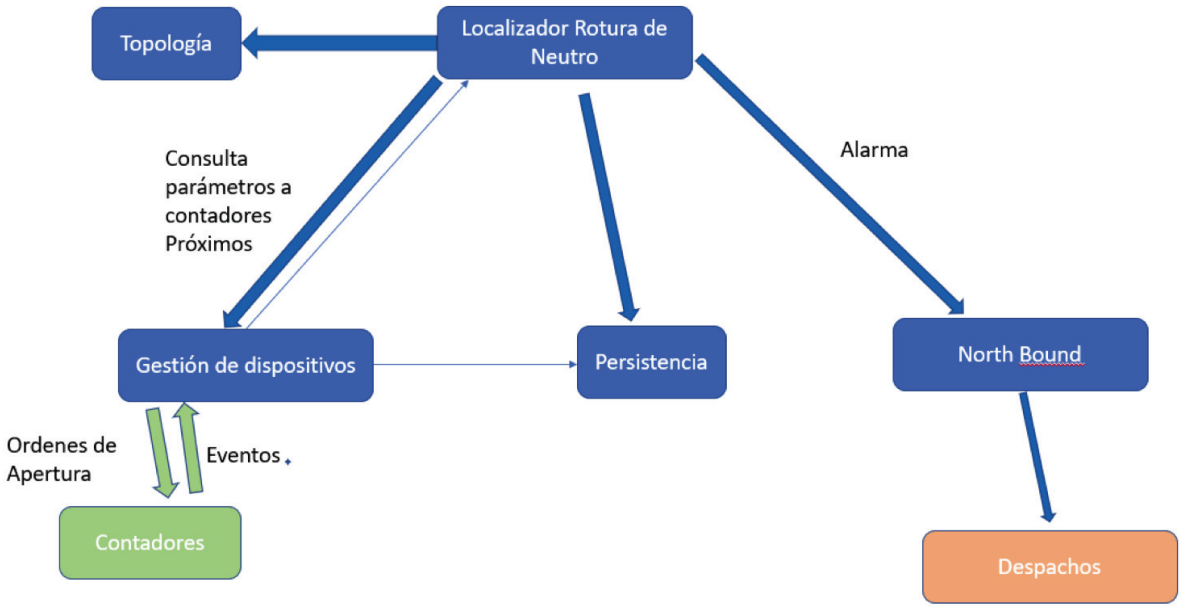


Figura 98: Esquema flujo de detección rotura de neutro.

7.6.3. Listados de CNs sospechosos (anomalías de tensiones)

Con los mismos criterios que para los supervisores, se mantendrá un listado de CNs sospechosos de tener una anomalía, cuyos datos no se tendrán en cuenta para alimentar los diferentes algoritmos, por no ser fiables o por ser erróneos.

De esta manera se detectarán anomalías como: tensiones B2 desequilibradas, tensión B2 alta (sobreV), tensión B2 baja (subV), sobretensión extrema (posible fallo CN o permutación fase-neutro en B2), tensión cero en contador trifásico (posible conexión especial de CN), subtensión extrema en CN trifásico (posible neutro flotante o fallo CN), subtensión extrema en CN monofásico (posible fallo CN), tensiones null incorrectas, tres tensiones cero, etc... que deben confirmarse que solo afectan al CN en cuestión y no a los vecinos, para incorporarlo a la lista de sospechosos y notificar al sistema central.

7.6.4. Detección fallos de aislamiento

Sistemas de campo para la localización de fallos de aislamiento en BT y AT. Uso datos medida corrientes de SABT y CNs

7.6.5. Detección anomalías MT

Uso eventos del supervisor de BT para detección de FAI: Detección de conductores caídos y pérdidas de fase con faltas a tierra.

Con la monitorización de las tensiones en BT se pueden inferir averías en la MT. En el caso de caer dos de las tensiones a valores equivalentes a raíz (3) de su valor y mantener la tercera de las fases en parámetros normales de suministro puede ser la representación en valores de la rotura de una de las fases de alimentación (apertura de un XS; rotura de puente).

Para proteger a los clientes (principalmente los trifásicos y en concreto los que tengan motores) se debería de actuar sobre las fases de BT que están en subtensión (abriéndolas en el caso de estar automatizadas) y sobre los clientes trifásicos (reales).

En caso de no estar automatizadas las salidas de BT debería de hacer una consulta a los clientes de BT y mandar su apertura a aquellos que presentan subtensión, registrando las órdenes de apertura. Una vez terminadas las aperturas debe seguir vigilando para detectar la corrección del problema y mandar reenganchar a aquellos clientes que abrieron.

Debe mandar un aviso al despacho correspondiente para avisar que hay una falta de alta impedancia que no se han activado las protecciones de cabecera y que se debe proceder a la localización.

El contador de supervisión de BT al ser trifásico, en caso de subtensión de una o dos fases puede seguir funcionando cuando se produce la fase abierta en MT, sin embargo, en el caso del equipo de comunicaciones, alimentado con una tensión monofásica, es posible que quede inoperativo. La mínima tensión de las tres que puede llegar a producirse es de 100 voltios, tensión simple, luego es recomendable que los equipos que se alimenten de una tensión monofásica simple mantengan su funcionamiento un 20% por debajo, es decir hasta 80 voltios.

Dado que, en los Centros de Transformación, la conexión del supervisor al sistema trifásico de tensiones de BT no se puede garantizar que se realiza en secuencia positiva (en situación estable de red), es necesario que el concentrador disponga de un algoritmo autoadaptable al tipo de secuencia que "ve" en situación estable de red, positiva o negativa, debiendo "buscar" por tanto la secuencia contraria para detectar la situación de Falta de Alta Impedancia en MT por fase abierta.

Se propone a modo de sugerencia un algoritmo del tipo:

Se activa la unidad sólo si "s1/s2 > 20% Y s2/s1 > 20%", donde 20 es el ajuste "Arranque (V2/V1 en tanto por 100)".

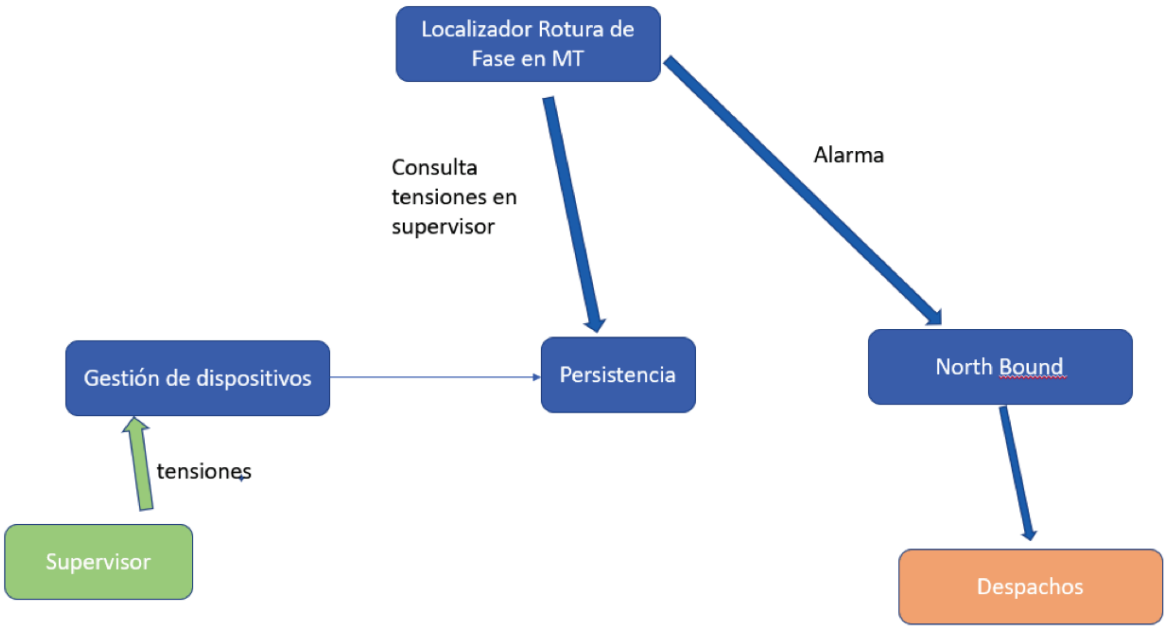


Figura 99: Esquema flujo de detección de anomalías en MT.

7.7. Analítica de Red

La ventaja del procesamiento distribuido es que permite análisis de datos en el momento y lugar donde se están generando, habilitando mecanismos ágiles de detección y predicción que conlleva beneficios de ahorro en ancho de banda (envío de grandes volúmenes de datos a sistemas centrales), mejora de la seguridad (cifrado de datos desde su generación), etc. El procesamiento distribuido elimina el problema de privacidad que supone la transmisión de millones de datos y su almacenamiento en la nube (sistemas centrales)

Estos procesos analíticos avanzados ejecutados de manera distribuida utilizan algoritmos de Machine Learning e Inteligencia Artificial para el tratamiento de los datos que permiten pronosticar comportamientos y estados, así como ir aprendiendo y enriqueciendo los modelos que pueden ser compartidos con los sistemas centrales para volver a desplegarse ese aprendizaje (clasificación de situaciones) a los centros distribuidos (CTs), así como disponer de un modelo digital completo (Gemelo Digital) de un Centro de Transformación, sobre el que permita realizarse simulaciones.

7.7.1. Topología-Conectividad Contadores

La conectividad aporta información adicional a los procesos que utilizan datos y medidas relacionados con la telegestión y la digitalización en la red de BT, puesto que supone identificar con detalle el punto de medida en la realidad (cable de fase y línea de BT), de modo que para utilizar los datos no es necesario realizar hipótesis simplificadas de repartos entre fases. Esta funcionalidad optimiza la capacidad de la red de BT, dirige las acciones de mejora de forma eficaz y garantiza una gestión eficiente de la red y los recursos.

Los procesos más relevantes que utilizarán la información de conectividad son:

- **Gestión de Nuevos Suministros.** Con la telegestión por fase identificará la capacidad de la red de BT por fase, de modo que optimizará las nuevas conexiones en las fases óptimas, reduciendo la necesidad de aumentos de capacidad y tendiendo a equilibrar la red para reducir la saturación y las pérdidas.
- **Gestión de incidencias.** La información de eventos y pings a CNs conociendo la fase a la que se encuentran conectados permite detectar y confirmar mejor la localización

de la avería, dar coherencia a las respuestas cuando comunican y cuando no, enriquecer la información con los CNs monofásicos, y optimizar la predicción y confirmación de incidencias en la red de BT.

- **Calidad de servicio al cliente.** La información de tensiones fuera de límites y la información de calidad de producto con la capacidad de distinguir por fase permite una gestión más eficiente de las actuaciones, adelantándose a las reclamaciones o gestionándolas en menor tiempo.
- **Capacidad de red.** La información de conectividad, combinada con los datos de supervisión avanzada permite una gestión de la red de BT con medidas reales que evitan la utilización de coeficientes de seguridad y simultaneidad conservadores para situaciones puntuales.

El presente apartado describe la funcionalidad de detección de la conectividad de los puntos de suministro a línea de BT y fase. La conectividad es un dato de inventario que relaciona un punto de suministro con la topología de la red (Grafo topológico indicado en Predicción de red). Esta información es un dato fundamental para la operación, el mantenimiento y la gestión de los nuevos suministros, puesto que permite conocer la afección de las incidencias y cortes programados sobre los clientes, y optimizar la capacidad de la red repartiendo los consumos y la generación de forma óptima entre las fases de la red de BT.

La conectividad es un dato cambiante con la topología de la red y más útil cuanto más detallado y con mayor fiabilidad. El objetivo es disponer de la conectividad de los clientes a la fase de la línea de BT de cada CT.

Se describirá los requerimientos actuales del único sistema validado actualmente que se basa en datos de telegestión de los CNs (consumos) y la supervisión avanzada de BT, en el que se realiza la correlación entre los datos de corrientes medidas en los suministros y en las líneas, para obtener su asociación. Existen otras iniciativas y proyectos para la detección de la conectividad (entendida como asociación de la fase/s conectada/s de cada CNs con respecto el secundario del transformador) a través de las comunicaciones PRIME, basadas en la especificación de sincronismo de trama en la versión 1.4, que está en proceso de desarrollo e implementación. Asimismo, se están desarrollando diferentes algoritmos de conectividad, agnósticos al sistema de comunicaciones PLC, que también se basan en datos de telegestión de los CNs y la supervisión avanzada de BT y que no requieren de la modificación del firmware de los CNs.

El sistema de conectividad deberá actualizar automáticamente los contadores vinculados a cada salida de BT del cuadro del CT, sin necesidad de que manualmente se corrijan asignaciones por nuevas incorporaciones o cambios de frontera en la red de BT.

El objetivo es mantener la conectividad de los CNs/puntos de suministro actualizada, para lo que se configurará una:

- Ejecución del algoritmo periódicamente.
- Ejecución a demanda: Identificación de situaciones de actualización adicionales según las necesidades de los procesos de utilización del dato de conectividad.

Las causas principales de actualización de la conectividad son:

- Nuevo punto de suministro/CN. Ejecución de la conectividad para detectar el nuevo CN.
- Sustitución del CN. El CN nuevo hereda la conectividad del punto de suministro inicialmente y a posteriori se debe confirmar ejecutando el algoritmo.
- Modificación de red "provisional" por incidencias por cambios topológicos y/o maniobras durante la resolución temporal de averías en BT. Los procesos que utilicen la conectividad deberán definir la necesidad de actualización provisional (tiempo mayor de 48 horas), de la conectividad, teniendo en cuenta el tiempo de convergencia y la resolución definitiva de la incidencia con la reparación y vuelta a la topología inicial.
- Modificación de topología de red definitiva por desarrollo, renovación, modificación de sectores, cambio B1-B2. Es necesario ejecutar el algoritmo de conectividad.

Respecto al algoritmo actualmente utilizado y validado, los datos de entrada necesarios para su ejecución son:

- CNs: almacenan 48 eventos instantáneos de máxima carga. El CN vigila que la medida instantánea modifique su valor en un determinado "paso" (parametrizable, en estos momentos 0,1 A) y si el valor es superior al menor del buffer hasta el momento, se actualiza.
- Concentrador: programación de ciclos para solicitud de los buffers de eventos que almacenan los CNs.
- Supervisión avanzada de BT: almacena la intensidad cada segundo de cada fase de cada línea de BT.

Las condiciones que mejoran la convergencia del algoritmo son:

- Consumo en los CNs. Cuantos más eventos de consumo (corriente), mejor será la convergencia, debido al uso que hace el algoritmo de correlación de máximos de corrientes.

Como resultado el algoritmo actualizará el grafo de topología y notificará actualización al sistema central.

7.7.2. Detección y prevención de fraude

La disponibilidad de Supervisión de Red vista en la sección anterior, habilita la posibilidad de detección de pérdidas, simplemente comparando los consumos de todos los puntos de suministro con respecto el consumo medido en cabecera. Ahora bien, una vez detectado este desequilibrio entre consumos se debe distinguir el motivo: pérdidas técnicas o pérdidas no técnicas (fraude).

7.7.2.1. Perdidas no técnicas

Para el cálculo de las pérdidas no técnicas (posibles fraudes), es necesario conocer previamente la información anterior (pérdidas técnicas) y construir una matriz de datos que agrupe la información de los CTs, grafo topológico, sumatorio de los consumos de todos los puntos de suministro, curva o consumo total del supervisor del DC o curva del supervisor avanzado.

Ya existen en el mercado modelos de cálculo de pérdidas Técnicas basado en los datos de los elementos de la red, que hay que restar a la diferencia total de pérdidas, para obtener las pérdidas no técnicas.

Se deberá tener en cuenta todos los consumos de todos los puntos de suministro del CT, sean telegestionados o no. Asimismo, se deberán tener en cuenta más mediciones que puedan aportar valor en el análisis.

7.7.2.2. Modelo de detección de Fraude

Existen diversos modelos de detección de fraude basado en datos de las curvas de carga de los clientes (consumos), entre los que a continuación se propone y se describe con

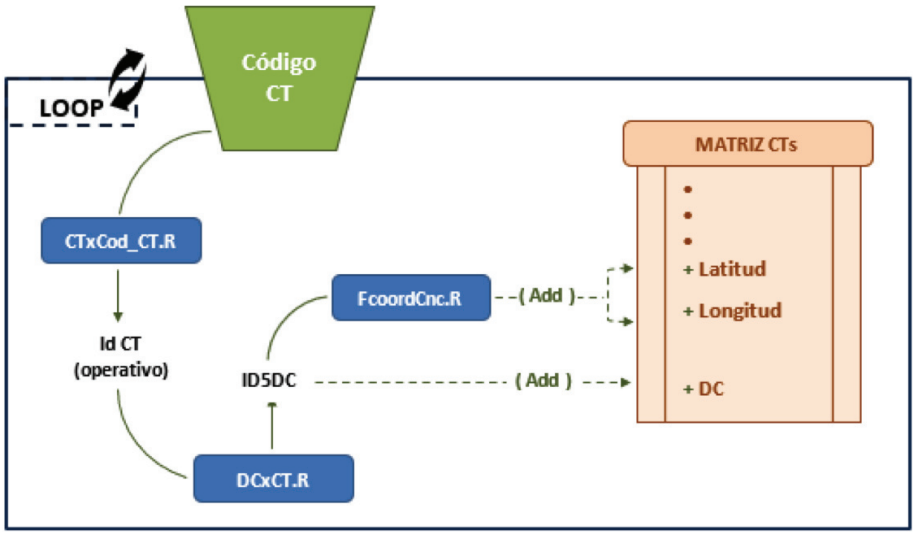


Figura 100: Esquema flujo de cálculo de pérdidas no técnicas.

mayor detalle uno de los más sencillos. Además, estos modelos se podrán aplicar a diferentes ámbitos:

. Modelo para detección anomalías.

. Modelo detección Fraude.

. Modelo fraude por zonas geográficas.

. Modelo fraude por tipo cliente (CCH).

7.7.2.2.1. Consumos

Para la agrupación y tratamiento de los consumos, no se tendrán en cuenta aquellos con un Bit de calidad diferente de cero (por fiabilidad del dato).

Como se indicó anteriormente, es necesario que se traten las localizaciones de los puntos de suministro.

7.7.2.2.2. Pérdidas por Curva horaria

Los cálculos de las pérdidas técnicas y no técnicas se hacen a partir de la matriz de consumo generada anteriormente y estos se deberán agrupar por un único identificador. En el ejemplo, se muestra la agrupación hecha por el DC (CncId) y la fecha y, finalmente se realiza el sumatorio de la lectura activa de importación (AI).

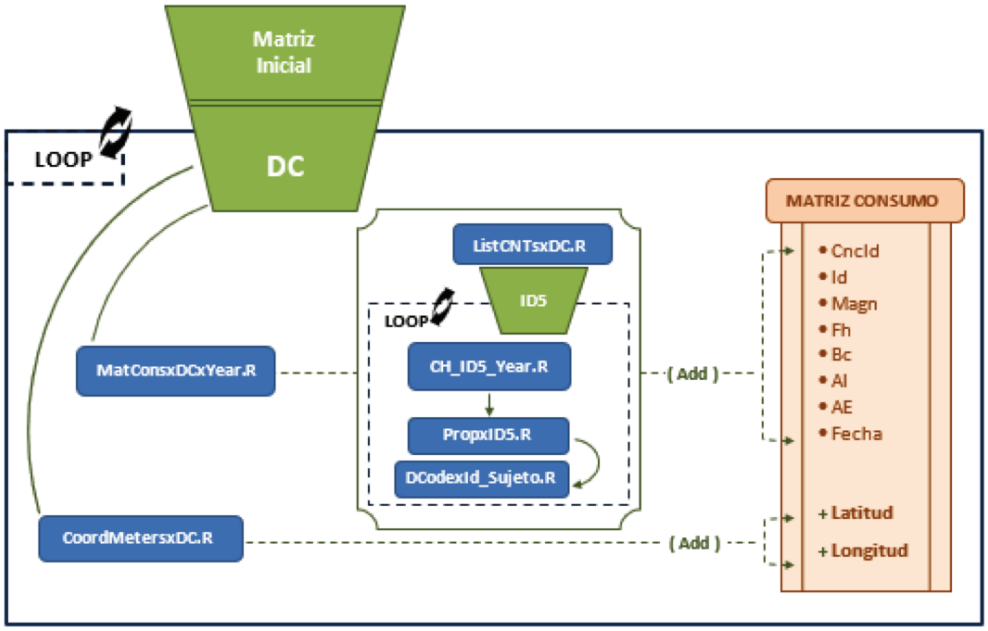


Figura 101: Esquema flujo agrupación y tratamiento de los consumos.

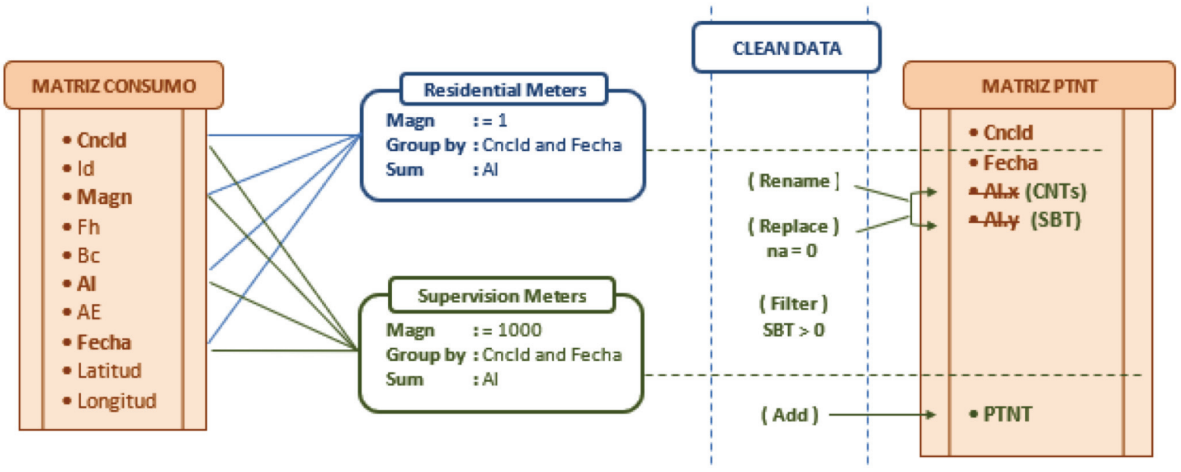


Figura 102: Esquema de cálculo de perdidas por curva horaria.

Se calcula el campo PTNT (Potencia Técnica y No Técnica) de la siguiente manera:

$$PTNT = \frac{SBT - CNTs}{SBT}$$

7.7.2.2.3. Análisis de pérdidas no técnicas

Para analizar la probabilidad de fraudes de los puntos de consumo se utiliza la matriz de consumo calculada anteriormente. Se hace el siguiente tratamiento a través de cuatro bloques analíticos

1. **Pasos por 0 de los suministros.**

   A partir del identificador CncId, se recupera el total de elementos (k) de la matriz de consumo, se filtran los consumos (AI) y Bit de calidad que sean igual a cero, se cuentan los elementos filtrados (P_Z) y se calcula el porcentaje de suministros que pasan por cero con la siguiente formula:

   $$P_{Zt} = \frac{P_Z}{K * 100}$$

2. **Correlación de los suministros con las pérdidas.**

   La correlación no es más que el análisis de la proporcionalidad o relación lineal que existe entre, mínimo, dos variables. A continuación, se calculan las pérdidas (%), para buscar la correlación con la matriz de consumo.

   $$PTNT = \frac{(SBT - CNTs) * 100}{SBT}$$

   Una vez calculada las pérdidas horarias por CT (matriz de pérdidas), se crea una matriz de correlación que corresponde a la matriz resultante de aplicar un left join entre las matrices de consumos y pérdidas. Finalmente, el valor de la matriz de correlación resultante se multiplica por 100 y se seleccionan los campos Id5 y PTNT (peso de la correlación - Crr_P) para añadirlos a una nueva matriz, Matriz de Fraude.

3. **Consumos fuera de la media agrupados por CNAE.**

   Se usa una técnica de agrupación por el parámetro CNAE, que deberá agregarse a una nueva matriz para identificar los puntos.

   Por cada tipo de CNAE se intenta determinar los consumos fuera de la media, para ello, se busca determinar los elementos anómalos en la matriz de fraude, con la función boxplot, graficando la lectura activa (IA), variable de agrupación y como variable continua la fecha.

   Una vez se han obtenido los elementos anómalos se crea una matriz de objetos compartidos (Mat_Avrg_tipso) que es el resultado de las lecturas activas de importación (AI) que se encuentran dentro de los resultados anómalos (outliers). A partir de esta matriz se procede a estandarizar los datos.

   El proceso de estandarización de los datos consiste en calcular la media y la desviación de las variables cuantitativas para trabajar con rangos comprendidos entre 0 y 1. El resto de los cálculos se realizan a través de las funciones estándares disponibles en las librerías.

   Tras conseguir la estandarización, se deberá buscar el límite inferior de la muestra a partir de la media y desviación estándar

   $$LimInf = M - SD$$

   Para un mejor manejo de los datos se agrega una columna, booleana, a la matriz de datos que permitirá agrupar por tipos para finalmente determinar, con un valor porcentual, los consumos que se encuentran fuera de la media por tipo CNAE. La columna booleana se calcula de la siguiente manera:

   $$bLimInf = (AI < (M - SD))$$

   Esta nueva columna nos permite obtener el total de elementos que cumple con

la condición antes mencionada por lo que se agrupan los datos de la matriz por identificador y la nueva columna, bLimInf, filtrando solo los elementos que se encuentran fuera del límite, es decir, los valores verdaderos. Este valor devuelto le llaman NLimInf.

El valor porcentual se calcula dividiendo el total de elementos que se encuentra fuera del límite inferior entre el total de elementos de la matriz multiplicado por cien. Tal y como muestro en la siguiente formula:

$$KLimInf = \frac{\mathbf{NLimInf}}{\mathbf{K} * \mathbf{100}}$$

Para completar el análisis, se le asigna un peso estadístico, según los estudios realizados por cada empresa. En este caso, se asignó un 30% al paso por cero de los suministros, un 50% a la correlación existente entre los suministros y las pérdidas y un 20% al clustering por CNAE de los consumos fuera de la media.

$$K = (\mathrm{P_Z} * 0) * 0.3 + \mathrm{abs}(\mathrm{Crr_P}) * 0.5 + \mathrm{KLimInf} * 0.2$$

7.7.2.3. Localización de fraude a partir de algoritmos de PowerFlow

El algoritmo de Power Flow proporciona unas salidas teóricas en base a datos reales de contadores y las tensiones que hay en el secundario del transformador, dando así la tensión que en teoría debería tener cada nodo de la red.

A partir de esos datos teóricos, se podrán comparar en tiempo real con datos reales de dichos contadores para detectar caídas de tensión anómalas, provocadas por consumos no informados o fraudulentos.

De esta manera, se podrá localizar en qué tramo de la red de baja tensión se está produciendo un fraude y cuantificar qué potencia se está defraudando, así como las horas principales en las que se produce.

Esta información es de especial utilidad para los operarios, ya que saben exactamente a qué puntos de la red han de ir para quitar el fraude y las horas a las que han de acudir.

7.7.2.4. Localización enganches directos

De manera muy similar al algoritmo anterior y haciendo uso de modelos analíticos que realice una tipificación de consumos (con sus curvas de carga), usando valores instantáneos de tensiones (Mapa de tensiones síncrono) y variaciones de la topología de la red PRIME de contadores, es posible localizar tramos, segmentos donde se está produciendo fraude mediante un enganche directo a la red, estableciendo un índice de probabilidad de cada elemento de la red que facilite a los inspectores la localización.

Se están especificando nuevos objetos de perfiles de tensiones y corrientes instantáneas que estarán disponible en todos los contadores de la red, de manera que permita tener valores de tensiones sincronizados (valores instantáneos de todos los suministros en el mismo momento), que aportará mayor eficiencia en los índices de probabilidad de localización de este tipo de fraude.

7.7.3. Detección ruidos PRIME BT

Se trata de aprovechar la disponibilidad localmente de datos de tráfico de la red PRIME PLC, junto con datos topológicos y disponibilidad de CNs (con gran volumen de datos), junto con valores de niveles de tensiones y curva de carga y conectividad, para habilitar la posibilidad de localización de la fuente (suministro) que genera ruido en la frecuencia de comunicaciones PRIME, realizando una correlación entre el momento (la hora) que un suministro está consumiendo, con variaciones de topología (PRIME) y tensiones. De manera que se identifique y notifique al sistema central para la posible instalación de filtros.

Igualmente, también podrá analizarse secciones de la red de BT donde debido a sus longitudes la señal PRIME pueda sufrir grandes atenuaciones y requieran intervención e instalación de equipos repetidores.

Si se dispone de la conectividad por fase de todos los CNs y su disponibilidad PRIME, en caso que ciertos CNs conectados a una de las fases presenten menor disponibilidad, permitiría automatizar modificaciones de configuración

de la fase de inyección PRIME hasta obtener la configuración más conveniente y que mayor señal llegue a todos los CNs.

7.8. Control de Red

7.8.1. Regulación en carga transformador MT/BT

El control del CT actuará sobre la regulación del transformador subiendo o bajando tomas en función de la tensión de la red de BT aguas abajo del transformador.

El "Algoritmo optimizador de consigna" (en adelante AOC), determinará la toma óptima del transformador teniendo en cuenta los datos de tensión en la cabecera, pero sobre todo la tensión en los puntos de suministro a través de los informes de los CNs.

Los criterios de actuación son los siguientes:

- Monitorizará las tensiones de la red de BT mediante la información de la supervisión y los CNs, pudiendo solicitar lecturas instantáneas a CNs siguiendo una estrategia eficiente de número de consultas. Por ejemplo, identificando los puntos de suministro sensibles a variaciones y tensiones fuera de límites.
- Podrá recibir consignas remotas de tensión y de cambio de toma o realizar un control local en base a parámetros que podrá incluir una curva de actuación en función de tensiones límites y banda de no actuación.
- Detectará tensiones fuera de límites (sobre y sub tensiones) y la necesidad de modificar la toma y calculará que no se produce un impacto negativo en algún otro punto de suministro. La lógica de decisión a partir de los datos de tensión se implementará por fases. Por ejemplo:
- Actuará sobre el regulador, e implementará un control inteligente/histéresis de órdenes, evitando movimientos continuos de toma de regulación.

La estrategia de control tendrá en cuenta la capacidad de procesado de la información de tensiones de la red de BT, la estrategia de confirmación de medidas, el algoritmo para identificar la necesidad de actuación, la comprobación de seguridad de la acción y la ejecución sobre el regulador.

7.8.1.1. Algoritmo optimizador consigna trafo OLTC

El i-Trafo debe mantener una tensión en el secundario del transformador que optimice la tensión, partiendo de las medidas de tensión de los puntos de suministro críticos de la red de BT alimentada por el i-Trafo.

Para ello, se dispondrá de un sistema de determinación de consigna de tensión óptima, u optimizador, que inicialmente será una funcionalidad integrada en el sistema central (ejemplo STG) y se podrá trasladar al nodo local de procesamiento. El algoritmo se encargará de establecer la consigna a seguir por parte del regulador de tensión integrado en la funcionalidad de "Regulación transformador OLTC".

Esta consigna tendrá un valor constante durante un periodo ajustable de varios minutos, pero que se actualizará periódicamente siguiendo las variaciones de tensión en la red a lo largo del día. La consigna se establecerá en función de la estadística de tensiones proporcionada por los contadores de BT y el supervisor del secundario de transformador.

EL AOC se comunicará de forma periódica con el regulador de tensión, para enviar la nueva consigna.

La consigna se determinará de acuerdo a la estadística de tensiones de los minutos anteriores al cálculo. Para ello, el optimizador debe disponer de las medidas de los CNs y SPV.

El cálculo óptimo sería el derivado de disponer de las tensiones de todos los contadores. Debido a las limitaciones de la telegestión (comunicaciones concentrador-CNs), se usa una lista de contadores "sensores" representativos de los puntos de la red (idealmente serían todos los puntos de suministro si las comunicaciones lo admitieran) con las tensiones extremas, las más elevadas y las más bajas.

Por otra parte, los datos a utilizar no pueden ser excesivamente antiguos, dado que las condiciones de tensión de la red pueden haber variado, por lo que existirán diversos ajustes que afectan a los períodos de actualización.

La información que está previsto disponer a futuro, cuando se disponga de mejor información (en desarrollo nueva ET de CNs 2.0):

- Informes de perfiles de tensiones de los CNs (p.e. cincominutarios).
- Medidas promedio de los CNs (en vez de instantáneas).
- Mejora de la captura de la información por el DC.

7.8.1.2. Regulación transformador OLTC: envío consignas

La funcionalidad del regulador del i-Trafo está basada en la funcionalidad especificada en [15] realizada desde la RTU de BT. Pero en este caso el algoritmo de regulación del transformador podrá recibir una consigna variable de tensión de BT del i-Trafo X desde el STG (sistema central) o desde el "algoritmo optimizador de consigna" (descrito en el punto anterior), y dará órdenes de subir y bajar toma al control del i-Trafo, cuya especificación técnica se detalla en [14], para mantener la tensión medida en BT de acuerdo a la consigna, según los parámetros de control del regulador.

Para poder realizar el modo de funcionamiento automático, se identifican los siguientes tipos de datos intercambiados entre los diferentes componentes del sistema:

- **Consigna** (de tensión fase-neutro) (recibida del Algoritmo optimizador de consigna): tensión objetivo que se recibe desde el algoritmo optimizador de consigna con un tiempo de refresco de 1 minuto o superior. En el caso de recepción de una nueva consigna, el regulador seguirá funcionando y reiniciará únicamente la detección de cruce de umbrales y el contaje del tiempo correspondiente.
- **Ajustes del algoritmo de regulación** (recibidos del Algoritmo optimizador de consigna): recibidos vía comunicaciones, que suponen una reconfiguración del equipo que puede conllevar una parada temporal del algoritmo, seguida de su reinicio.
- **Ajustes del OLTC** (recibidos desde i-Trafo por DLMS). Estos son ajustes de la electrónica i-Trafo (de sólo lectura, ver [14]) que el Algoritmo de regulación debe conocer para poder realizar la regulación automática. Concretamente son los parámetros siguientes:
  - "taps": indica el número de tomas del transformador disponibles.
  - "tapStep", paso por toma o incremento de tensión por toma.

Este último será necesario para poder cumplir con las restricciones en el ajuste de los parámetros de configuración de la regulación automática (SlowRegTTol $\geq$ tapStep/2 y SlowRegCTol $\geq$ tapStep/4). Esto significa que las tolerancias (SlowRegTTol y SlowRegCTol) correspondientes a la unidad lenta, que se describe posteriormente, dependen del salto de tensión entre tomas (ver [14]).

- **Tensión en tiempo real** (información del Supervisor BT o SABT): el regulador recibirá tres tensiones fase-neutro (Vr, Vs y Vt).
- **Posición de tomas** (recibido desde la electrónica i-Trafo por DLMS). El regulador recibirá la posición de tomas del i-Trafo "nTap".
- Otras variables de i-Trafo (recibido desde la electrónica i-Trafo por DLMS). Tanto el estado del proceso del cambio de toma como el estado de las alarmas de i-Trafo (temperaturas, nivel, presión de aceite, fallo de centralita, fallo OLTC) serán necesarias para completar las lógicas del algoritmo de regulación a implementar (ver [14]).

Como regla general, el regulador conocerá el número de tomas disponibles y la toma en que se encuentra la electrónica i-Trafo, generando un evento en caso de no poder subir o bajar toma por haber llegado a la toma extrema.

Cambio de toma del OLTC:

Se generará un evento en el momento que se detecte un cambio de toma del OLTC. Este cambio se ha podido producir por diferentes razones:

- Cambio local y actuación manual (actuación manual en el CT). Puede ser mediante botonera o bien desde un ordenador conectado localmente a la tarjeta de i-Trafo.
- Cambio remoto y actuación manual (comando desde el STG).
- Cambio remoto y actuación automática (regulador de tensión en la RTU BT).

El timestamp asociado al evento de cambio de toma coincidirá con el momento en que se tiene constancia de que la toma se ha cambiado. Es por ello por lo que se debe mantener una variable con el estado de la toma actual.

7.8.2. CBT Automatizado

La automatización del cuadro de baja tensión se realizará mediante la instalación de un interruptor automático dotado de protecciones, motorizado y con telemando.

El control del CT actuará sobre la motorización de apertura y cierre del interruptor de cada fase de cada LBT.

- La operación estará basada en un estado normal cerrado, y la actuación de apertura se producirá principalmente por acción local de la unidad de protección, que puede estar integrada en el interruptor, en caso de cortocircuito o del control del CBT en caso de sobrecarga.
- El control permitirá la programación de reenganche por tiempo y tipo de falta. Si se cumple la parametrización ordenará el cierre de la fase abierta.
- El control recibirá las órdenes remotas de apertura y cierre por fase (telemando desde el sistema de control) y las enviará al interruptor.
- El interruptor señalizará el estado de apertura y cierre, aunque esta condición se detectará y comprobará a través de la supervisión avanzada de BT (SABT fusión fusible).
- El control recibirá información de la SABT en tiempo real, intensidades y tensiones, además de los eventos especiales de corriente de falta y los informes como la oscilografía.

En caso de disponer de Cuadro de BT automatizado que incluya interruptores automáticos que serán monitorizados y controlados por una electrónica que se le llamará i-CBT. Se espera que al menos realicen la funcionalidad de protección y control prevista:

- El i-CBT incluye la función de protección frente a cortocircuitos de forma autónoma hasta el despeje de la falta.
- El i-CBT incluye la función de protección frente a sobrecargas severas por encima de un umbral que requiera la apertura del circuito. Sobrecorriente temporizada (entorno de milisegundos a segundos).
- La Remota o SASCTI que controle el i-CBT incluye la función de reenganche y la función de protección frente a sobrecargas, tanto severas (redundancia) como no severas: protección de sobrecorriente temporizada con distintos umbrales (entorno de milisegundos a minutos) y de imagen térmica (minutos).
- Las funcionalidades de monitorización (vigilancia excepto disparo) se incluirá en la Remota de BT incluida en el SASCTI. Por ello se mantiene la referencia al ajuste de protección:
  - CBT con SABT. Ajuste de protección=calibre del fusible
  - i-CBT. Ajuste de protección=umbral de sobrecarga severa.

Se creará un algoritmo que hará las veces de RTU de CBT para la gestión de las tarjetas i-CBT.

Se identifican dos funcionalidades asignadas a la RTU de CBT, y relacionadas con el armario automatizado de BT (i-CBT).

- Función de reenganchador (ANSI code 79) que permitirá efectuar un cierre controlado de cada IA ante determinados disparos, y siempre y cuando se cumplen unas determinadas condiciones.
- Funciones de protección de sobrecarga o cortocircuito actuando de forma automática sobre la apertura del interruptor automático por fase (IA), coordinadas adecuadamente con las funciones equivalentes integradas en las propias tarjetas de control i-CBT de cada línea de BT.

Para poder realizar la función de reenganchador, se identifican los siguientes tipos de datos intercambiados entre los diferentes componentes del sistema:

- **Ajustes de la función reenganchador** (recibidos del Sistema central): recibidos a través del correspondiente orden, que suponen una reconfiguración del equipo que puede conllevar una parada temporal de la función, seguida de su reinicio.
- **Señalización de los disparos de los IA**, enviados por las electrónicas i-CBT por DLMS a la RTU de CBT, indicando el disparo de una o varias fases del IA de cada una de las líneas de BT.

- **Estado de los IA** (valores recibidos de las tarjetas i-CBT por DLMS) (abierto/cerrado/abierto por disparo): información adicional sobre el estado de apertura/cierre de los IAs como seguimiento del proceso de reenganche (ver [13]).
- **Otras variables de i-CBT** (valores recibidos de la tarjeta i-CBT por DLMS). Estas variables complementarias como son el estado LOCAL/REMOTO del armario i-CBT y el estado de alarma urgente, son variables necesarias para poder activar o no la función de reenganchador.

Una vez que está inicializado el reenganchador, el ciclo de reenganches (hasta un número máximo de intentos de reenganche) comienza cuando se detecta, por parte de la electrónica i-CBT correspondiente a un IA, una falta que provoca la apertura de una o varias fases del IA. La falta puede ser ocasionada por cualquiera de las siguientes causas:

- Sobrecorriente instantánea en las fases.
- Sobrecorriente temporizada en las fases.
- Sobrecorriente instantánea en el neutro.
- Sobrecorriente temporizada en el neutro.
- Falta a tierra.

El módulo reenganchador generará eventos asociados al estado del proceso de reenganche, disparo definitivo y ordenes de cierre de interruptor, todos ellos por fase. Todos ellos formarán parte del grupo de eventos asociados a la funcionalidad de reenganche, tales como:

- Eventos de desactivación-activación del reenganchador.
- Evento de disparo definitivo: Se generará un evento de disparo definitivo correspondiente a una determinada fase cuando se hayan cumplido los reintentos de cierre programados y aún persista un disparo de la protección del IA.
- Orden de cierre del reenganchador: Se generará un evento de cierre del reenganchador correspondiente a una determinada fase cuando se haya enviado una orden de cierre al IA fruto de uno de los intentos.

La funcionalidad de gestión de sobrecarga estará basada en la vigilancia de la corriente en cada fase de cabecera de LBT en relación a la capacidad del conductor de salida de la LBT (y del ajuste de protección).

La monitorización del nivel de carga provocará el envío de eventos de alarma de distintos niveles, locales SASCTI y al STG y en el caso de superar los umbrales de sobrecarga y tiempo, el disparo del interruptor automático de la fase con sobrecarga.

La protección de sobrecarga estará basada en dos módulos:

- Sobreintensidad temporizada.
- Imagen térmica

7.9. Gestión de la energía – flexibilidad

En este apartado se encuentran todas las funcionalidades que permitirán la gestión de la capacidad de la red en cada momento, permitiendo interactuar con consumidores activos sobre los que se permita actuar reduciendo potencia, cortando consumo (mediante gestión de la demanda), admitiendo vertido a la red en los autogeneradores (DER), etc. Permitiendo interactuar con puntos de almacenamiento, agregadores (integradores DER), microredes... de manera que doten de flexibilidad tanto en el consumo como en la generación distribuida que evitará el sobredimensionamiento del sistema para convertirlo en un sistema energéticamente eficiente.

Las funciones de DSO requieren monitorizar la red de BT y gestionar las restricciones en tiempo real y previstas, enviando las consignas o solicitud de servicios de flexibilidad de los recursos distribuidos (DER) conectados en la red de BT con flexibilidad, es decir, proporcionando servicios a la red.

Los requerimientos de alto nivel para proporcionar este servicio son:

- Capacidad de monitorización de la red de BT en tiempo real (Supervisión de red).
- Previsión de cargas y generación de escenarios previstos de corto plazo (Predicción de red).
- Análisis de capacidad de la red en tiempo real y sobre los escenarios previstos: detección de restricciones y evaluación de las necesidades/servicios de red.

- Simulación de la flexibilidad de los DER para resolver restricciones.
- Control DER. Envío de consignas (en caso de no gestión en plataformas de flexibilidad).
  - o Gestión activa de la demanda.
  - o Gestión de puntos de recarga de VE / coordinación de centros de recarga.
  - o Gestión de generación distribuida (autoconsumo).
  - o Gestión de equipos de almacenamiento (baterías).
- Consideración de posibles acuerdos existentes con DERs de prestación de servicios de flexibilidad, a considerar de forma preferente por el Centro de Transformación en caso de necesidad de activación del servicio.

El requerimiento de captura de la información en tiempo real es una funcionalidad local.

La implementación del resto de requerimientos puede ser local o centralizado o híbridos sincronizados.

Los principios básicos de las soluciones de gestión activa de la demanda (ANM) se basan en:

- Escalabilidad necesaria para desarrollo de automatización de la red de BT. Solución escalable de forma económica y técnicamente eficiente, con capacidad de respuesta en tiempo real analizando la utilización de nuevas arquitecturas de IoT frente a conceptos tradicionales SCADA.
- Integración/Interoperabilidad con infraestructura existente. Necesidad de arquitectura modular, adaptadores de protocolo que permitan el despliegue en los CTs actuales de equipos inteligentes con capacidad de procesamiento y su integración inmediata con dispositivos existentes y nuevos, a la vez que se incorpora interoperabilidad avanzada IoT con sistemas y plataformas centrales.
- Capacidad de procesamiento y control distribuido. La arquitectura distribuida, que permita de forma flexible la distribución del procesamiento de la información y el control entre los puntos de procesamiento en la red con subniveles de red (subestaciones, CTs, CGPs, CNs).

7.9.1. Gestión local de la demanda

La gestión activa de la demanda se podrá implementar en los CNs mediante funcionalidades de limitación de consumo, mientras no existan otras plataformas de gestión comerciales que permitan la modulación inteligente de las cargas de los distintos equipos del cliente.

La funcionalidad de gestión "activa" de la demanda ante la detección de situaciones de red con incidencia inminente por sobrecarga en líneas de BT que provocarían con gran probabilidad la fusión de fusible (a futuro apertura de interruptor).

Las futuras plataformas de flexibilidad "comercial" permitirán realizar esta gestión de congestiones de forma planificada y en la operación optimizando los recursos disponibles y previamente "contratados" con clientes y/o agregadores. El escenario de definición de esta funcionalidad es previo a esta capacidad de gestionar ofertas de flexibilidad. Sin embargo, aun disponiendo de estas futuras plataformas, podrían llegar a producirse situaciones de red de "emergencia" local o en redes superiores (situación a determinar por el Operador de Red, DSO / TSO), en las que, por la inminencia de incidencias, el DSO tendría igualmente que actuar directamente sobre la demanda para evitar un incidente de mayor ámbito.

Por tanto, esta funcionalidad se considera necesaria en ambos escenarios, el inicial sin gestión comercial de flexibilidad y el final, con flexibilidad "insuficiente".

Las sobrecargas se detectarán a través de los eventos espontáneos de sobrecarga de la SABT/iCBT. Estos eventos/alarmas permiten actuar antes de que se produzca la fusión del fusible de la fase y por tanto una incidencia con corte de suministro a los clientes de la fase y los clientes trifásicos de la línea. Para evitar esta incidencia inminente se propone actuar sobre la demanda de los puntos de suministro, limitando la potencia de consumo en los CNs, o incluso en caso necesario, desconectando alguno de los CNs para evitar el corte de suministro a todos los conectados a la fase, el concentrador de datos se encargará del envío de las consignas de limitación a los CNs. El CN programa la potencia límite temporal para la actuación del interruptor del ICP para consu-

mo o inyección (signo positivo/negativo respectivamente) y anulando temporalmente las actuaciones sobre la potencia contratada.

La propuesta cumple con las especificaciones de plataforma de flexibilidad de USEF (https://www.usef.energy/), especialmente para el modo de operación de alerta (naranja), en el que el control de la flexibilidad la asume el DSO en condiciones de inestabilidad por incidentes, tormentas, falta de flexibilidad por error de previsión de energía renovable, de demanda, cambios atmosféricos...

7.9.2. Potencia de generación flexible

Ajuste de potencia de generación flexible (entre 0 y potencia máxima de exportación). Valor de máxima exportación neta flexible. La superación del umbral deberá realizar la apertura del contacto de conexión de la generación. Ese valor se modificará de acuerdo con:

- Contrato de flexibilidad de largo plazo (condiciones de conexión) con el DSO y/o agregador. Modificación de ajuste puntual.

La lógica de aviso y gestión será análoga a la de gestión activa de demanda.

7.9.3. Flexibilidad distribuida

La Supervisión de red junto con la Predicción de red (Flujos de carga) deberá monitorizar la red de BT y gestionar las restricciones en tiempo real y previstas (Control de red), enviando las consignas o solicitud de servicios de flexibilidad de los recursos distribuidos (DER) conectados en la red de BT con flexibilidad, es decir, proporcionando servicios a la red.

Flujo de cargas óptimo: Realizará la simulación de la utilización de flexibilidad de los DER para resolver las restricciones, identificando el servicio a solicitar basado en modos de funcionamiento y modelos de los DER simplificados.

7.9.4. Integración sistemas de almacenamiento

Los sistemas de almacenamiento energético son clave para garantizar la transición a una economía neutra en emisiones y la efectiva integración de las energías renovables en el sistema, ya que permiten guardar la energía en los momentos en que hay excedente para utilizarla cuando el recurso renovable es escaso o la demanda es elevada.

Las tecnologías de almacenamiento favorecen el desarrollo de nuevos modelos de negocio como los agregadores independientes o las comunidades de energías renovables, que impulsan el papel activo de los consumidores al permitir su participación directa en la gestión de su energía, integrándose en los mercados de flexibilidad de la misma manera que si de generación distribuida se tratase, por lo tanto, su gestión se realizará de manera análoga.

7.10. Movilidad, operación y mantenimiento de Red

La movilidad en este caso debe ser entendida como el servicio que de manera local en el CT se ofrece para dar soporte para el mantenimiento al operador que debe realizar alguna operación o maniobra de manera manual. De esta manera, se dispondrá de la posibilidad de reconocimiento local de activos y que mediante dispositivos móviles mostrarán detalles de parametrización, configuración y ayudas para su mantenimiento, enumerando cada paso a realizar en cada operación y dejándolo registrado tanto localmente como en el sistema central.

7.10.1. Acceso a datos inventario de manera local

Todos los elementos físicos y digitales serían posible tener identificados mediante códigos tipo QR, etiquetas NFCs o tecnologías similares que permita registrarlos en un terminal móvil antes de realizar cualquier maniobra, sustitución, manipulación, etc. sobre ellos. De esta manera se logra tener desde los despachos centrales, la seguridad que se va a actuar sobre los elementos correctos, al tenerlos identificados de manera unívoca, aportando una clara mejora en la protección de la seguridad física de los operarios locales.

Además de permitir identificar cada elemento de manera local, también permite añadir información extra de cada elemento, tanto de inventario, ayudas, parametrización, etc. Y quedarán registrados todas las maniobras manuales que se realicen sobre ellos, que servirán para tener en cuenta en otras funcionalidades (cálculo de vida útil, anomalías, actualización activos, etc.)

7.10.2. Realidad aumentada

Los servicios de realidad aumentada por medio de dispositivos móviles (gafas de Realidad Virtual o aplicaciones de Realidad Aumentada en el smartphone) cada vez se integran más en procesos y flujos de trabajo, sobre todo en casos donde la operación de la red se realice por terceros (empresas subcontratadas para mantenimiento) y con ello exista una elevada rotación de empleados y escasez de trabajadores expertos.

7.11. Ciberseguridad

La ciberseguridad en un requisito transversal a toda la arquitectura y tendrá que integrarse desde origen, tanto en el uso de protocolos seguros, gestión y administración de usuarios, firmado electrónico y gestión de certificados digitales, uso de algoritmos critpográficos, así como control de las mejores prácticas en el desarrollo, programación e implementación de algoritmos y aplicaciones.

Con esta arquitectura además se permitirá desplegar aplicaciones que realicen monitorización de cumplimiento de todos los requisitos de ciberseguridad anteriores e incluir la monitorización y análisis de los procesos en ejecución, estados, uso de memoria, tráfico, conexiones establecidas, acceso a datos, etc... y localizar anomalías que puedan suponer un intento de ataque o ejecución algoritmos mal intencionados. Ya existen en el mercado multitud de empresas y aplicaciones que desarrollan este tipo de vigilancia de ciberseguridad distribuida, incluyendo mecanismos de aprendizaje (Machine Learning) e Inteligencia Artificial.

Se podrá también añadir capacidades de engaño que simulará una entidad o recursos falsos (a modo de señuelo) que un posible atacante tratará de atacar en vano y por lo tanto será detectado y permitirá realizar las actuaciones necesarias para su desactivación.

Todos estos mecanismos de detección serán notificados también de manera segura, siguiendo protocolos de log (tipo Syslog) manteniendo actualizado la información en un SIEM de la distribuidora.

En entornos distribuidos como el que estamos tratando, donde se tratan gran variedad de datos, muchos de ellos incluso se podrían considerar privados, existen nuevos riesgos de conservación de la privacidad a pesar de que la transferencias de información como el almacenamiento sea cifrado, sobre todo cuando el intercambio de datos se realiza con dispositivos físicos externos, por lo que deberá cuidarse la integridad de dispositivos físicos para que no sean suplantados (ejemplo una cámara de video), para lo que se debería usar contramedidas como tecnologías basadas en huellas hardware, etc.

En este entorno se deberían implantar medidas de protección a nivel de dispositivo y tecnología PUF anti-falsificación. Todo modelo de amenazas define las amenazas que tienen que ser consideradas y aquellas que no. Un ataque es una instancia de una amenaza, que viola las propiedades de seguridad de un sistema (como confidencialidad, integridad, disponibilidad, autenticación, no repudio, trazabilidad, frescura de información, control de acceso, etc.). Se debe tener siempre presente el costo en relación al beneficio a la hora de implantar medidas de seguridad. El responsable de mantener las políticas de seguridad es el componente trusted (de confianza). La confianza (trust) debe estar en la raíz del hardware (establecido en el encendido del sistema en base a hardware root-of-trust extensible a chain-of-trust). Fidedigno es aquello diseñado para ser seguro. TCB (Trusted Computing Base) es el hardware, software, firmware y componentes de red que deben ser tanto correctos como no corrompibles para poder asegurar que la política de seguridad no se viole. TEE (Trusted Execution Environment) es un área segura de almacenamiento de procesador que garantiza que el código y los datos allí localizados se encuentren protegidos (por ejemplo, respecto a confidencialidad, integridad, disponibilidad, etc.).

7.12. Seguridad y sostenibilidad

En este apartado se trata la seguridad desde el punto de vista físico, como el control de acceso, monitorización de parámetros ambientales o monitorización de incidencias de los activos físicos (desgastes, aislamientos, fugas, etc...). Generalmente los Centros de Transformación son infraestructuras ubicadas en localizaciones remotas no vigiladas y son vulnerables a daños accidentales, ataques de delincuentes con malas intenciones, así como

trabajos programados de personal propio que pueden cometer errores por falta de información o control y poner en riesgo su propia integridad, la del centro y o el medio ambiente.

La sostenibilidad es parte intrínseca y transversal a todas las funcionalidades descritas en este documento y causa por la que se requiere una solución de procesamiento distribuido que permita de una manera ágil la incorporación de nuevos requerimientos y actores que aportarán a la descarbonización de la economía y a la consecución de los objetivos de desarrollo sostenible (ODS). Aunque en este apartado se considera la medida de sostenibilidad del propio CT y la red de BT, mediante la reducción de consumo de los equipos electrónicos (reduciendo el número de equipos y optimizando su consumo), alargando la vida útil de los activos, teniendo en cuenta la sensórica para reducir riesgos de fugas de gases y aceite, riesgos de incendio, inventariado y seguimiento de proceso de reciclaje de activos, etc.

7.12.1. Control de acceso inteligente

El control de acceso inteligente no se trata simplemente de la instalación de un dispositivo IoT tan puesto de moda como es el "Smart lock" que permite abrir una puerta sin necesidad de una llave, sino por identificación de la persona, que podría realizarse mediante un código enviado al operario desde el despacho central, tras la concesión del acceso, o validación de su código NFC, etc... Pero además de permitir el acceso al personal indicado al CT, también será necesario identificar que va equipado con los EPIs correctos y actualizados, que podrían detectarse a la entrada mediante tecnología RFID, al igual que se realiza con el inventariado de equipos.

Otro método a incluir es el control mediante video vigilancia e integrar algoritmos de Inteligencia Artificial (AI) para detección de personal y que van equipados con sus correspondientes EPIs (detección de casco, guantes, botas, etc...).

7.12.2. Detección anomalías CT

A través de los dispositivos de Supervisión y concentrador de datos del CT recibirá los datos de los equipos de sensórica: fuego, inundación, temperaturas, corrientes, acceso..., realizará un procesado para detectar valores anormales de alarma, informará al Sistema central y realizará acciones de control en el caso de que se encuentren programadas.

La supervisión del CT también podrá analizar mediante técnicas avanzadas los datos de funcionamiento de los equipos generales y particulares de un equipo con el objeto de determinar el estado de salud dinámico del mismo y poder detectar riesgos de fallo más o menos inminentes generando bien actuaciones automáticas para protegerlo, bien alarmas para iniciar posibles actuaciones preventivas.

Pendiente la definición de la necesidad y la especificación de las estrategias a implantar para la gestión del CT como activo y de los equipos:

- Confirmación de fuego y/o inundación: desenergización mediante desconexión de equipos.
- Confirmación de alarma de temperatura: diferenciales en más de una zona.
- Gestión de acceso: activación de barreras virtuales, control de personal, desenergización.
- Cálculo dinámico de riesgo de fallo de equipamiento crítico y gestión de actuaciones preventivas.

7.12.3. Tratamiento de imagen

Otro método que con toda seguridad requeriría mucha mayor capacidad de procesamiento, es el uso de cámaras de video vigilancia para detección de anomalías, control de acceso, cámaras térmicas para detección de puntos calientes, etc. que deberán integrar algoritmos de Inteligencia Artificial (AI) que obligará a dimensionar los equipos electrónicos con capacidad suficiente de procesamiento para soportar estos nuevos requerimientos.

A pesar de esto, disponer de los procesos algorítmicos junto a los dispositivos de vigilancia permite detectar y procesar actividades sospechosas en tiempo real, reduciendo al mínimo el almacenamiento de imágenes y grabaciones.

8. PROYECTOS PILOTOS EN CURSO Y POC

8.1. Introducción proyectos pilotos y PoC incorporados

En este capítulo se pretende recopilar los diferentes proyectos o pilotos en los que los diferentes colaboradores de esta edición han participado, relacionado con funcionalidades desplegadas en el entorno del centro de transformación o tecnologías de procesamiento distribuido, con el objetivo de compartir experiencias y detectar intereses comunes, tecnologías comunes y por lo tanto objetivos comunes, que posibilite nuevos ámbitos de colaboración.

A continuación, se enumeran los proyectos en curso o realizados que los diferentes colaboradores del presente documento y breve descripción del objetivo principal de cada uno de ellos:

Piloto	Objetivo	Promotor
E4S-SSP	Definición de un estándar abierto para soluciones de centros de transformación de MT a BT Como proceso de definición de dicho estándar se desarrolla un pilotaje utilizando la plataforma denominada Secondary Substation Platform (SSP)	E4S
MiDE4S	Se trata de un proyecto piloto que permita confirmar (PoC) la viabilidad de un posible despliegue de arquitectura de procesamiento distribuido. Para lo que se ha dividido en diferentes fases o hitos, que permita comprobar desde el concepto de despliegue de aplicaciones desde un entorno IT (cloud Azure) a dispositivos OT (nodo inteligente junto dispositivos legacy), así como la adaptación e interoperabilidad del nuevo dispositivo con los protocolos actualmente en uso. En una segunda fase se ha trasladado tanto el servidor de gestión y despliegue de aplicaciones como el Nodo Inteligente (PC industrial) a un entorno de laboratorio seguro de iDE, habilitando conexiones con CTs reales para recibir datos de los equipos (CD y SABT) de los centros y permitir ejecutar aplicaciones y operaciones simulando como si estuviera el Nodo Inteligente en el propio centro, que sería el paso antes de la instalación de un dispositivo que cumpla los requerimientos físicos para instalarse en un CT (colaboración con hardware de CIRCUTOR). Si bien en esta fase del proyecto se ha enfocado más en la evaluación tecnológica (ciberseguridad, interoperabilidad, especificación requerimientos, conservación propiedad intelectual entre aplicativos, etc.) también se ha logrado desplegar y probar una serie de funcionalidades tanto desarrolladas internamente por Minsait (Interfaz STG-CD para comunicar con CD de manera local, algoritmos de regulación y cálculo de toma óptima, algoritmo de balance energético, interfaz comunicación DLMS con tarjetas i-Trafo e i-CBT, etc..) como por empresas externas (algoritmo detección conectividad CNs de ARIADNA), manteniendo los requerimientos de interoperabilidad necesarios.	i-DE
CT 4.0 Unión Fenosa Distribución	Este despliegue incluye la definición, desarrollo/configuración y prueba de casos de uso avanzadas de supervisión y control de la Baja Tensión y una primera definición de impacto de negocio y evaluación de la rentabilidad de su aplicación masiva. Los objetivos de la primera fase del piloto, ya completada eran los siguientes:	UFD

	1. Despliegue y verificación de arquitectura Onesait Edge en laboratorio UFD y CT en campo. 2. **Prueba de concepto** de casos de uso mediante la programación de lógicas de monitorización y control en forma de dockers. 3. **Integración con equipos existentes:** Concentrador de Datos y Supervisor de Baja tensión, mediante protocolos soportados fundamentalmente PRIME-STG. 4. **Gestión del nodo y contenedores central** a través de sistema Onesait EMS (Edge Management System) en zona 3. 5. **Verificación de modelo de negocio.** Estimación de impacto de la nueva arquitectura propuesta y proyección de costes de despliegue, operación y mantenimiento. 6. Definición de escenario de pruebas para la **estandarización** de esta nueva arquitectura. 7. Piloto coordinado con el grupo de trabajo de Futured y estará coordinado con otros pilotos a realizar dentro del grupo de trabajo.	
Integración de protocolos industriales en el CT a través de dispositivos IoT en el Edge	El objetivo del piloto es demostrar la posibilidad de instalar un nodo de computación Edge que sea capaz de: 1. Integrar múltiples protocolos de comunicaciones con dispositivos del CT. 2. Correr algoritmos localmente para el tratamiento de datos, paquetizados en contenedores Docker. 3. Ser gestionado remotamente para poder actualizar el firmware (drivers, protocolos de comunicaciones, otros) y el software (contenedores Docker) sin la necesidad de disponer de personal en el CT ser gestionado remotamente para poder actualizar el firmware (drivers, protocolos de comunicaciones, otros) y el software (contenedores Docker) sin la necesidad de disponer de personal en el CT.	Grupo Cuerva
Proyecto DISCOVERER (2018)	Control de la tensión mediante la operación coordinada del smart transformer (master) con los inversores conectados a la red de BT. El objetivo del proyecto se centró en ensayar y evaluar en un laboratorio (Fraunhofer IEE - SysTec) diferentes algoritmos de control de la tensión que permitiesen mejorar la integración de las energías renovables en la red de BT.	Ormazabal
Proyecto HOLISTICA (2019)	Operación coordinada entre el smart transformer (master), los inversores, las baterías y la carga del VE. El objetivo del proyecto se centró en ensayar y evaluar en un laboratorio (DTU-Syslab) diferentes algoritmos de control de la tensión que permitiesen: 1. Mejorar la integración de la generación renovable distribuida y del VE en la red de BT. 2. Reducir las pérdidas de la red de BT. 3. Mejorar la vida útil de los equipos mediante la optimización de su operación.	Ormazabal
POC100 Edistribución	Dentro del proyecto COORDINET y en el ámbito de la Smart City de Málaga se encuadra el proyecto de sensorización POC100. Los objetivos han sido incrementar la capacidad de integración de energías renovables distribuidas y de nuevas cargas como el VE, reducir las pérdidas en la red de BT y mejorar la vida útil de los equipos con capacidad de operar la red de BT. Todo ello a través de la monitorización de una serie de CTs.	E-Distribución

8.2. Descripción proyectos pilotos y PoC incorporados

8.2.1. Pilotos E4S Alliance - SSP

Edge for Smart Secondary Substation Solutions (E4S) tiene como objetivo la definición de un estándar abierto para soluciones de centros de transformación de MT a BT. Como proceso de definición de dicho estándar se desarrolla un pilotaje utilizando la plataforma denominada Secondary Substation Platform (SSP).

8.2.1.1. Descripción y alcance del piloto

De entre todos los casos de uso contemplados se han seleccionado dos casos que interaccionan con dispositivos de campo y dos casos más que procesan la información de los anteriores:

1. Concentrador de datos de medida de contadores.
2. Supervisión avanzada de baja tensión.
3. Conectividad de contadores para determinar la topología de la red de BT.
4. Detección temprana de interrupciones de suministro en la red de BT.

Las aplicaciones residen en un único equipo en el que disponen de todos los recursos necesarios para obtener los datos de campo, almacenarla, procesarla y poner la información a disposición de los sistemas de IT/OT (La solución proporciona interfaces con sistemas IT/OT como el MDC, OMS, GIS y ADMS) e incluso actuar localmente.

Platform	Apps	Objectives
• One to one Comms *FTP & WS*	DCU *ZIV/CIR*	1. Run Containerized Apps 2. Study container Resources 3. Container Deployment config
• Node Orchestration • Internal Comms *(MQTT & REST)*	LVSup - AdLVS *Merytronic* AdLVS *Merytronic*	1. Test WOT/MQTT 2. Node Orchestration Mgmt. 3. Study cluster resources
• Full Orchestration • Shared Resources	Topology *Ariadna* Outage *L&G*	1. Shared DBs 2. Full Orchestration 3. App deployment strategy 4. Test deployment timings and recovery modes
• Cybersecurity • External Comms	Separation *LVSup - AdLVS*	1. Implement cybersecurity policies 2. Integration with IB Systems 3. DCU and adLVS migrate to WOT Schema
• Full System	New Apps?	1. Run full substation model 2. Test Pre-Production-Commercial HW

8.2.1.2. Arquitectura

E4S ha definido una nueva arquitectura flexible y modular basada en un hardware multifunción y una plataforma software.

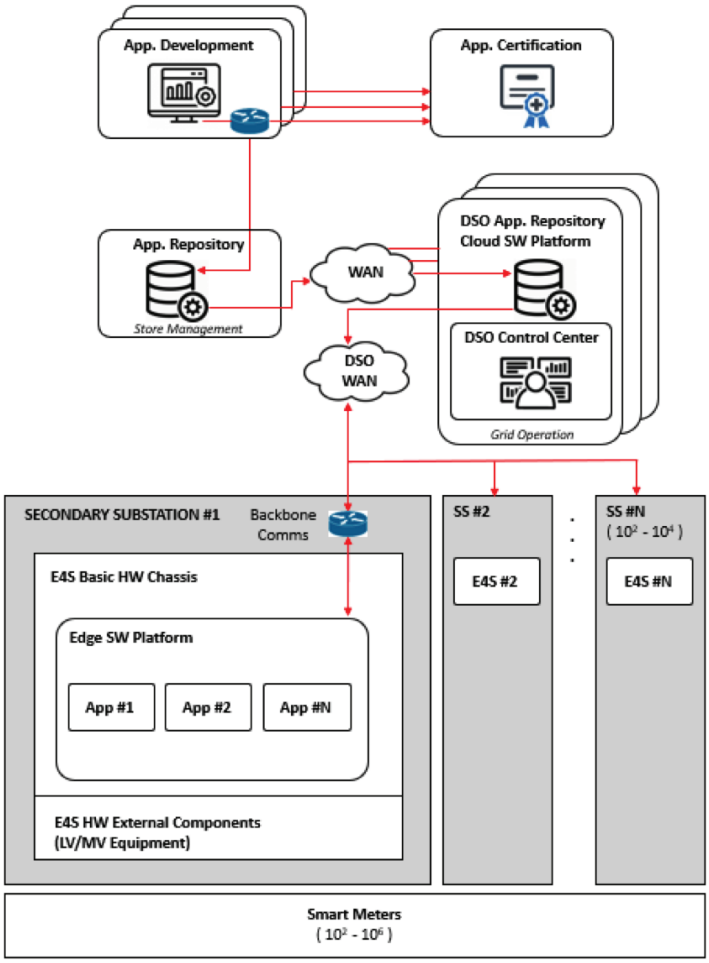


Figura 103: Arquitectura E4S.

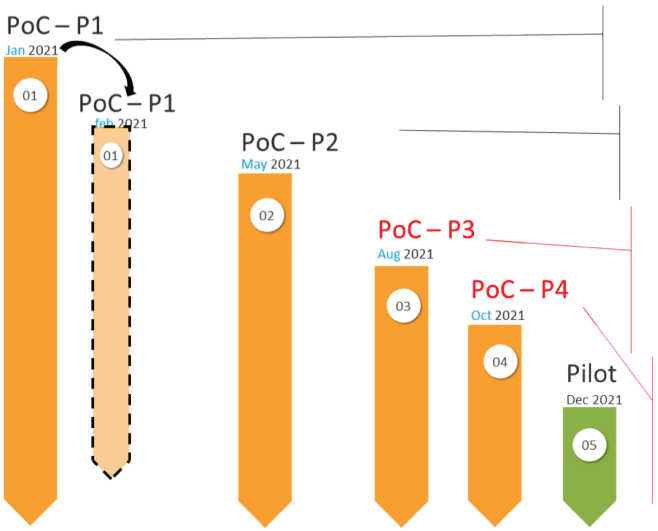
8.2.1.3. Tecnologías

La arquitectura del sistema se define a partir de estándares abiertos de containerización de aplicaciones, protocolos de comunicaciones IoT y WoT y modelos de datos en uso en despliegues existentes.

8.2.1.4. Participantes

Figura 104: Participantes E4S.

8.2.1.5. Roadmap



Platform	Apps	Objectives
• One to one Comms *FTP & WS*	DCU *ZIV/CIR*	1. Run Containerized Apps 2. Study container Resources 3. Container Deployment config
• Node Orchestration • Internal Comms *(MQTT & REST)*	LVSup - AdLVS *Merytronic* AdLVS *Merytronic*	1. Test WOT/MQTT 2. Node Orchestration Mgmt. 3. Study cluster resources
• Full Orchestration • Shared Resources	Topology *Ariadna* Outage *L&G*	1. Shared DBs 2. Full Orchestration 3. App deployment strategy 4. Test deployment timings and recovery modes
• Cybersecurity • External Comms	Separation *LVSup - AdLVS*	1. Implement cybersecurity policies 2. Integration with IB Systems 3. DCU and adLVS migrate to WOT Schema
• Full System	New Apps?	1. Run full substation model 2. Test Pre-Production-Commercial HW

Figura 105: Roadmap E4S.

8.2.2. Proyecto MiDE4S (Minsait-iDE)

8.2.2.1. Alcance y objetivos

El objetivo del proyecto ha consistido en pilotar primero a nivel laboratorio y segundo en dos centros de transformación (CT) en operación real, una solución de procesamiento distribuido basado en despliegue de aplicativos, primero sobre hardware industrial disponible en mercado (para prueba de concepto en laboratorio), y segundo en hardware homologado (para instalación en CTs reales), gestionado desde un sistema central (basado en cloud) para despliegue de aplicaciones basados en arquitectura de microservicios (mediante contenedores o virtualización ligera) y el desarrollo de aplicaciones con capacidad de monitorización, análisis y control automático e inteligente en tiempo real a los cambios en la red, dando de esta manera respuesta a los nuevos desafíos en la red de baja tensión descritos anteriormente.

El proyecto se ha dividido en cuatro fases:

Fase I: Despliegue y verificación a nivel laboratorio de desarrollo toda la arquitectura de CT Inteligente, tanto a nivel de nodo-edge como de plataforma cloud. Nivel prueba de concepto con desarrollo de aplicativo básico analítico (balance de cargas), sobre datos obtenidos de concentrador de datos, considerado como elemento terciario.

Fase II: Despliegue y verificación a nivel laboratorio de integración (instalaciones de distribuidora iDE) de toda la arquitectura de CT Inteligente y su evaluación desde el punto de vista de Ciberseguridad, integrando elementos de campo tales como el concentrador de datos mediante accesos de red (obtención de datos reales) y aplicaciones desarrolladas por terceras empresas, por ejemplo, algoritmos de análisis topológico desarrollados por la empresa Ariadna.

Fase III: Despliegue y verificación en dos CTs bajo operación real la solución implementada con especial interés las funcionalidades de regulación y cálculo de toma óptima de transformador con regulador de carga. Este despliegue por requisitos de seguridad y aislamiento eléctrico se deben realizar sobre equipamiento hardware certificado, para esta prueba de concepto se cuenta con la participación de la empresa Circutor quien proporciona estos equipos sobre los cuales se despliega todo el aplicativo de monitorización y control.

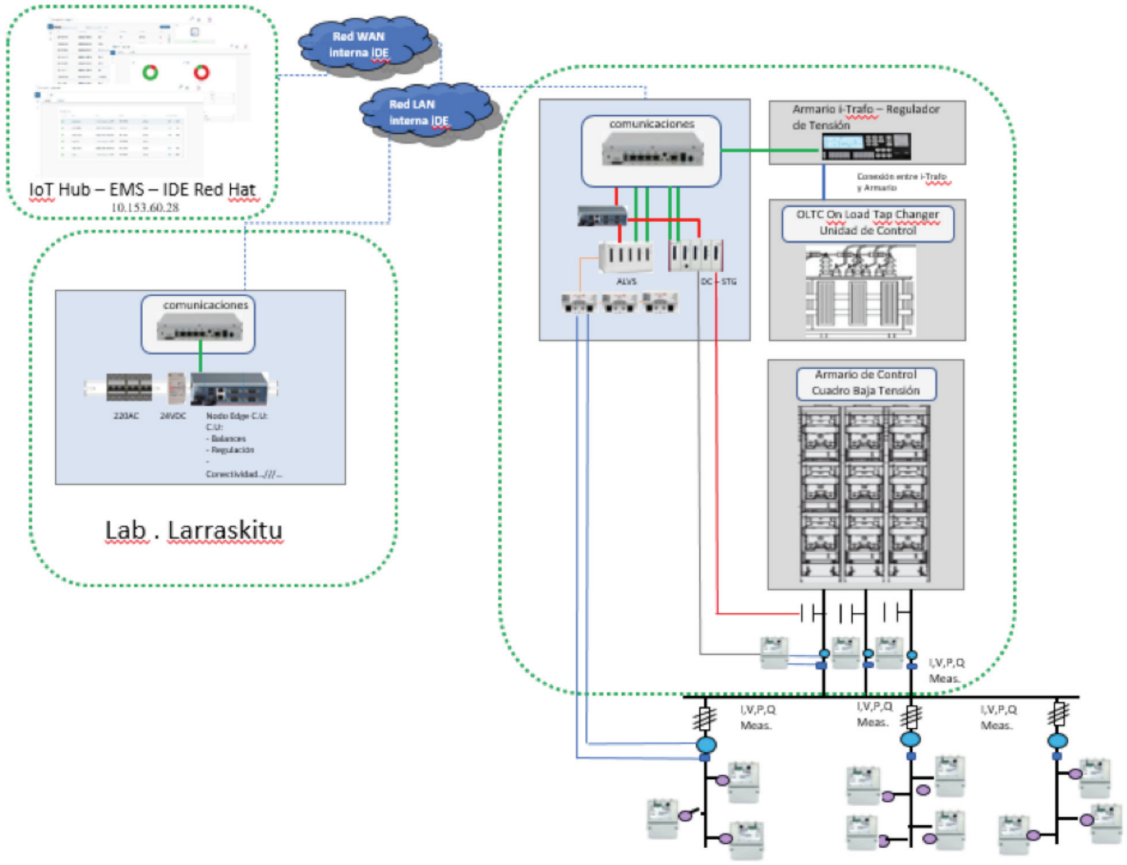


Figura 106: Esquema Físico del Proyecto.

Fase IV: Fase de análisis de resultados de monitorización y control, recursos consumidos, estudio de eficiencia, evaluación de coste de solución unitaria y previsión de coste según escalabilidad.

8.2.2.2. Descripción solución desplegada

La solución que se plantea en este proyecto (Prueba de Concepto) se basa en el concepto de nodos de computación distribuida que conforman una capa de inteligencia en el borde (Edge) de la red para la ejecución de algoritmos, análisis y toma de decisiones de manera local en lugar de procesar todo en los Centros de Control en base a una arquitectura centralizada, y supervisado desde una plataforma cloud orientada al despliegue y gestión de dichos nodos.

El esquema que se presenta a continuación muestra la solución desplegada por Minsait en el marco del proyecto de Centro de Transformación Digital con Iberdrola.

El primer elemento que forma parte de la solución desplegada lo constituye la Onesait Platform, plataforma de desarrollo y operación, potente y escalable para IoT/Edge Computing, IA y otras soluciones digitales. Onesait Platform brinda la flexibilidad para que los desarrolladores puedan construir sus propias soluciones de una manera sólida y ágil utilizando tecnologías "Open Source", bajo una arquitectura flexible y un enfoque innovador.

Dentro de Onesait Platform, el elemento principal empleado en el proyecto es Things IoT/ Edge HUB. Este componente dentro de Onesait Platform proporciona las funciones de gestión distribuida de cargas de trabajo para Edge Computing. Things IoT7Edge HUB habilita un entorno virtual de aplicaciones (empaquetadas en contenedores) gestionado y securizado, permitiendo el despliegue de un amplio espectro de aplicaciones y casos de uso distribuidos que se conectaban en tiempo real a dispositivos y sensores en campo (mediante protocolos estándar en el sector SGT, IEC, etc).

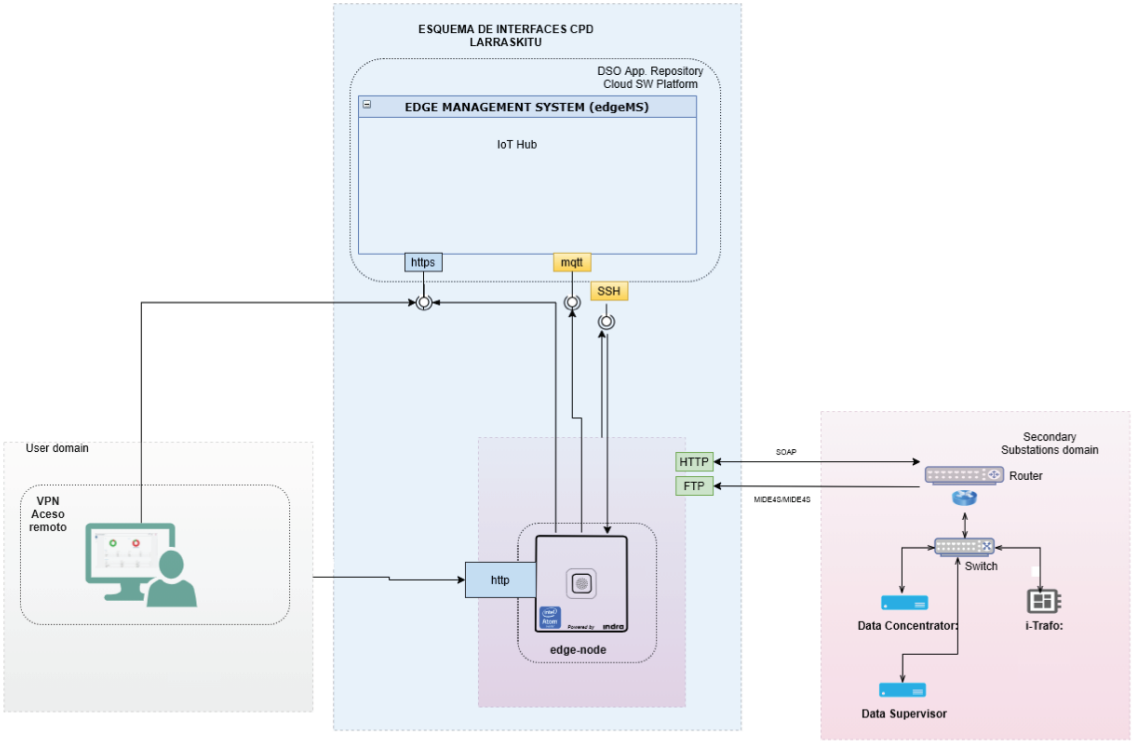


Figura 107: Esquema Lógico de la Arquitectura Fase II.

Things sigue un esquema de comunidad de agentes (Edge Agent), estos agentes están integrados en el SO (disponible para distintas distribuciones de Linux) de los dispositivos Edge Devices y son los encargados de establecer y mantener la comunicación con la plataforma. Para grandes despliegues, estos agentes se instalan durante el proceso de producción de los equipos y confía en TPM (Trusted Platform Module) (1.2 o 2.0) para administrar las distintas credenciales que proporcionan ciberseguridad end-to-end contra una infraestructura PKI (Public Key Infrastructure) con "auto-enrollment". Para la creación rápida de prototipos, caso del actual proyecto, el agente se descarga e instala localmente en una máquina tipo Linux (en el proyecto actual la distribución empleada es Clear Linux de Intel©); realizando un proceso de "enrollment" por operador a través de un token de conexión de seguridad que es servido desde la propia plataforma en un formato seguro.

El último elemento lo constituye el nodo Edge Device, este nodo de computación es el encargado de implementar los diferentes casos de uso definidos en el proyecto, microservicios en contenedores encargados de adquirir la información de elementos de campo, su proceso, implementación de algoritmia avanzada y control de dispositivos externos de una manera distribuida y autónoma. Como se ha comentado la implementación se ha realizado vía contenedores docker (aunque otros runtime de contenedores son también gestionables por Onesait Edge Agent como los basado en podman, microk8s, k3 o k8s completos). Las ventajas de emplear orquestación de cargas trabajo (aplicaciones) basada en contendores, son muy variadas, siendo especialmente importante la reducción del tamaño del software, limitación del ancho de banda y el uso optimizado de recursos de CPU y memoria.

Los contenedores implementados en el proyecto constituyen aplicaciones aisladas conectadas entre sí mediante un "broker" de mensajería MQTT (v.3.0) proporcionado por defecto dentro de la arquitectura gestionada por el Onesait Edge Agent.. MQTT (Message Queue Telemetry Transport) es un protocolo diseñado como un transporte de mensajería de publicación/subscripción extremadamente liviano

ideal para conectar aplicaciones/dispositivos con un ancho de banda mínimo. Aunque MQTT es agnóstico del formato del "payload" intercambiado, la opción más generalizada es su uso empleando JSON como formato de datos. El principal objetivo buscado con esta decisión es facilitar la interoperabilidad entre las diferentes aplicaciones. Adicionalmente, la interacción entre los distintos microservicios puede seguir una estructura Petición/Respuesta utilizando mecanismos RESTfull cuando es necesario .

8.2.2.3. Arquitectura

La arquitectura implementada se basa en la construcción de un conjunto de contenedores divididos en dos grupos:

1. **Contenedores de infraestructura:** proveen servicios básicos como la comunicación entre contenedores a través de MQTT, base de datos temporal y seguridad local.
2. **Contenedores de aplicación:** contenedores que encapsulan aplicaciones como protocolos de bus de campo o modelos de IA. Las principales aplicaciones implementadas en el proyecto han sido las siguientes:

STG-DC-Connector: Esta aplicación es la responsable de comunicar con los concentradores de datos mediante implementación de protocolo STG-DC, actuando como STG secundario para recoger toda la información adquirida por los concentradores proporcionada por los contadores a través del protocolo PLC PRIME.

El protocolo utilizado STG-DC, está basado en "Web Services" (implementados bajo SOAP) y envío de ficheros FTP, para lo que también es necesario habilitar y configurar una segunda IP de STG y FTP en cada concentrador con el que comunique (funcionalidad solo disponible en firmware de concentradores del fabricante CIRCUTOR)

A este contenedor se le ha añadido la capa de adaptación al estándar Web of Things de la W3C. Gracias a esta capa, el contenedor STG-DC-Connector puede ser consumido como Digital Twin (activo digital) del concentrador STG-DC físico, habilitando sus capacidades actuales (configuración, alarmas, eventos y operación) y extendiendo las mismas con nuevas como el "plug-in-play" y el autodescubrimiento.

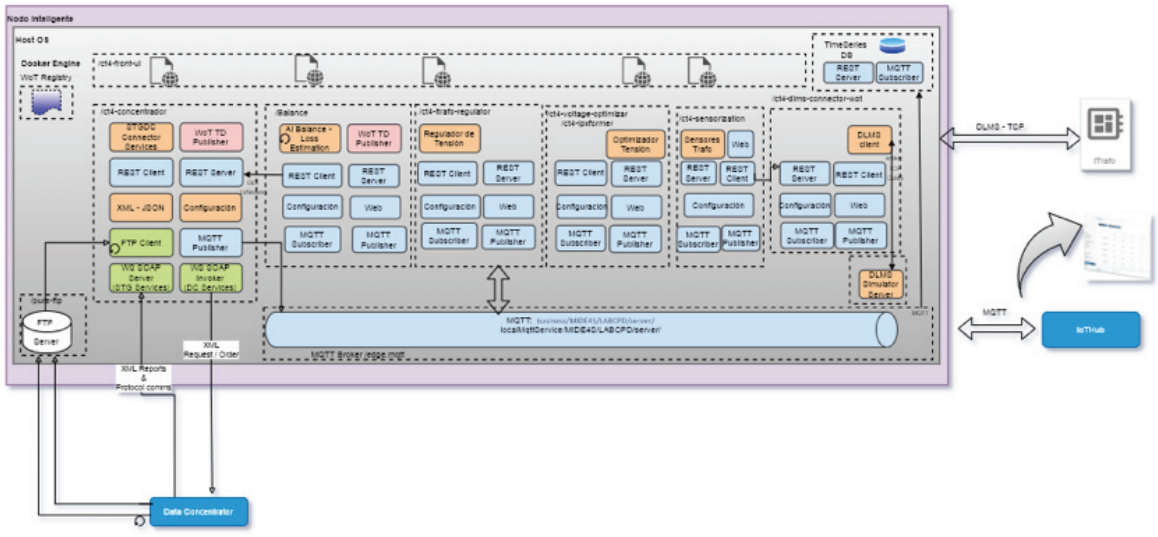


Figura 108: Esquema Lógico Arquitectura nodos inteligentes.

Balances: Uno de los objetivos de esta PoC ha sido la implementación de un algoritmo que calcule los posibles desbalances energético en un Centro de Transformación, a partir de esta información y de los datos almacenados, procesados a partir de los puntos de suministros y de la información suministrada por los supervisores poder detectar las causas de dichos desbalances.

La información de curvas de carga de CNs y supervisor (informe S02) requerida para la ejecución de este algoritmo es recibida desde los concentradores configurados a través del protocolo STG-DC, implementado a través de contenedor STG-DC-Connector.

A este contenedor se le ha añadido la capa de adaptación al estándar Web of Things de la W3C. Gracias a esta capa, el contenedor Balance puede ser consumido como Digital Twin (activo digital).

Regulación con optimización de voltaje: Esta aplicación monitorea los parámetros de BT del transformador y regula la tensión de salida para adaptar la calidad de la energía al estado de la red. Utiliza información de datos de valores instantáneos (informe S21) proveniente también del Concentrador de datos vía STG-DC-Connector. Proporciona una interfaz con el controlador del transformador para modificar la salida del transformador. Se utiliza cuando se instala un transformador OLTC en el centro de transformación.

El control del CT **(iTrafo-Regulator)** actuará sobre la regulación del transformador subiendo o bajando tomas en función de la tensión de la red de BT aguas abajo del trasformador.

El CT determinará la toma óptima del transformador teniendo en cuenta el dato de tensión en la cabecera a través de la monitorización del supervisor y de las LBT, pero sobre todo la tensión en los puntos de suministro a través de los informes de tensiones instantánea de los contadores, esta toma optima es calculada a través del contenedor **(voltaje-optimizer)**.

Sensorización: El transformador inteligente integra una serie de sensorización necesaria para vigilar el estado de salud de este, mediante el contenedor "sensorization" el nodo captura dichas medidas analógicas y las disponibiliza para futuras aplicaciones como por ejemplo aquellas asociadas al mantenimiento predictivo.

Por último, se ha desplegado el contenedor "**DLMs connector**" con objeto de comunicar el nodo con la tarjeta electrónica de control del transformador, este Docker ha implementado además de toda la capa de enlace necesaria, los objetos privativos de control en este dominio de aplicación.

Entre los contenedores de infraestructura se han desplegado utilidades de Graphana (aplicación web de visualización interactiva y analítica

Figura 109: Métricas de validación.

de código abierto multiplataforma) con objeto de representar gráficamente y validar los requerimientos de proceso y comunicaciones de la máquina.

Con el mismo objetivo de representar y validar la funcionalidad de las diferentes aplicaciones (contenedores) se ha utilizado Chronograf (de la suite Tick Stack) como herramienta de verificación funcional de datos.

8.2.2.4. Beneficios de la solución.

Desde la perspectiva de las redes inteligentes, esta prueba de concepto aporta una serie de ventajas y beneficios para la gestión de la misma, permitiendo identificar y resolver en "cuestión de segundos" situaciones de riesgo para el suministro eléctrico gracias a la combinación de tecnologías 'cloud' con capacidades 'edge' de monitorización y operación en tiempo real, suponiendo además el "elemento central" para una operación más dinámica, segura y eficiente de la red de baja tensión. Estos aspectos permitan afrontar con seguridad la penetración de generación renovable, infraestructuras de recarga del vehículo eléctrico y los nuevos modelos de gestión de energía.

Este tipo de solución aporta unos ahorros en los costes y mejora de la calidad del suministro: se estima que pueden facilitar reducciones del 80% del 'time to market' en la implementación de nuevos servicios para adaptarse a las necesidades de consumo o producción de energía de los clientes, en los análisis preliminares realizados para la estimación de tiempo y esfuerzo necesario para el desarrollo de aplicaciones en base a microservicios se están obteniendo reducciones muy significativa sobre todo en los tiempos de desarrollo y despliegue.

También se prevén ahorros del 30% en los costes de gestión y mantenimiento del centro de transformación, incrementos de un 10% en el aprovechamiento de la producción renovable distribuida o mejoras del 20% en los índices de calidad del suministro de baja tensión.

Así, este nuevo SASCTI permite simplificar la arquitectura de los centros de transformación actuales, integrando en su estructura otros dispositivos digitales, como el concentrador de medidas o la Unidad Terminal remota (RTU), en este sentido Minsait está participando en un alianza (E4S Alliance) conjuntamente con Iberdrola, Ariadna Grid, Intel, Merytronic, ZIV, Nebbiolo Technologies, Landys Gyr y Circutor con el objetivo de acelerar la creación de una arquitectura basada en estándares, abierta, interoperable y segura, que abarque los retos técnicos y comerciales a los que se enfrenta la red eléctrica del futuro. Toda la arquitectura utilizada en este proyecto está alineada con las especificaciones y acuerdos alcanzados en esta alianza.

La integración de otros dispositivos digitales permitiría ahorros evidentes al contar con menos equipamiento y al mismo tiempo hasta un 25% en disminución de consumos, apoyando los objetivos de eficiencia energética y sostenibilidad propuestos en la iniciativa de la UE Agenda 2030.

Por último, cabe destacar que esta prueba de concepto del Centro de Transformación Inteligente (SASCTI) ha sido premiado en la VIII edición de los enerTIC Awards 2020, en la categoría de 'Intelligent IT Infraestructures'.

8.2.2.5. Conclusiones

Uno de los principales objetivos del proyecto era la dotación a la red de baja tensión de unos nuevos equipos y funcionalidades con el propósito de transformar dichas redes en una infraestructura inteligente, evaluando una solución en base a un arquitectura distribuida con servicios implementados en nodos inteligentes que aseguren la escalabilidad y agilidad en la adopción de dichas nuevas funcionalidades, minimizando los tiempos de desarrollo y flexibilidad de implementación de nuevas necesidades (en base a microservicios de diferentes proveedores), asegurando la interoperabilidad entre las diferentes aplicaciones desarrolladas y cuyo despliegue sea posible en hardware abierto y de bajo coste, demostrado con la colaboración en el proyecto de las empresas Ariadna, mediante la ejecución del algoritmo de detección de conectividad, y de Circutor mediante la disponibilidad de la plataforma hardware basada en arquitectura del concentrador de datos y SABT con capacidades ampliadas.

Esta PoC ha validado que mediante la utilización de metodologías estándar tales como mensajería "MQTT", protocolos de

comunicación tales como DLMS o STG, formatos JSON o lenguajes de programación tales como GO, las diferentes funcionalidades necesarias para convertir la red de baja tensión en una red inteligente se pueden realizar desde un punto de vista interoperable, rápido y de bajo coste.

Queda aún camino que recorrer, por ejemplo, facilitar los problemas de integración entre las plataformas IoT/Edge con las aplicaciones desplegadas y entre ellas mismas haciendo uso del conjunto de estándares WoT (Web of Things). El uso de WoT-A proporciona al nodo edge una forma simple de interoperabilidad entre los servicios (o aplicaciones) implementados.

También es necesario extender los mecanismos de seguridad que protejan todos los activos de información desplegados e interconectados, asegurando al mismo tiempo la integridad de la información como su confidencialidad. El perímetro de exposición en este nuevo escenario es mayor al que se daba en las arquitecturas anteriores. Entre las futuras tareas que hay que acometer son tales como estudiar los mecanismos de cifrado necesarios para asegurar la protección de la propiedad intelectual, la detección de malware en tiempo de ejecución, la instalación de software integral de seguridad o el control exhaustivo de sesiones y puertos de accesos externo.

A nivel lógico también se pretende desplegar algoritmos que necesiten más recursos de máquina tales como algoritmos en base a inteligencia artificial (por ejemplo, aplicaciones orientadas al mantenimiento predictivo mediante tecnologías cognitivas dotando a los nodos distribuidos de capacidad de aprendizaje y detección de problemas de forma autónoma, o gestión de imágenes orientadas a la protección física de los equipos instalados. Estos despliegues además de proporcionar valiosa información funcional, también nos proporcionarán los requisitos de máquina a futuro.

8.2.2.6. Próximos objetivos

Como hemos visto el cambio en la estructura de generación eléctrica, con cada vez mayor participación de fuentes renovables, su mayor dispersión, maximizando la eficiencia de la red de manera global y permitiendo al mismo tiempo una reducción de costes siempre manteniendo o mejorando la calidad del suministro nos lleva a implementar funcionalidades avanzadas de control con objeto de regular el flujo de energía con los objetivos puestos en los puntos referenciados.

En esta prueba de concepto hemos integrado una plataforma embebida (Edgenode) dentro del Centro de Transformación para el despliegue de algunas estrategias de monitorización y control local, respetando una estructura de despliegue jerárquica (Onesait Platform) dentro del contexto de red inteligente.

Juntamente con las nuevas acciones propuestas previamente hay toda una serie de nuevas acciones necesarias de llevar a cabo con objeto de poder gestionar una red inteligente tales como:

- Necesidad de un marco de estandarización para la red inteligente:
  - o Existencia de una especificación basada en estándares que definan el marco sobre el que especificar nuevas funcionalidades o casos de uso mediante una metodología única.
  - o Existencia de una base de datos unificada a modo de "Companion", donde se registren cada caso de uso, sus interrelaciones y sus implementaciones (versiones).
  - o Interoperabilidad bajo normalizaciónW3C.
  - o Tecnologías semánticas en el dominio de las redes y los entornos inteligentes, con un enfoque particular en los cambios introducidos por dichas tecnologías en las arquitecturas, técnicas de programación y herramientas adoptadas.
  - o Uso de IEC Common Information Model (CIM) como estándar para permitir la integración de sistemas y el intercambio de información basado en un modelo de información común en el último tramo de comunicación con los dispositivos finales.
- Evaluación y mejora de las medidas de ciber seguridad bajo el nuevo entorno de control distribuido, integración e interoperabilidad

con servicios y sistemas proporcionados por diferentes proveedores y fabricantes.

- Implementación de nuevos algoritmos de control
  - o Algoritmos de análisis predictivo para respaldar la planificación eficiente y el control avanzado de las redes eléctricas en un paradigma de suministro y demanda de servicios públicos que cambia dinámicamente.
  - o Técnicas de Visión artificial orientadas al mantenimiento y seguridad.
  - o Técnicas de aprendizaje automático para la captura los patrones de consumo de los clientes, pronosticar la demanda de energía y la generación de energía de fuentes intermitentes y predecir fallas en los equipos.
- Análisis detallado de los futuros requisitos ante despliegues masivos
  - o Evaluación de necesidades hardware de acuerdo con los requisitos específicos de cada despliegue.
  - o Evaluación de necesidades software de acuerdo con los requisitos específicos de cada despliegue.
  - o Evaluación de técnicas de codificación, ejecución y bastionados acordes a los diferentes escenarios de despliegue.
  - o Requisitos y evaluación de plataformas de gestión de activos inteligentes distribuidos orientados a afrontar, entre otros, los siguientes desafíos:
    - Gestionar un conjunto de equipos y dispositivos extremadamente heterogéneo en términos de capacidades, funcionalidades, robustez y grado de seguridad.
    - Gestionar la diversidad de combinaciones de software y sistemas operativos que evoluciona constantemente con el tiempo.
    - La necesidad de combinar un conjunto cada vez más amplio de herramientas de gestión.
    - Gestión de un volumen cada vez mayor de información disponible
    - Difusión de la información a otros entornos cuyo acceso debe estar asegurado y protegido mediante diferentes mecanismos tanto para clientes internes como para proveedores externos.

8.2.3. CT4.0 UFD

El piloto se basa en la arquitectura hibrida Edge/Cloud y componentes de la plataforma Onesait Things de Minsait.

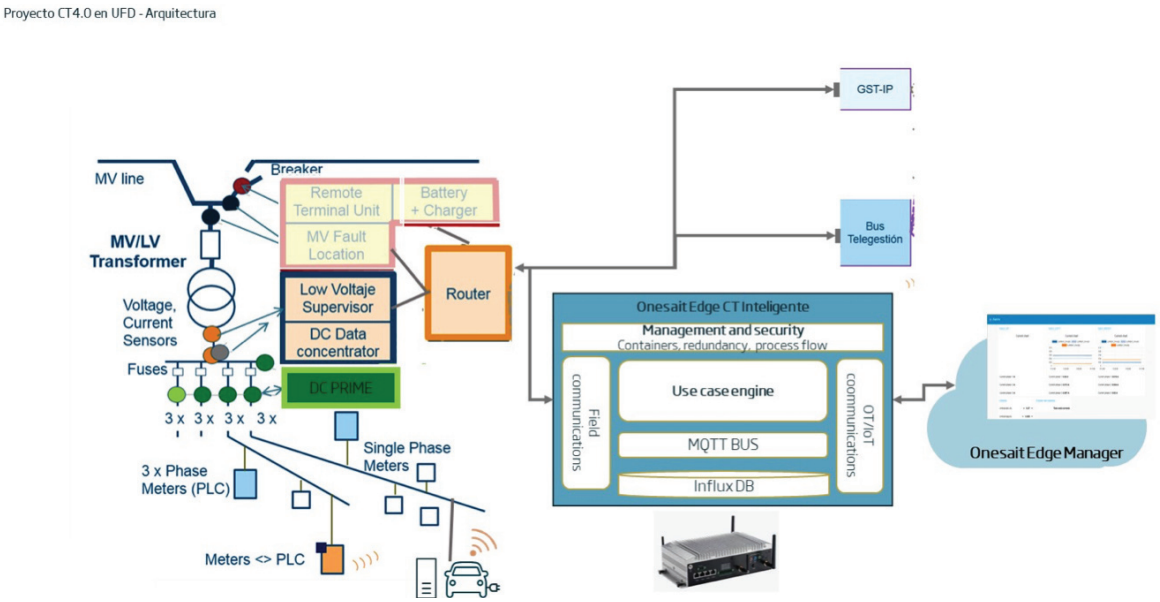


Figura 110: Arquitectura física UFD CT 4.0 Fase.

Esta plataforma se despliega en tres niveles:

- Dispositivos: Integración de dispositivos y de su gestión.
- Edge en este caso el CT 4.0.
- Data Center. Cloud o centro de control. En el piloto UFD CT 4.0 este Data Center está en zona 3 de Purdue, (zona de OT protegida de operación de red).

Figura 111: Arquitectura Lógica Nodo Edge UFD CT 4.0 Fase.

8.2.3.1. Funcionalidades

Detección de Rotura de neutro:

Detección del evento espontáneo de la rotura de neutro y mandar abrir (desconectar) a todos los clientes de alrededor (topología) que presenten una sobretensión.

Con la finalización de la OT que recupera el neutro se consulta el listado de suministros interrumpidos para recuperarlos.

Envío de entradas potenciales (listado de interrupciones) a gestión de reclamaciones para agilizar los tiempos de gestión de la reclamación.

Rotura de la fase en media tensión:

Monitorización de las redes de las tensiones en BT para inferir averías en MT.

Envío de alarma cuando existan fases de BT en subtension a la salida del transformador.

En el momento que la avería es subsanada los niveles de tensión recuperan el nivel nominal y esto al ser detectado por el nodo provocará el cese de la alarma.

Reinicio remoto de equipos

Monitorización de correcto funcionamiento de los equipos digitales (remota Router).

mediante consulta para comprobar los tiempos de respuesta o la coherencia de las mismas. Por medio de la fuente de alimentación se puede ordenar el reinicio de la totalidad de los equipos conectados.

Este caso de uso permite evitar los desplazamientos y visitas a campo necesarios para realizar este reinicio de componentes.

8.2.3.2. Roadmap

Los resultados de la fase 1 han confirmado el alcance de las siguientes fases, siendo la prioridad fundamental de la fase 2, el seguir profundizando en la integración de las **funciones de concentración de medida, supervisión y RTU de MT** dentro de esta nueva arquitectura, avanzando en el diseño del concepto de RTU universal que agrupe todos los equipos de medida y actuación en tensión y que gestione la conversión IP de este flujo de información y control hacia el nodo Edge.

En siguientes fases se abordarán pruebas piloto que permitan abordar **nuevas funciones de negocio como la coordinación local con recursos energéticos distribuidos o incluso modelos de Shelf-healing que permita seguir ampliando la funcionalidad del centro de transformación sobre una misma infraestructura común de CT Inteligente.**

8.2.4. Grupo Cuerva

8.2.4.1. Alcance

El piloto se centra en el desarrollo de Nodos Edge (tanto a nivel software como hardware) junto a Barbara IoT para ser instalados en centros de transformación con el objetivo de:

- Integrar múltiples protocolos de comunicación con dispositivos del centro de transformación, principalmente Modbus RTU e IEC-60870-104
- Comunicar de manera inalámbrica con la infraestructura IT de Grupo Cuerva
- Correr algoritmos localmente para el tratamiento de datos, paquetizados en contenedores Docker
- Ser gestionado remotamente para poder actualizar el dispositivo sin la necesidad de personal in situ en los centros de transformación.

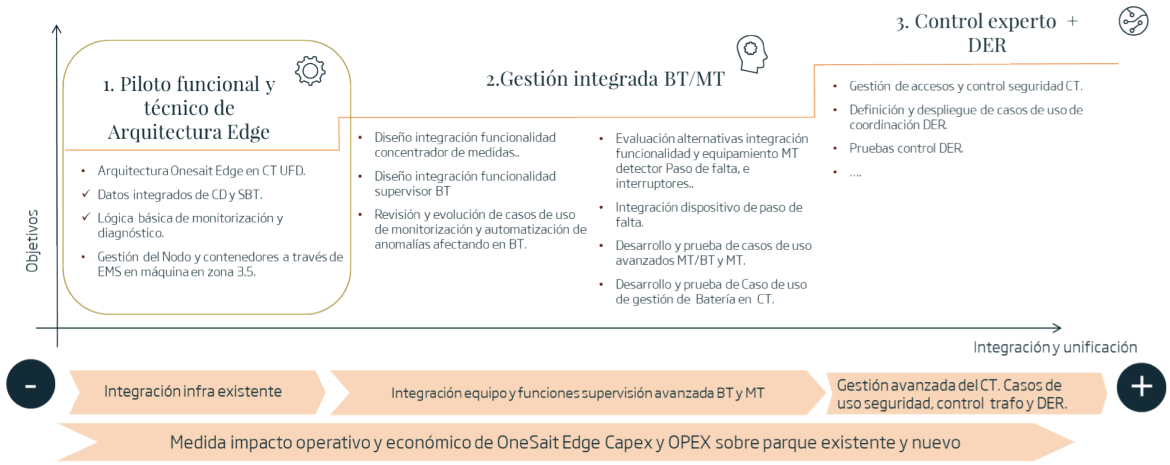


Figura 112: Roadmap CT4.0 UFD.

8.2.4.2. Esquema físico y lógico

El esquema físico del piloto es el siguiente:

En el piloto en particular nos centramos en integrar los dispositivos marcados en azul, las celdas de línea del centro de transformación y la supervisión avanzada de media tensión, dejando el resto de dispositivos para futuras integraciones:

- **Celdas de línea.** Permiten monitorizar y controlar el centro de transformación, así como modificar la explotación de la red a través del control del relé de estas celdas. Su protocolo de integración es Modbus RTU.
- **Supervisor Avanzado de Media Tensión**. Este dispositivo mide en el lado de alta del transformador, dando valores de tensión, intensidad, potencia activa y reactiva por fase,

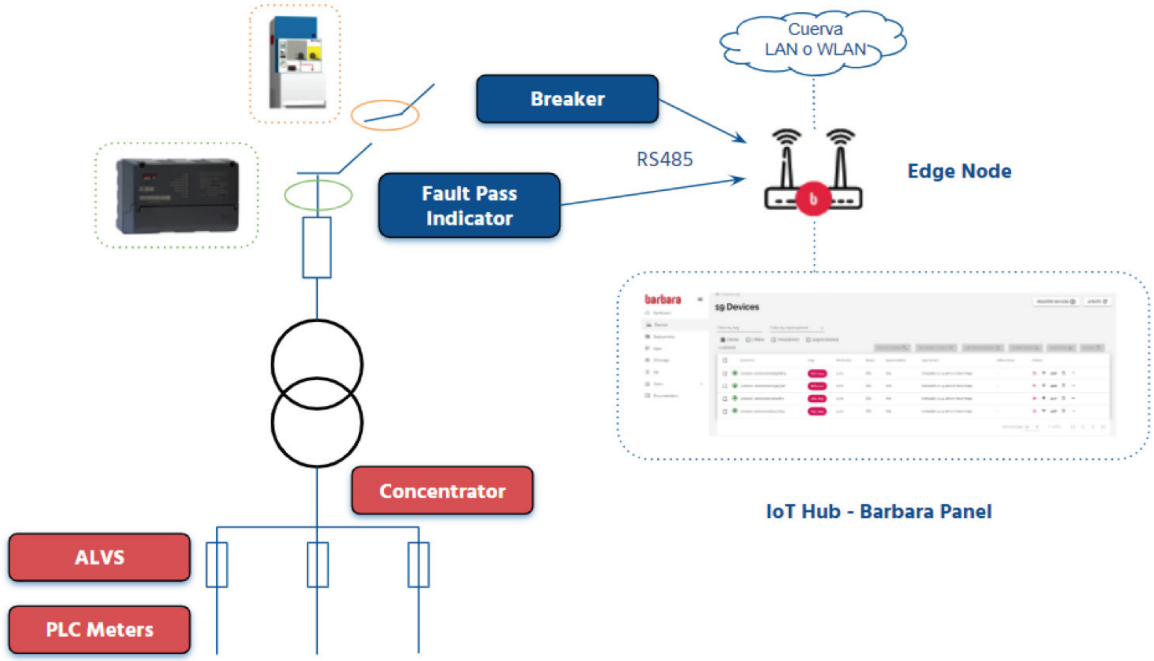


Figura 113: Esquema físico del piloto de Grupo Cuerva.

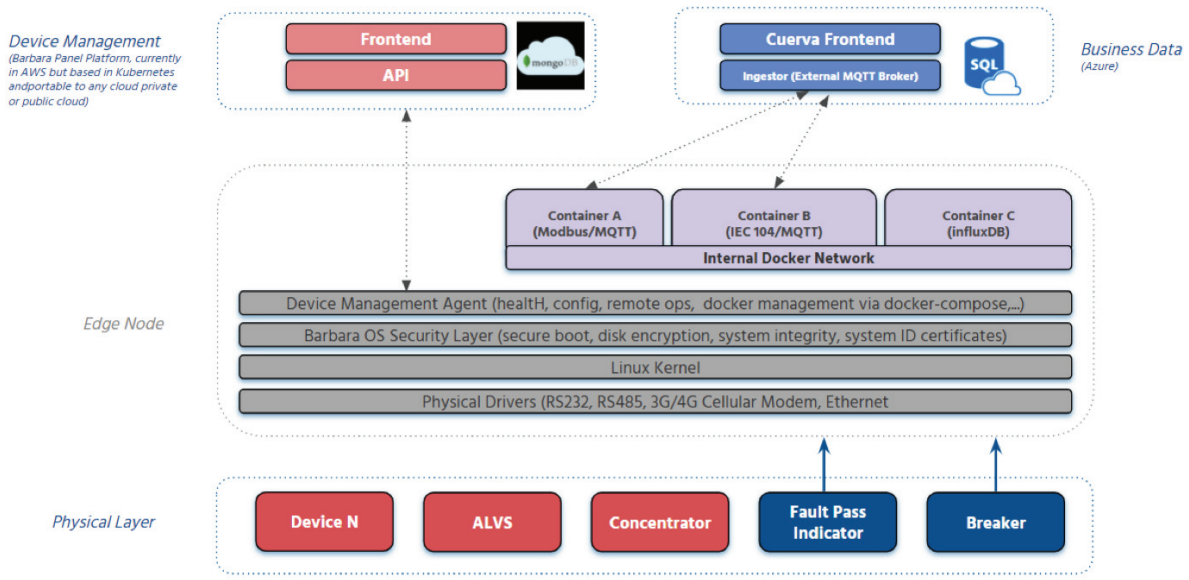


Figura 114: Arquitectura del piloto de Grupo Cuerva.

así como una serie de eventos que pueden ocurrir en la red como direccionalidad de la falta, tipo de falta, etc. Su protocolo de integración es el IEC-60870-104.

Para ello, se han usado las siguientes tecnologías:

- Docker, para ejecutar llamadas a los distintos dispositivos y obtener datos de los mismos.
- MQTT / AMQP, para el envío de datos a la infraestructura de Grupo Cuerva.
- BBDD interna en el Nodo Edge (InfluxDB), lo que permite que ante una pérdida de comunicación no se produzca la pérdida de ningún dato. Esta base de datos tiene almacenamiento para aproximadamente un día de datos.
- Plataforma de gestión remota de dispositivos (Barbara Panel).

8.2.4.3. Roadmap

En la fase 1 de proyecto se ha diseñado el alcance y las funcionalidades junto a Barbara IoT, en la fase 2 se ha diseñado la integración mediante protocolo Modbus RTU y en la fase 3 se ha testeado en campo dicho piloto, validando que los datos llegan a la infraestructura de Cuerva con granularidades menores de 30 segundos.

Actualmente nos encontramos finalizando la fase 4, donde se está desarrollando la integración con el protocolo IEC-60870-104, y en la fase 5 se validarán dichos datos y se comprobara su granularidad.

En paralelo, se están desarrollando casos de uso asociados a las medidas proporcionadas por las celdas de línea:

- Monitorización de tensiones anómalas en la red.
- Detección de desequilibrios de intensidad.
- Información de las faltas y eventos usadas en el algoritmo de localización de faltas.

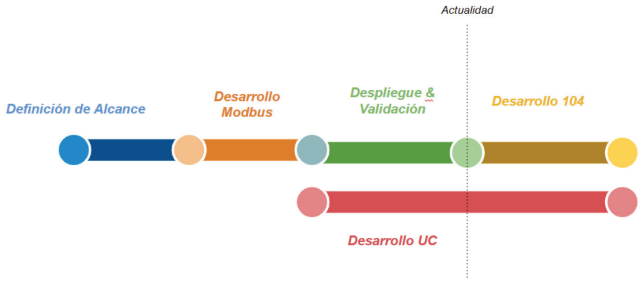


Figura 115: Roadmap del piloto de Grupo Cuervaprueba con dos líneas y carga al final de las lineas

8.2.5. DISCOVERER (2018) - Ormazabal

8.2.5.1. Alcance y objetivos

En el proyecto DISCOVERER (Distributed and Intelligent System for Coordination and Optimization of Voltage to Empower Renewables and Electric Resources) se ha investigado el funcionamiento coordinado del transformador con intercambiador de tomas en carga inteligente (OLTC) y los inversores fotovoltaicos (PV), y proponiendo y evaluando el algoritmo de control de voltaje simétrico para aumentar la eficiencia del control durante los períodos de generación fotovoltaica.

Se analizó un sistema de regulación de la tensión basado en el flujo de potencia óptimo (OPF) que utiliza la topología de la red y las mediciones en tiempo real de diferentes nodos.

8.2.5.2. Resumen de ensayos realizados

El laboratorio SysTec del Fraunhofer IEE proporcionó la infraestructura para evaluar el comportamiento coordinado del transformador de distribución inteligente con OLTC junto con los inversores fotovoltaicos.

Figura 116: Montaje de pruebas laboratorio proyecto DISCOVER.

Se han realizado 6 familias de ensayos que resultan de la combinación 2 diferentes configuraciones de la red (generación "distribuida" y "concentrada") y de 3 estrategias de control diferentes.

Test set-up	Type of control strategy
Set-up 1	No control
	Local control
	Coordinated control
Set-up 2	No control
	Local control
	Coordinated control

En cada una de las familias de ensayos se han ensayado diferentes configuraciones de generación y carga:

- Generación FV: {0; 20; 40; 60; 80} kW
- Carga: {0; 20; 40; 70; 90; 110} kW

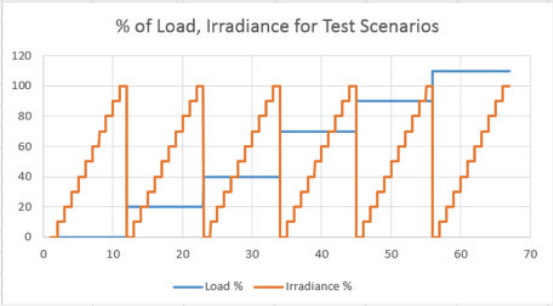


Figura 117: Configuración de escenarios de evaluación.

8.2.5.3. Configuraciones estudiadas

Red con dos líneas, generación "distribuida" y carga al final de una de las líneas:

Red con una línea, generación "concentrada" y carga al final de la línea:

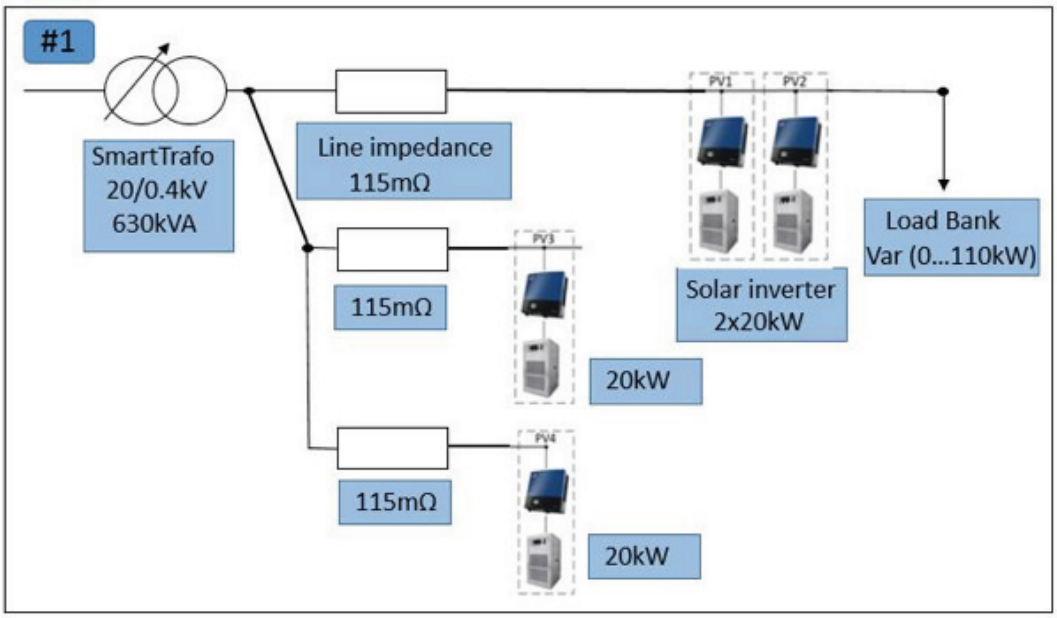


Figura 118: Esquema del entorno de red de prueba con dos líneas y carga al final de las lineas.

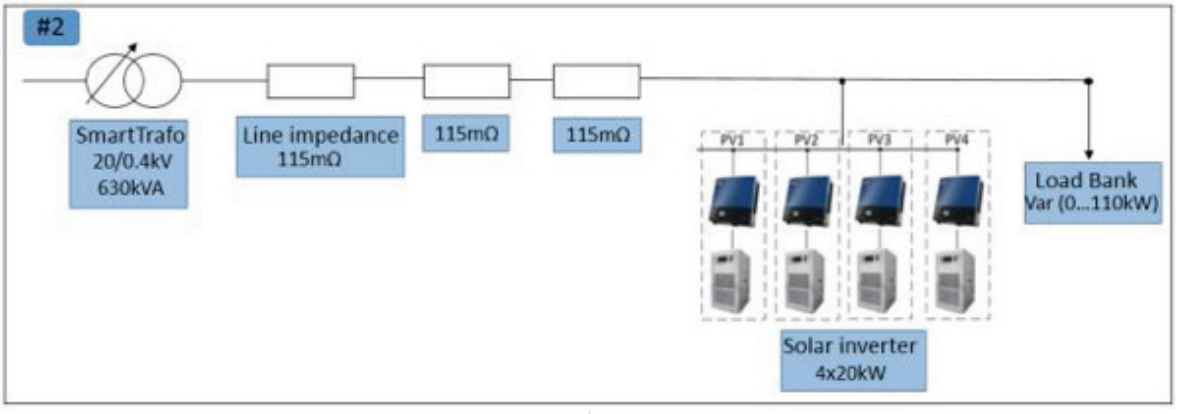


Figura 119: Esquema del entorno de red de prueba con una línea y carga al final de la línea.

8.2.5.4. Algoritmos evaluados

- Sin control: El sistema funciona como red pasiva con inversores fotovoltaicos conectados.
- Control local convencional para el transformador inteligente con OLTC y los inversores fotovoltaicos.
- Control coordinado del smart transformer junto con los inversores fotovoltaicos.

8.2.5.5. Comunicaciones del control coordinado

El controlador con algoritmo de control coordinado implementado recibe, mediante Modbus, todas las medidas obtenidas del lado BT del transformador y de cada uno de los 4 inversores fotovoltaicos y envía las órdenes de operación al OLTC y a los inversores.

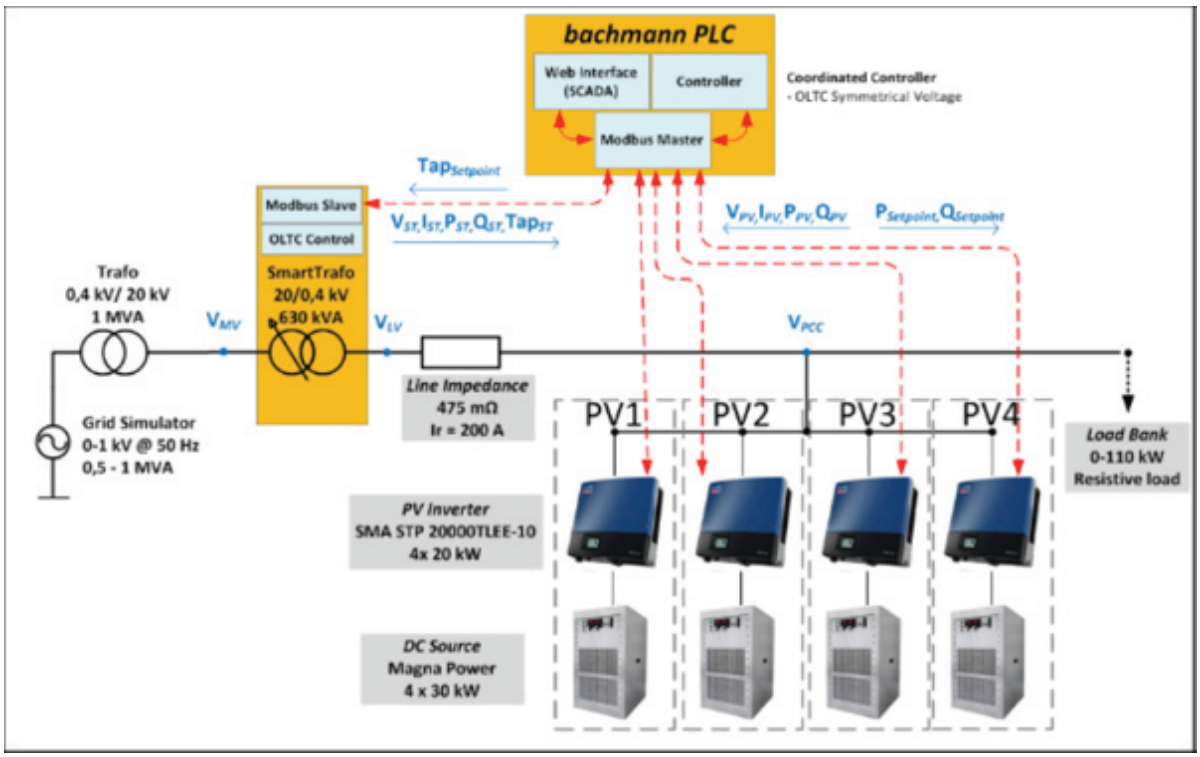


Figura 120: Esquema comunicaciones del entorno de pruebas.

8.2.5.6. Resultados

Se observó que solo el 50% de la penetración FV se integra de forma segura sin ningún control adicional (sin control), mientras que los niveles de penetración más altos se vuelven inaceptables, superando la banda de ± 10%.

La misma situación se observa con el control local, porque la carga no es suficiente para superar el umbral de variación de la tensión del 1,8% (que hace operar al OLTC) en ningún escenario, ya que la carga máxima del sistema no supera el 17% de la potencia nominal del transformador.

La aplicación del control coordinado permite la reducción de las desviaciones de tensión y el aumento de la generación fotovoltaica hasta un 100% en el peor de los casos (carga 110kW).

8.2.5.7. Conclusiones

Se ha demostrado que el control coordinado de transformadores inteligentes con OLTC e inversores fotovoltaicos incrementa la capacidad de las redes para admitir generación renovable.

En base a los resultados de esta investigación, se propone una jerarquía de tecnologías de coordinación: el transformador inteligente con OLTC puede actuar como el controlador de tensión principal en la red de BT (maestro), mientras que los inversores fotovoltaicos (esclavos) podrían seguir sus consignas de tensión para conseguir una operación de la red de BT óptima.

NO CONTROL and LOCAL CONTROL strategy						
	Load 0KW	Load 20KW	Load 40KW	Load 70KW	Load 90KW	Load 110KW
Irr 0%	0,00%	0,00%	0,00%	X	X	X
Irr 20%	20,00%	20,00%	20,00%	20,00%	X	X
Irr 30%	30,00%	30,00%	30,00%	30,00%	X	X
Irr 40%	40,00%	40,00%	40,00%	40,00%	40,00%	X
Irr 50%	50,00%	50,00%	50,00%	50,00%	50,00%	X
Irr 60%	X	60,00%	60,00%	60,00%	60,00%	60,00%
Irr 70%	X	70,00%	70,00%	70,00%	70,00%	70,00%
Irr 80%	X	80,00%	80,00%	80,00%	80,00%	80,00%
Irr 90%	X	X	90,00%	90,00%	90,00%	90,00%
Irr 100%	X	X	97,42%	100,00%	100,00%	100,00%
COORDINATED CONTROL strategy						
	Load 0KW	Load 20KW	Load 40KW	Load 70KW	Load 90KW	Load 110KW
Irr 0%	0,00%	0,00%	0,00%	0,00%	0,00%	X
Irr 20%	20,00%	20,00%	20,00%	20,00%	20,00%	20,00%
Irr 30%	30,00%	30,00%	30,00%	30,00%	30,00%	30,00%
Irr 40%	40,00%	40,00%	40,00%	40,00%	40,00%	40,00%
Irr 50%	50,00%	50,00%	50,00%	50,00%	50,00%	50,00%
Irr 60%	60,00%	60,00%	60,00%	60,00%	60,00%	60,00%
Irr 70%	70,00%	70,00%	70,00%	70,00%	70,00%	70,00%
Irr 80%	80,00%	80,00%	80,00%	80,00%	80,00%	80,00%
Irr 90%	90,00%	90,00%	90,00%	90,00%	90,00%	90,00%
Irr 100%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%

No voltage violation
Undervoltage violation
Overvoltage violation

Figura 121: Resultados de desviación en tensión final sin control y con control coordinado.

8.2.6. HOLISTICA (2019) - Ormazabal

8.2.6.1. Alcance y objetivos

En el proyecto HOLISTICA (Holistic Optimization of Losses using an Improved Synergy of Technologies under an Innovative Coordination Algorithm) se ha investigado el funcionamiento coordinado del transformador con intercambiador de tomas en carga inteligente (OLTC) junto con los inversores fotovoltaicos, las baterías y la carga del VE.

Los objetivos han sido incrementar la capacidad de integración de energías renovables distribuidas y de nuevas cargas como el VE, reducir las pérdidas en la red de BT y mejorar la vida útil de los equipos con capacidad de operar la red de BT.

8.2.6.2. Resumen de ensayos realizados

El laboratorio Syslab de la DTU proporcionó la infraestructura para evaluar el comportamiento coordinado del transformador de distribución inteligente con OLTC junto con los inversores fotovoltaicos, las baterías y la carga del VE.

Figura 122: Entorno de pruebas del laboratorio Syslab.

Se han realizado 8 familias de ensayos que resultan de la combinación diferentes configuraciones de la red (rural, urbana y "flexible") y de 4 estrategias de control diferentes.

Para la red rural y urbana, se probó un perfil de generación de carga completa, modificando el porcentaje de consumo de energía total (α, 0 a 100%) y limitando el porcentaje

de potencia activa total (β, 0 a 100%). Esto ha permitido el análisis de diferentes perfiles de carga y generación basados en otros estudios y mediciones reales.

En total, se realizaron 288 ensayos en la DTU SYSLAB durante un período de 6 días.

Además, posteriormente se realizó una configuración de prueba de 24 horas, incluyendo casi todos los recursos disponibles en el laboratorio con el fin de probar la viabilidad del sistema de control en un entorno "flexible" y casi real.

8.2.6.3. Configuraciones estudiadas

Se configuraron 3 escenarios diferentes: una red rural y una urbana y una "flexible".

Rural:

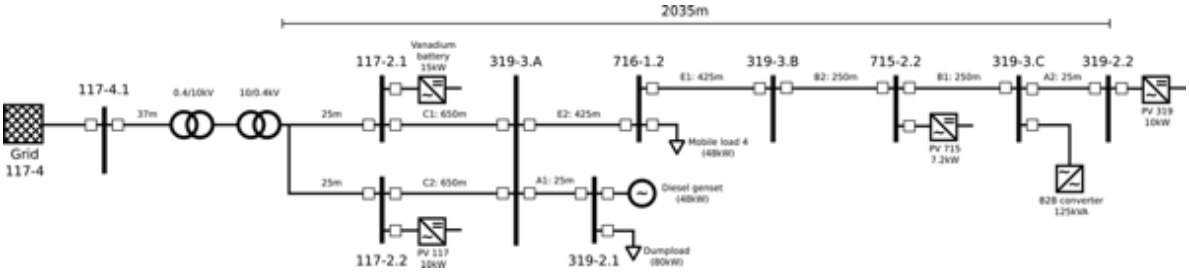


Figura 123: Configuración red rural.

Urbana:

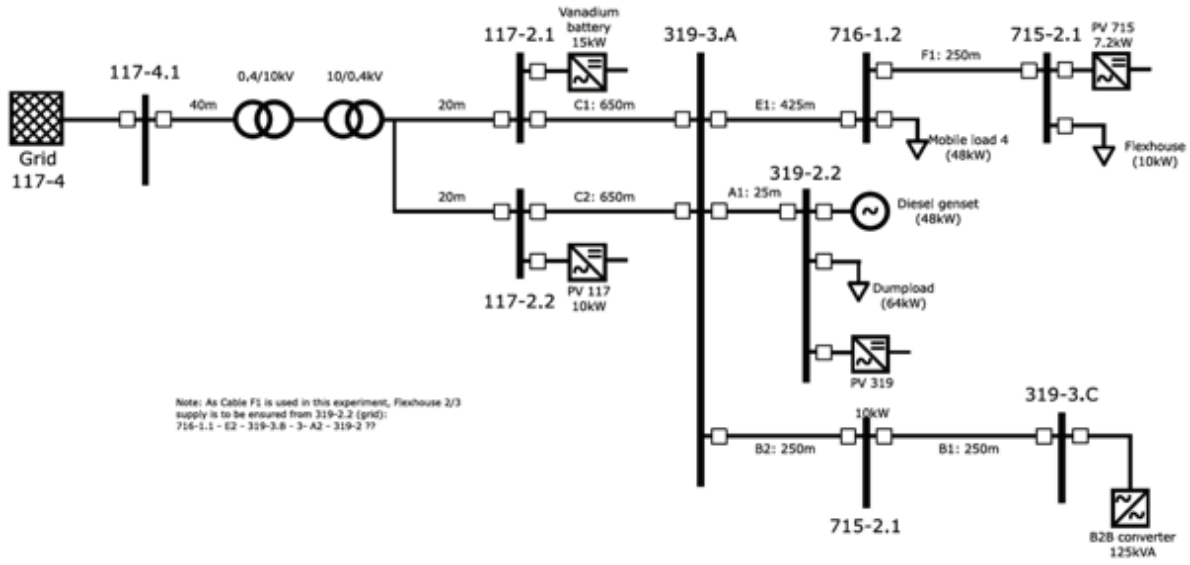


Figura 124: Configuración red urbana.

"Flexible":

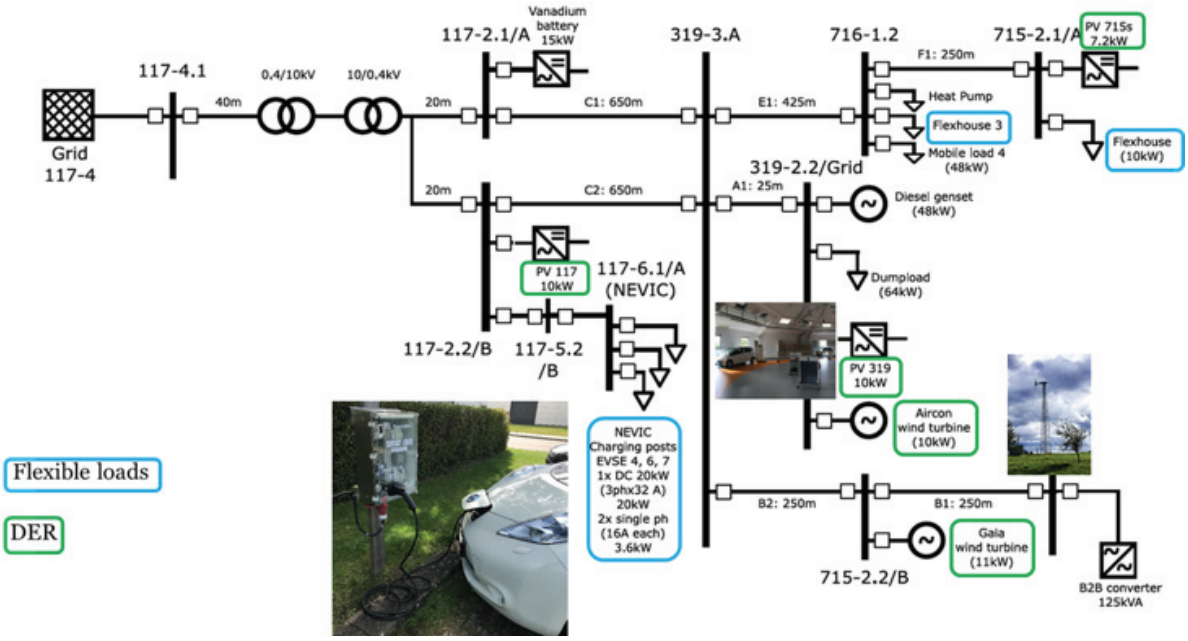


Figura 125: Configuración red flexible.

8.2.6.4. Algoritmos evaluados

- Sin control (NC)
- Control OLTC (control T)
- Control de potencia reactiva (control Q)
- Control coordinado de potencia reactiva y OLTC (control QT)

8.2.6.5. Resultados

El impacto de cada estrategia de control se evaluó comparando la "Hosting Capacity" (HC) de la red, la reducción de las pérdidas y el incremento de la estabilidad de la red, al tiempo que se optimizó el número de operaciones del OLTC.

Control strategy	HC (%)	Losses reduction (%)
NC	0.00	0.00
T	61.65	2.56
Q	63.27	6.31
QT	61.07	9.35

Los resultados muestran que una aplicación de control T aumenta la HC en un 61,65%. En el caso de utilizar un control coordinado QT las pérdidas de energía se pueden reducir en un 9.35%.

8.2.6.6. Conclusiones

Se ha demostrado experimentalmente que el control coordinado del transformador de distribución inteligente con OLTC puede mejorar la eficiencia de las redes de distribución mediante la provisión de una óptima flexibilidad y confiabilidad de la red.

Esta estrategia de control integral, que gestiona de manera eficiente los recursos distribuidos existentes, evitaría la necesidad de electrónica de potencia dedicada y baterías a nivel del CT, al gestionar de manera coordinada tanto el almacenamiento como la electrónica de potencia conectada a la red de BT.

Este enfoque para resolver las congestiones de tensión locales, basado en la operación y coordinación de los recursos distribuidos, es complementaria a los mercados de flexibilidad locales.

8.2.7. POC100 E-distribución

8.2.7.1. Alcance y objetivos

Dentro del proyecto COORDINET y en el ámbito de la Smart City de Málaga se encuadra el proyecto de sensorización POC100.

Los objetivos han sido incrementar la capacidad de integración de energías renovables distribuidas y de nuevas cargas como el VE, reducir las pérdidas en la red de BT y mejorar la vida útil de los equipos con capacidad de operar la red de BT. Todo ello a través de la monitorización de una serie de CTs.

8.2.7.2. Descripción

La zona elegida es la Smart City de Málaga. Donde se van a instalar más de 100 Equipos de tres proveedores:

- Ormazabal.
- Pronutec.
- Circutor

Los criterios de selección fueron los siguientes:

- Proximidad a FSP.
- Observabilidad de la red.
- Número de incidencias.
- Potencia nominal de los CDs.
- Características del patrón de consumo de los CDs.
- Número de clientes.
- Curvas de carga de clientes.
- Sensores de intensidad.
- SSEE controladas remotamente.
- Presencia del LVS.

Figura 126: Zona de sensorización en la Smart City de Málaga.

8.2.7.3. Arquitectura

La arquitectura y el esquema de comunicaciones se puede ver en el siguiente gráfico:

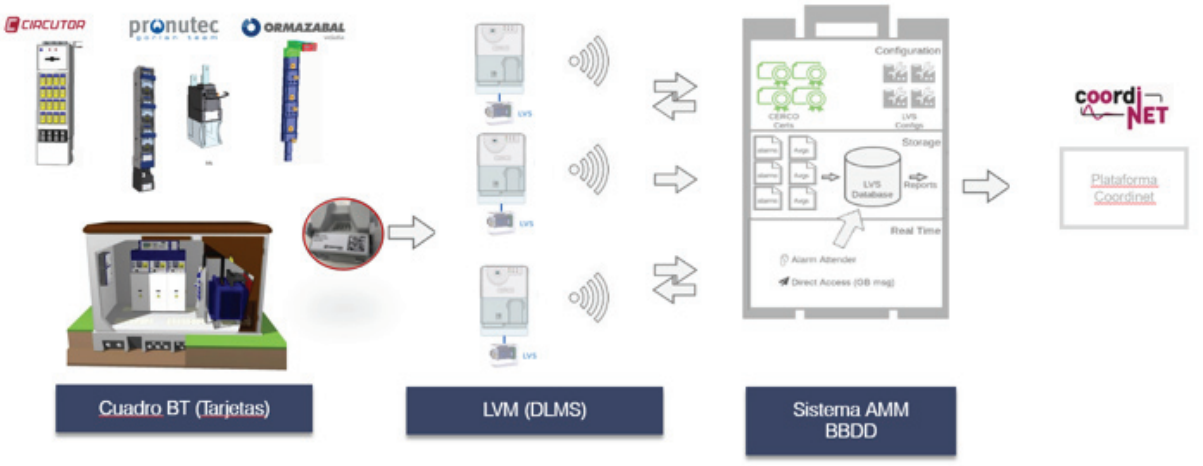


Figura 127: Esquema de comunicaciones.

Donde los cuadros de BT cuentan con sensorización adaptada. Estas medidas se transmiten vía protocolo DLMS/COSEM a través del concentrador (LVM). Finalmente se recogen estos valores en una BBDD central donde son procesadas y utilizadas para los algoritmos de Mantenimiento preventivo y vinculación dinámica.

Por su parte en esta imagen se muestran los tres tipos de tecnologías de sensorización utilizadas:

8.2.7.4. Resultados y conclusiones

Actualmente se encuentra en fase de desarrollo e implantación, por lo que no podemos compartir resultados finales. Se han instalado gran parte de los equipos de sensorización y se espera que para final de 2022 queden instalados todos. Se adjunta la tabla con cada tecnología:

Figura 128: Tipos de tecnologías de sensorización empleadas en la Smart City de Málaga.

8.3. Comparativa tecnologías entre proyectos

A continuación, se muestra tabla comparativa con las diferentes tecnologías utilizada en cada proyecto, a fin de localizar puntos comunes:

Piloto		E4S Alliance-SSP	MiDE4S (Minsai i-DE)	CT 4.0 UFD	Grupo Cuerva	Discoverer (2018)_ Ormazabal	Holistica (2019) Ormazabal	POC 100 E-distribi-cion
Plataformas y protocolos		Secondary Substation PLatform	Onesait edge	Onesait edge	Barbara IOT	PLC	PLC	Plataforma Coordinet
Tecnologías	Dockers	X	X	X	X			
	Protocolos IOT	X	X	X				
	Protocolos WOT	X	X	X				
	Open Source		X	X		X	X	
	Things IOT Hub- Edge Mana-gement system		X	X	X			
	MQTT		X	X	X			
	JSON		X	X				
	https		X	X	X			
	OPC - UA							
	61850							
	Prime		X	X				
	104				X			X
	MODBUS				X	X	X	X

8.4. Conclusiones – ámbitos de colaboración

Necesidad de un marco de estandarización para la red inteligente para la mejora de:

- Escalabilidad y agilidad en la adopción de nuevas funcionalidades, minimizando los tiempos de desarrollo y flexibilidad de implementación.
- Interoperabilidad entre las diferentes aplicaciones desarrolladas y cuyo despliegue sea posible en hardware abierto y de bajo coste.

Evaluación y mejora de las medidas de ciber seguridad bajo el nuevo entorno de control distribuido, integración e interoperabilidad con servicios y sistemas proporcionados por diferentes proveedores y fabricantes.

Desarrollo de control integral que gestione de manera eficiente los recursos distribuidos existentes

Despliegue de algoritmos que necesitan más recursos de máquina tales como algoritmos en base a inteligencia artificial para nuevas aplicaciones y funcionalidades y control.

Requisitos ante despliegues masivos.

Nuevas funciones de negocio como la coordinación local con recursos energéticos distribuidos o incluso modelos de Shelf-healing que permita seguir ampliando la funcionalidad del centro de transformación sobre una misma infraestructura común de CT Inteligente.

9. REFERENCIAS

[1] CIRED, «Technology Development and Distribution System Benefits CIRED's point of view,» Working Group on Smart Secondary Substations, 2017.

[2] Iberdrola Distribución Eléctrica , MT 2.11.03 (Ed. 07) - PROYECTO TIPO PARA CENTRO DE TRANSFORMACIÓNEN EDIFICIO DE OTROS USOS, 2018.

[3] A. Guerrero Fernández, Instalaciones de distribución, ISBN 13: 9788448171483: McGraw-Hill Interamericana de España S.L., 2010.

[4] IEC 62559-1:2019, Use case methodology - Part 1: Concept and processes in standardization: IEC, 2019.

[5] SG-CG/M490/F, Overview of SG-CG Methodologies. CEN-CENELEC-ETSI Smart Grid Coordination Group, 2014.

[6] SG-CG/M490/C, Smart Grid Reference Architecture. CEN-CENELEC-ETSI Smart Grid Coordination Group, 2012.

[7] DISCERN (Offis), Architecture templates and guidelines, Deliverable (D) No: 1.3. DISCERN, 2013

[8] i-DE, ET Funcionalidad Supervisión Avanzada BT.

[9] Iberdrola, STG – Advanced LV supervision interface specification, 1.7 ed.

[10] i-DE, SABT - DLMS Profile.

[11] i-DE, i-CBT DLMS Profile.

[12] i-DE, i-Trafo DLMS Profile.

[13] i-DE, ET Funcionalidad - i-CBT.

[14] i-DE, ET Funcionalidad - i-Trafo.

[15] i-DE, RTU-BT: Especificación Técnica Funcional.

[16] DLMS User Association, DLMS Blue Book - COSEM Interface Classes and OBIS Object Identification System, 12th ed.

[17] Iberdrola, Advanced Low Voltage Supervision DLMS Profile, 1.7 ed., February 2020.

[18] IEEE, Sdt C37.111-1999, IEEE Standard Common Format for Transient Data Exchange (COMTRADE) for Power Systems, 1999.

[19] IEC, 60255-151:2009. Measuring relays and protection equipment - Part 151: Functional requirements for over/under current protection.

[20] Iberdrola, ET Requisitos de Seguridad (URTs, Cargadores y Remota de supervisión avanzada BT).

[21] AENOR, UNE-EN 61000-4-30. Compatibilidad electromagnética (CEM) Parte 4-30: Técnicas de ensayo y medida. Métodos demedida de la calidad de suministro.

[22] AENOR, UNE-EN 50160. Características de la tensión suministrada por las redes generales de distribución.

[23] i-DE, ET Funcional del concentrador de datos de telegestión.

[24] iDE, Especif interfaz_STG-CD_Vers.3.4 y Vers 4.0.

[25] PRIME-Spec_v1.3.6

[26] PRIME COSEM PROFILE version 1.07, versión 1.08 y versión 1.09

[27] CIRED, «Technology Development and Distribution System Benefits CIRED's point of view,» Working Group on Smart Secondary Substations, 2017.

[28] Iberdrola Distribución Eléctrica , MT 2.11.03 (Ed. 07) - PROYECTO TIPO PARA CENTRO DE TRANSFORMACIÓNEN EDIFICIO DE OTROS USOS, 2018.

[29] A. Guerrero Fernández, Instalaciones de distribución, ISBN 13: 9788448171483: McGraw-Hill Interamericana de España S.L., 2010.

[30] Maria Yatsenko,Market Research Specialist "What Is the Difference Between Cloud Computing and Edge Computing" 14 de abril de 2018 https://www.apriorit.com/dev-blog/531-cloud-edge-computing.

[31] AWS lambda Developer Guide "Getting started with Lambda" https://docs.aws.amazon.com/lambda/latest/dg/lambda-app.html

[32] "Estimador de Estado en el dominio complejo para grandes sistemas de Transporte y Distribución de potencia", VI Congreso Smart Grids 2019 (https://www.smartgridsinfo.es/comunicaciones/comunicacion-estimador-estado-dominio-complejo-grandes-sistemas-transporte-distribucion-potencia). J.Besada, A.González, J.Ferro, G.Plaza .

ANEXOS

ANEXO I - Plantilla para desarrollo de Casos de Uso (DISCERN)

Description of the use case

Name of use case

Use case identification		
ID	*Area / Domain(s) / Zone(s)*	*Name of use case*

Version management

Version management				
Version No.	*Date*	*Name author(s)*	*Changes*	*Approval status*

Scope and objectives of use case

Scope and objectives of use case	
Scope	
Objective(s)	
Related Business Case(s)	

Narrative of Use Case

Narrative of use case
Short description
Complete description

Key performance indicators (KPI)

Key performance indicators			
ID	*Name*	*Description*	*Reference to mentioned use case objectives*

Use case conditions

Use case conditions
Assumptions
Prerequisites

Further information to the use case for classification / mapping

Classification information
Relation to other use cases
Level of depth
Prioritisation
Generic, regional or national relation
Nature of the use case

Further keywords for classification

General remarks

General remarks
General remarks

Diagrams of use case

Diagram(s) of use case
Diagram(s) of use case

Technical details

Actors

Actors			
Grouping		*Group description*	
Actor name	*Actor type*	*Actor description*	*Further information specific to this use case*

References

References						
No.	*Reference Type*	*Reference*	*Status*	*Impact on use case*	*Originator/ organisation*	*Link*

Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario description	Primary actor	Triggering event	Pre-condition	Post-condition

Steps – Scenarios

Scenario								
Scenario name :								
Step No.	Event	Name of process/ activity	Description of process/ activity	Service	Information producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirements, R-IDs

Information Exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of Information exchanged	Requirement, R-IDs

Requirements (optional)

Requirements (optional)		
Categories ID	Category name for requirements	Category description
Requirement R-ID	Requirement name	Requirement description

Common terms and definitions

Common terms and definitions	
Term	Definition

Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

ANEXO II – Marco de referencia para la implementación de interoperabilidad entre aplicaciones en el Edge.

El modelo de interoperabilidad se basa la en la definición de dos protocolos de comunicaciones para uso interno entre aplicaciones. Un primer protocolo HTTP/REST para las comunicaciones directas entre aplicaciones y otro, MQTT, para compartir información de forma general con todos los servicios del sistema.

Sobre los protocolos de comunicaciones, se define un modelo de intercambio de datos estandarizado, el WoT, que permitirá definir el modelo de datos que ofrece cada servicio de una forma clara y concisa.

A.II.1 WOT

El uso de WOT-A proporciona al SASCTI una forma simple de interoperabilidad entre los servicios (o aplicaciones) implementados en el SASCTI. Para los propósitos de usar el estándar WOT, dentro de SASCTI, en esta fase no se pretende modelar la granularidad más básica de todos los elementos físicos administrados en el dominio del SASCTI y aguas abajo.

Arquitectura WOT

Los elementos, interacciones y propiedades esenciales de una arquitectura WOT-A y SASCTI que se utilizará se limitan a lo siguiente:

- Cada una de las aplicaciones que se implementarán en el SASCTI se considera una cosa (Thing) según se define en el estándar WOT
- Cada Aplicación cubrirá el conjunto completo de funcionalidades detalladas en la Sección 5.1.2 del Estándar WOT:
  - Leer la información de estado de la cosa.
  - Actualización de la información de estado de la cosa que podría causar activación.
  - Suscribirse, recibir y darse de baja de notificaciones de cambios en la información del estado de la cosa.
  - Invocar funciones con parámetros de entrada y salida que provocarían cierta actuación o cálculo.
  - Suscribirse, recibir y cancelar la suscripción a notificaciones de eventos que son más generales que solo informes de transiciones de estado.
- ICM solo admitirá el patrón de comunicación directa en el que los consumidores y las cosas están conectados sin intermediarios (sección 6.7.1 del estándar WOT). Es posible que se agreguen nuevos patrones en el futuro para cubrir la conexión externa a los sistemas de control fuera del SASCTI, la interacción con las cosas contenidas en el SASCTI a través de un intermediario o cualquier otro caso de uso que surja.

Protocolo vinculante

La selección de estos protocolos de aplicación establece lo que en WOT se denomina plantilla de enlace y protocolo de enlace.

Thing Description (TD)

El modelo de datos TD permitirá caracterizar una aplicación dentro del SASCTI. Dada la amplia expresividad del TD, para esta primera versión del ICM se han acotado varios aspectos sobre el formato JSON para obtener un TD sencillo y suficientemente adaptado a los casos de uso.

No se admite el uso de extensiones semánticas con JSON-LD que no sean "https://www.w3.org/2019/wot/td/v1".

Aunque la definición de seguridad aún está pendiente, la definición de TDs en esta versión debe incluir en el atributo SecurityScheme con el valor "NoSecurityScheme".

Un TD SASCTI válido que describa una solicitud debe incluir las siguientes secciones:

A. Root Object

El objeto raíz JSON incluye el @context https://www.w3.org/2019/wot/td/v1, junto con los siguientes valores:

Things Root Object:

```
{
 "@context": "https://www.w3.org/2019/wot/td/v1",
 "type": "[topo|outage|DCU|AdvLVS|LVS]",
 "id": "$IdService",
 "description": "Human readable information.",
 "version": {"instance": "1.2.1"},
 "created": "YYYY-MM-DDTHH:MM:SS",
 "modified": " YYYY-MM-DDTHH:MM:SS ",
 "securityDefinitions": {
 "no_sc":{
 "scheme": "no-sec"}
 },
 "security": ["no_sc"],
 "properties": {...},
 "actions": {...},
 "events": {...},
 "links": [...]
}
```

El id debe contener el identificador del servicio ($ IdService), proporcionado por el sistema. Este identificador debe contener la información necesaria para que el servicio de enrutamiento y el DNS incluidos en el software base puedan conectarse al servicio. Esta es la razón por la que la definición del servicio en el archivo .yml debe declarar el servicio con este id. Todo sistema registrado como una cosa que ofrece servicios debe tener un idService.

B. Properties

Se definen dos propiedades principales como obligatorias para todos los servicios:

- Inventario: Proporciona un inventario completo de los elementos gestionados por el Servicio. Obligatorio sólo para aquellos servicios que gestionen hardware auxiliar.
- State: Parámetro indicando el estado del servicio.

Otras propiedades específicas se definirán individualmente por Servicio.

C. Actions

Los servicios deben detallar las acciones que permiten: parámetros necesarios, tipo y formato de respuesta.

Se incluye a continuación ejemplo de declaración de acciones para un servicio que publique informes instantáneos y batch.

```
“actions”: [
“getExampleReport”: {
 “description”: “Request an example report, with optional values to select a specific subset of meters or feeders”,
 “input”: {

 “from”: “dateTime”,
 “to”: “dateTime”,
 “Synchronous”: “Boolean”
 “idMeters”: “String”
 “idFeeders”: “String”
 “required”: [“Synchronous”,”from”, “to”]

 “output”
“type”: “object”,
 “properties”: {
 .....
 “forms”: [
 {...}
 ]
 },
 }
 ]
```

D. Events

Se definen cuatro tipos de eventos por servicio:

Operación	TD Event	Accesibilidad
Espontaneo	alarms	Publico
Espontaneo	events	Publico
Planificado	globalReports	Publico
Bajo demanda	individualReports	Privado

WOT Context / Things Directory

En ICM, el directorio WOT reflejará el TD del SASCTI. Cada cosa que se muestre en el SASCTI debe comunicarse con el Directorio WOT y proporcionar su TD para que pueda ser consultada por todos los demás. El Directorio WOT expondrá esta información utilizando dos canales complementarios:

1. El conjunto completo de TD de cosas estará disponible a través de una solicitud WS-REST a la URL: hhtp.://SASCTI-directroy/tds

2. Cada vez que haya un cambio en el contenido del Directorio WOT (registro de un nuevo TD o eliminación de un TD existente), el TD actual se publicará en el tema público de MQTT "SASCTI-directory/tds".

El ciclo de vida de la aplicación requiere la siguiente sincronización con el estado del directorio WOT:

- Cuando se implementa una aplicación en el SASCTI, se debe realizar una solicitud de registro al servicio de directorio WOT a la URL "https: // SASCTI-directory/tds/" a través de un mensaje POST, incluido el JSON TD. La respuesta obtenida contendrá el ticket de registro, un idService en formato urn, único para la aplicación.
- Cuando se elimina una aplicación o se retira del SASCTI, una solicitud para darse de baja del servicio de directorio WOT debe establecerse en la URL "https: // SASCTI-directory/tds/:idService" mediante un mensaje DELETE, incluido el idService (en formato urn) y el ticket de registro.
- Una aplicación puede obtener la lista de TD disponibles en el contexto del SASCTI de dos formas diferentes

  I. On Demand enviando una solicitud de consulta GET al directorio WOT. La respuesta contendrá la lista completa de las aplicaciones que se ejecutan en el SASCTI junto con sus TDs

  II. Suscribiéndose al tema MQTT previamente comentado donde de forma espontánea, se publica la información de cambios en la lista completa de TDs.

A.II.2 MQTT

Todas las comunicaciones de ICM usan o pueden usar los temas de MQTT. Para admitir este mecanismo, la infraestructura debe hacer que un intermediario MQTT esté disponible dentro de los componentes implementados.

Este protocolo debe ser compatible con un pod / contenedor que declare el servicio **"mqtt: // localMqttService: 8883"**. Este servicio debe ser accesible desde cualquier pod / contenedor implementado en la infraestructura de borde.

Los temas disponibles serán los incluidos en los enlaces incluidos en los TD de cada una de las cosas desplegadas.

Consideraciones a la configuración del bróker MQTT.

El broker MQTT utilizará TLS para las conexiones y establecerá el oyente en el puerto conocido **8883. No se aceptarán conexiones anónimas.** El broker-MQTT permitirá modificar las credenciales o invalidar un cliente usando

API y una consola de operación. El repositorio de credenciales final se definirá en la sección de seguridad, aunque para las PoC actuales se puede utilizar el mecanismo proporcionado por el broker-MQTT. El corredor admitirá permisos sobre temas basados en expresiones regulares y por identificación de cliente. El mecanismo de protección del tema final se definirá en la sección de seguridad. En las PoC actuales, se puede usar la identificación del ID del cliente. Hasta que se conozca en detalle el tráfico admitido después de las primeras pruebas, se establece un **keepAlive = 60** segundos predeterminado. Mientras espera poder medir el rendimiento del intermediario con los diferentes tamaños de carga útil por mensaje, no existe una limitación predeterminada en el tamaño del mensaje.

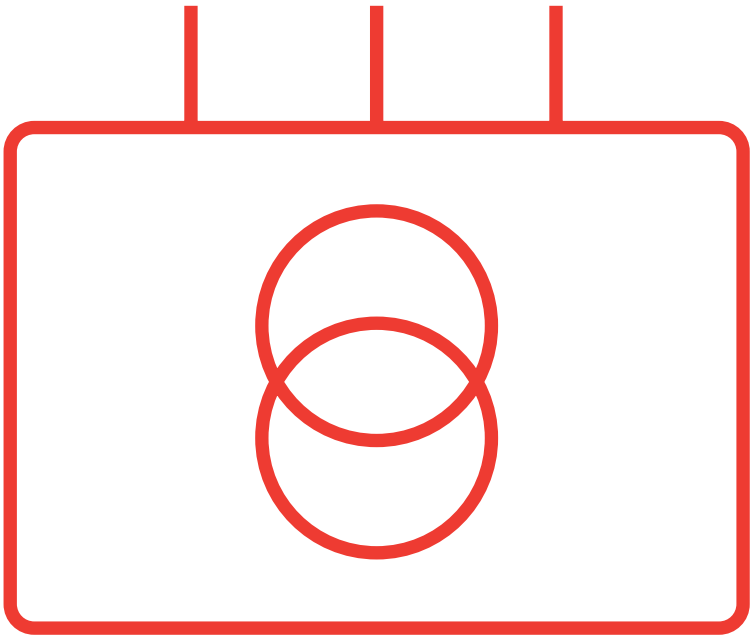
Consideraciones a la configuración de los clientes MQTT.

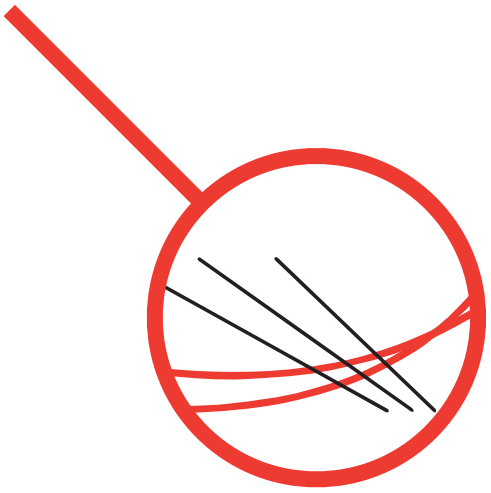
Todos los clientes conectados al bróker MQTT deben identificarse con una identificación, no se permitirá la conexión anónima al broker. Todos los clientes deben utilizar credenciales de **usuario / contraseña** en su conexión. El servicio para la provisión de estas credenciales se definirá en el apartado de seguridad. Todas las conexiones al intermediario se definirán como **cleanSession = true** para evitar tener que implementar dos flujos de conexión diferentes.

Todas las publicaciones cumplirán con el parámetro **QoS = 2**, para evitar la entrega de mensajes duplicados. Las publicaciones de mensajes programados que no son frecuentes, marcarán el indicador **retain = true**. De esta forma, el último informe publicado se almacenará en el broker.

A.II.3 RESTful API

De acuerdo con los end-points definidos en el TD correspondiente, todas las aplicaciones desplegarán una **Web API** y expondrán los servicios necesarios a través de **RESTfull**. Por el momento, solo se consideran los servicios de consulta que deben utilizar el mecanismo **GET**. La seguridad de las llamadas en estos servicios se debera desarrollar.





FutuRed

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

AGENCIA ESTATAL DE INVESTIGACIÓN