Departamento de Arquitectura y Tecnología de Computadores

UNIVERSIDAD DE GRANADA

Tesis

Futuros Sistemas Embebidos en SmartGrid: nuevas aportaciones en Unidades Terminales Remotas

Realizado por:

Francisco Ramos Peñuela

Dirigido por:

Dr. Héctor Pomares Cintas y Dr. Miguel Damas Hermoso

Editor: Universidad de Granada. Tesis Doctorales
Autor: Francisco Javier Ramos Peñuela
ISBN: 978-84-1306-013-2
URI: http://hdl.handle.net/10481/53830

Índice

Listado de Figuras

Agradecimientos

En primer lugar, quiero darles las gracias a mis tutores Hector y Miguel por la inestimable guía durante la realización de la tesis, la ayuda prestada durante todos estos años, y el continuo ánimo que han infundido en mí, sin ellos no habría sido posible realizar esta tesis y para ellos mi sincero agradecimiento.

Al mismo tiempo agradecer a mi familia su apoyo y comprensión por el tiempo que les he robado, así como por la ilusión que han puesto en verme finalmente convertido en Doctor.

Agradecer a la Universidad de Granada la formación que me ha proporcionado y que ahora culmino. A su vez, a Schneider Electric por brindarme la posibilidad de trabajar en un sinfín de proyectos de I+D innovadores y estar en contacto con las novedades tecnológicas.

Por último, a mis compañeros de los proyectos de I+D de Schneider Electric y de otras empresas, centros tecnológicos y Universidades en especial Seven Solutions (Granada), A2A Unareti (Italia) y la Universidad de Sevilla.

Resumen

El sector eléctrico se enfrenta a importantísimos desafíos como el drástico aumento de la población mundial y la necesidad de reducir las emisiones de CO_2. Al mismo tiempo, aparecen un sin fin de nuevas tecnologías tanto de información y comunicaciones, como son Internet de las Cosas, la sincronización, la seguridad y ciberseguridad, así como las nuevas tecnologías de potencia y almacenamiento.

En este contexto, las redes eléctricas se encuentran en un proceso de transformación sin precedentes para convertirse en las redes interconectadas, automatizadas e inteligentes del futuro utilizándose para ello el concepto de SmartGrid.

En SmartGrid, los sistemas embebidos parecen tener un papel secundario frente a los nuevos importantes protagonistas como el BigData. Sin embargo, en esta tesis, titulada "El futuro de los Sistemas Embebidos en SmartGrid: nuevas aportaciones en Unidades Terminales Remotas" se trata de poner de manifiesto la importancia, en la red eléctrica de hoy y del mañana, de las Unidades Terminales Remotas. Éstas, son el representante fundamental de los sistemas embebidos en dicha red y son el elemento clave de las Subestaciones eléctricas que son, en último término, la columna vertebral del sistema eléctrico en su conjunto.

Por consiguiente, en la presente tesis se realizan nuevas aportaciones a distintos sistemas de la red eléctrica, como son los Sistemas de Protección, los Sistemas de Sincronismo, y los Sistemas de Gestión y Mantenimiento, en los que las Unidades Terminales Remotas y, por tanto, los sistemas embebidos, son el elemento alrededor del cual se articula la investigación.

A su vez, la labor investigadora transcurre entre importantes estándares de SmartGrid, como son el IEC61850 (el principal para la automatización de Subestaciones), el IEC61508 (para seguridad funcional), el IEEE1686 e IPSec (para ciberseguridad) y el IEEE1588 (para sincronización), así como novedosas tecnologías como White-Rabbit, Internet de las Cosas, Redes Sociales, Internet Social de las Cosas, Procesamiento de Lenguaje Natural, entre otras.

Concretamente, se investiga sobre los tres aspectos siguientes, en el contexto de la Subestación eléctrica:

- Los sistemas de protección, donde se propone un "Nuevo Sistema de Protección Adaptativa Basado en el Estándar IEC61850", que permita la reconfiguración dinámica de los dispositivos de protección para implementar soluciones avanzadas de tratamiento de faltas en la red eléctrica de distribución.
- Los sistemas de automatización con alta disponibilidad y seguridad, donde se contribuye en "Nuevas Redes de Sincronismo Redundante de Precisión Basadas en Tecnología White-Rabbit para Subestaciones Confiables" que ofrezcan una mejora significativa de la precisión y disponibilidad.
- La "Concepción de un Nuevo Sistema de Gestión y Mantenimiento de Subestaciones Eléctricas Basado en Internet Social de las Cosas" donde se

redefine la interacción con las RTUs para adaptarse al nuevo mundo digital, posibilitando a su vez un acceso a la información de la Subestación eléctrica más ágil y eficiente.

Finalmente, se abren nuevas las líneas futuras de investigación, siempre con las Unidades Terminales Remotas como elemento central y, en este caso, con la Inteligencia Artificial como tecnología principal para el potencial desarrollo.

Abstract

The electric sector faces important challenges such as the drastic increase in the world population and the need to reduce the CO2 emissions. Moreover, there is an endless number of new information and communication technologies, for example Internet of Things, synchronization, safety and cybersecurity, as well as new power and storage technologies.

In this context, the electrical networks are in an unprecedented transformation process to become the interconnected, automated and intelligent networks of the future, using the SmartGrid concept.

In SmartGrid domain, the embedded systems seem to play a secondary role compared to technologies like BigData. However, in this thesis, entitled "The Future of Embedded Systems in SmartGrid: new contributions in Remote Terminal Units" highlights the importance of Remote Terminal Units in today's and tomorrow's electrical network. The Remote Terminal Units are the main representative of the embedded systems in the electrical network and they are the key elements of the electric substations which are the backbone of the electrical system as a whole.

Therefore, in this thesis new contributions are made to different systems of the electrical network, such as Protection System, Synchronization System, and Management and Maintenance System, in which the Remote Terminal Units are main object of the research activity of the thesis.

In addition, the research work takes into account important SmartGrid standards, such as IEC61850 (the main Substation Automation standard), IEC61508 (for functional safety), IEEE1686 and IPSec (for cybersecurity) and IEEE1588 (for synchronization), as well as new technologies such as White-Rabbit, Internet of Things, Social Networks, Social Internet of Things, Natural Language Processing, among others.

Accordingly, the thesis studies the three following aspects, in the context of the electric substation:

- The protection systems, where a "New Adaptive Protection System Based on the Standard IEC61850" is proposed, which allows the dynamic reconfiguration of the protection devices in order to implement advanced solutions for faults treatment in the electrical distribution network.
- High availability and safe Automation Systems contributing with a "New Redundant Precision Synchronization Networks Based on White-Rabbit Technology for Reliable Substations" that offer a significant improvement regarding the accuracy and availability of the system.
- The "Design of a New Management and Maintenance System for Electrical Substations Based on the Social Internet of Things" where in order to adapt to the new digital world scenario, the interaction with the RTUs is redefined, enabling most agile and efficient access to the electrical substation information.

Finally, new future research lines are presented, taking the Remote Terminal Units as a key element and using Artificial Intelligence as the main technology for the potential developments.

Glosario de Términos

ADMS (Advanced Distribution Management System): Sistema avanzado de la gestión de la distribución.

AMI (Advanced Meter Infrastructure): Infraestructura de Medida Avanzada de contadores eléctricos.

AMM (Advanced Metering Management): Gestión Avanzada de la Medida de contadores eléctricos.

AMQP (Advanced Message Queuing Protocol).

AMR (Automatic Meter Reading) o Lectura Automática de contadores eléctricos.

AoT (Agents of the Things): Agentes de las Cosas.

API (Application Programming Interface): Interfaz de Programación de Aplicaciones.

ARTEMIS: plataforma tecnológica Europea de Sistemas Embebidos.

ASCII (American Standard Code for Information Interchange).

ASONAM (Advances in Social Networks Analysis and Mining).

B2C (Business to Customer): negocio-consumidor.

BC (Boundary Clocks): Relojes Frontera.

BOM (Bill Of Materials): lista de materiales.

Bots: programa de envío de mensajes automáticos que interacciona con humanos y otros programas.

C2B (Customer to Business): consumidor-negocio.

CB (Circuit Breakers): interruptores.

CDC (Common Data Class): Clase de Datos Común de los Nodos Lógicos del IEC61850.

CERN: Consejo Europeo para la Investigación Nuclear.

CID (Configured IED Description): Fichero de configuración de dispositivos electrónicos inteligentes.

CoAP (Constrained Application Protocol).

CPU (Central Processing Unit): Unidad central de procesamiento.

CRM (Customer Relationship Management): Gestión de las Relaciones con Clientes.

DA (Data Attributes): Atributos de Datos de los Nodos Lógicos del IEC61850.

DANs (Double Attached Nodes): nodos del Parallel Redundancy Protocol.

DC (Diagnostic Coverage): Cobertura de diagnóstico.

DCS (Distributed Control System)

DDMTD (Dual Digital Mixer Time Difference).

DDS (Data Distribution Service).

DMS (Distribution Management System): Sistema de Gestión de la Distribución.

DN (Distribution Networks): redes de distribución eléctrica.

DO (Data Objects): Objetos de Datos de los Nodos Lógicos del IEC61850.

DSO (Distribution System Operators): Operadores de los Sistemas de Distribución.

Eclipse: plataforma de software compuesto por un conjunto de herramientas de programación de código abierto.

EDIF (Electronic Design Interchange Format): esquemático del diseño electrónico.

EMS (Energy Management System): Sistema de Gestión Eléctrico.

ERP (Enterprise Resource Planning): sistemas de planificación de recursos empresariales.

FBD (Function Block Diagram): lenguaje de programación del estándar IEC61131-3.

Feeder: salidas de los alimentadores de la Subestación.

FFU (Fast Forwarding Unit): Unidad de Envío Rápido.

FITS (Field Failure Rate): tasa de fallo de campo.

FLISR (Fault Location Isolation and Supply Restoration): localización de fallos, aislamiento y restablecimiento del servicio.

FMEDA (Failure Modes Effects and Diagnostics Analysis): Análisis de Diagnósticos, Efectos y Modos de Fallo.

FPGA (Field-Programmable Gate Array): matriz de puertas programables.

Front-end: concentrador de comunicaciones.

FSU (Fast Switchover Unit): Unidad de Conmutación Rápida.

FTA (Fault Tree Analysis): análisis de fallos en árbol.

GIS (Geographic Information Systems): Sistemas de Información Geográfica.

GM (Grand Master): Maestro de Sincronización.

GNI per capita (Gross National Income per capita): la renta nacional per capita.

GOOSE (Generic Object-Oriented Substation Events): Eventos de Subestación genéricos orientados a objetos del estándar IEC61850.

GPS (Global Positioning System): Sistema de Posicionamiento Geográfico.

HMI (Human Machine Interface): Interfaz Hombre Máquina.

HSR (High-availability Seamless Redundancy): protocolo redundante de comunicación industrial.

HTTP (Hypertext Transfer Protocol).

HU_A: módulo CPU de la familia de productos Saitel DR de Schneider Electric.

IEA (International Energy Agency): Agencia Internacional de la Energía.

IEC (International Electrotechnical Commission): Comisión Electrotécnica Internacional.

IED (Intelligent Electronic Device): Dispositivo Electrónico Inteligente.

IEEE (Institute of Electrical Electronics Engineers).

IETF (Internet Engineering Task Force).

IIC (Industrial Internet Consortium).

IIoT (Industrial IoT): Industrial Internet de las Cosas.

IL (Instruction List): lenguaje de programación del estándar IEC61131-3.

IoT (Internet of Things): Internet de las Cosas.

IP core (intellectual property core).

IPsec (Internet Protocol security): Protocolo de seguridad de internet.

IRIG-B (Inter Range Instrumentation Group – rate 100 PPS).

JVM (Java Virtual Machine): máquina virtual java.

KPI (Key Performance Indicator): indicador clave de rendimiento o métricas

L2TPv3 (Layer 2 Tunneling Protocol version3): Protocolo estático de tunelización de capa 2 versión3.

LAN (Local Area Network): Red de área local.

LD (Ladder Diagram): lenguaje de programación del estándar IEC61131-3.

LD (Logical Device): dispositivos lógicos del estándar IEC61850.

LN (Logical Nodes): Nodos Lógicos del estándar IEC61850.

LS (Logic Selectivity): Selectividad Lógica.

LTE (Long Term Evolution) o 4G: Cuarta generación de telefonía móvil o celular.

M2H: Máquina a Humano.

M2M: Máquina a Máquina.

MAC (Media Access Control).

MDM (Meter Data Management): Gestión de datos de los contadores inteligentes.

MMS (Manufacturing. Message Specification): Especificación de Mensajes de Fabricación del estándar IEC61850.

MQTT (Message Queuing Telemetry Transport).

MV (Medium Voltage): Media Tensión.

NIST (National Institute of Standards and Technology): Instituto Nacional de Estándares y Tecnologías de Estados Unidos.

NTP (Network Time Protocol): Protocolo de sincronización de red.

OMS (Outage Management System): Sistema de Gestión de Incidencias.

OPC UA (OLE for Process Control Unified Architecture).

OSI (Open System Interconnection): Modelo de interconexión de sistemas abiertos.

OAuth (Open Authorization): estándar abierto que permite flujos simples de autorización para sitios web o aplicaciones informáticas.

P2P: Peer-to-Peer.

PLC (Power Line Communications): comunicaciones mediante línea de potencia.

PLC (Programmable Logic Controller): Controlador Lógico Programable.

PLN: Procesamiento de Lenguaje Natural.

PMU (Phasor Measurement Unit): sincrofasores.

POU (Program Organization Units).

PPP (Point-to-Point Protocol).

PPS (pulse per second): Pulso por Segundo.

PPSi (PTP Ported to Silicon): un PTP portable desarrollado en el proyecto White Rabbit y bajo licencia GNU LGPL.

PRP (Parallel Redundancy Protocol): protocolo redundante de comunicación industrial.

PSTN (Public Switched Telephone Network).

PTP (Precision Time Protocol).

PYME: Pequeñas y Medianas Empresas.

RedBox: permite unir anillos HSR a redes convencionales.

RTU (Remote Terminal Unit): Unidad Terminal Remota.

SAIDI (System Average Interruption Duration Index): mide la media de tiempo que los consumidores están sin servicio por consumidor conectado a la red.

SAIFI (System Average Interruption Frequency Index): es una medida del número total de interrupciones experimentadas por los consumidores por número total de consumidores conectados a la red de distribución.

SARTECO: Sociedad de Arquitectura y Tecnología de Computadores.

SAS: Sistema de Automatización de Subestación.

SAU (Substation Automation Unit): Unidad de Automatización de Subestación.

SCADA (Supervisory Control And Data Acquisition).

SCL (Substation Configuration Language): Lenguaje para Descripción de Subestaciones del estándar IEC61850.

Self-healing: proceso automatizado de auto curación o auto cicatrización de la red.

SFC (Sequential Function Chart): lenguaje de programación del estándar IEC61131-3.

SFF (Safe Failure Fraction): porcentaje de fallos de seguridad.

SIL (Safety Integrity Level): Integridad de seguridad del sistema.

SIoT (Social Internet of Things): Internet Social de las Cosas.

SM_CPU866e: módulo CPU de la familia de productos Saitel DP de Schneider Electric.

SM_DO32T: módulo de salidas digitales de la familia de productos Saitel DP de Schneider Electric.

SmartGrid: Redes de Electricidad Inteligentes.

SN (Social Networking): Redes Sociales.

SNTP (Simple Network Time Protocol).

ST (Structured Text): lenguaje de programación del estándar IEC61131-3.

STOMP (Streaming Text Oriented Messaging Protocol).

SV (Sampled Values) del estándar IEC61850.

SyncE (Synchronous Ethernet): Ethernet síncrono.

TC (Transparent Clocks): Relojes Transparentes.

TC57 (Technical Committee 57): International Electrotechnical Commission, Power systems management and associated information exchange.

TCP/IP (Transmission Control Protocol/Internet Protocol): Protocolo transmisión de control/ Protocolo de Internet.

THR (Tolerable Hazard Rate): tasa de riesgo tolerable.

TIC: Tecnologías de la Información y Comunicaciones.

TSO (Transmission System Operators): Operadores de Sistemas de Transmisión.

UDP (User Datagram Protocol): protocolo de datagramas de usuario.

UE: Unión Europea.

URL (Uniform Resource Locator).

Utilities: Denominación genérica de aquellas compañías que ofrecen servicios públicos como electricidad, gas o agua.

VPN (Virtual Private Network): red privada virtual.

WAN (Wide Area Network): Red de área extensa.

WR (White-Rabbit): Sistema de sincronización.

WR-LEN (White-Rabbit-LEN): nodos White-Rabbit diseñados para trabajar en cascada

WRS (White-Rabbit Switch).

XML (eXtensible Markup Language): Lenguaje de Marcas Extensible.

XMPP (extensible Messaging and Presence Protocol).

λDU: parámetro que cuantifica la tasa de fallos no detectados.

Capítulo 1. Introducción

1.1 El Sector Eléctrico

En la actualidad, el sector eléctrico se enfrenta a varios desafíos críticos. Seguramente el más importante es la necesidad de responder a la creciente demanda por el drástico aumento de la población mundial. La población mundial alcanzó los 1.000 millones de personas después de casi 200.000 años de existencia de la humanidad. Fueron necesarios 100 años más para llegar hasta los 2.000 millones, lo que ocurrió a principios del siglo XX, y posteriormente, el 31 de octubre de 2011 se alcanzaron los 7.000 millones, lo que duplicó la población de los últimos 40 años. En la actualidad, hay más de 7.600 millones de personas y si bien la población mundial continúa aumentando, este crecimiento es más lento que en el pasado. De esta forma, se prevé que la población mundial llegue a ser de entre 9.500 y 13.300 millones en 2100 [1], como se presenta a continuación.

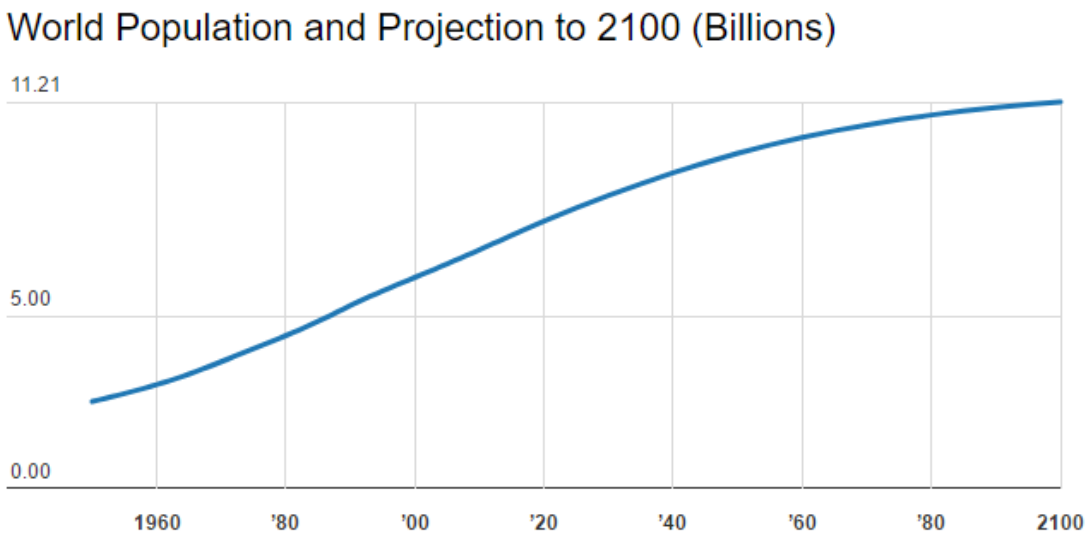

Figura 1: Histórico desde mediados del siglo XX y proyección de la población mundial. [Fuente: Naciones Unidas https://esa.un.org/unpd/wpp/]

Este crecimiento demográfico se traduce en un aumento de la demanda energética que se multiplica debido al aumento de los niveles de industrialización y urbanismo de las nuevas economías y por los nuevos modos de consumo, por ejemplo, el vehículo eléctrico.

El aumento de la población y el incremento del nivel de desarrollo de los países emergentes hacen que, según la IEA (International Energy Agency), para 2030 se dupliquen las necesidades de energía respecto a 2006 como se ilustra a continuación:

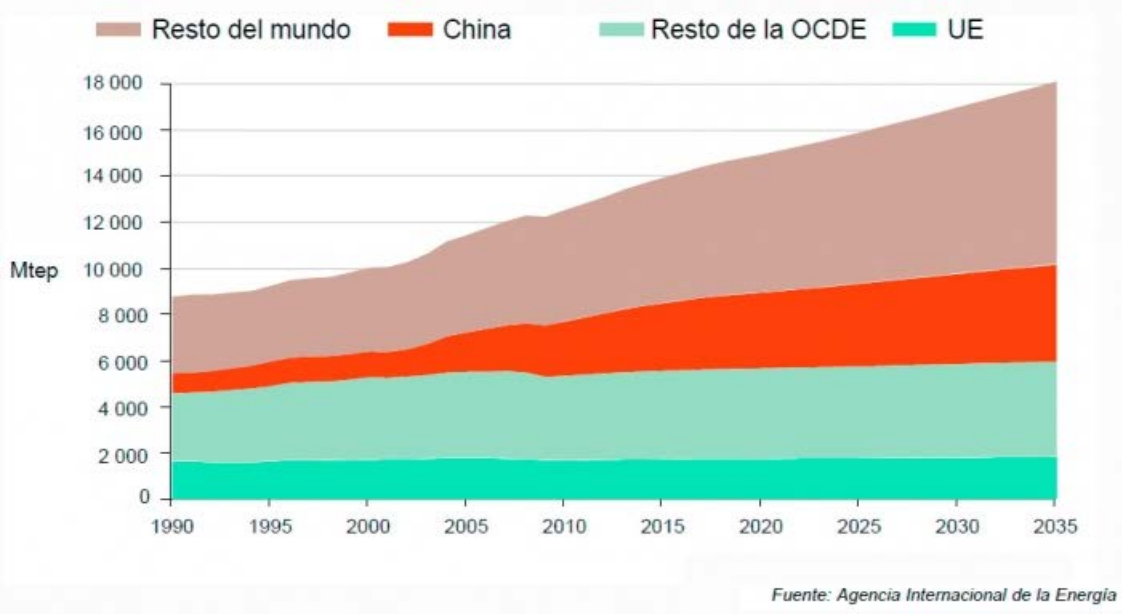

Figura 2: Evolución de la demanda energética mundial en millones de toneladas equivalentes de petróleo (Mtep). [Fuente: Agencia Internacional de la Energía]

En este contexto, el futuro se puede decir que estará electrificado. El uso de la electricidad crece imparablemente a nivel mundial, representando el 40% del aumento del consumo hasta 2040, que es el mismo porcentaje de crecimiento que el que tuvo el petróleo en los últimos 25 años [2]. Seguidamente se presenta de forma ilustrada la demanda de electricidad a nivel mundial por región y su crecimiento esperado:

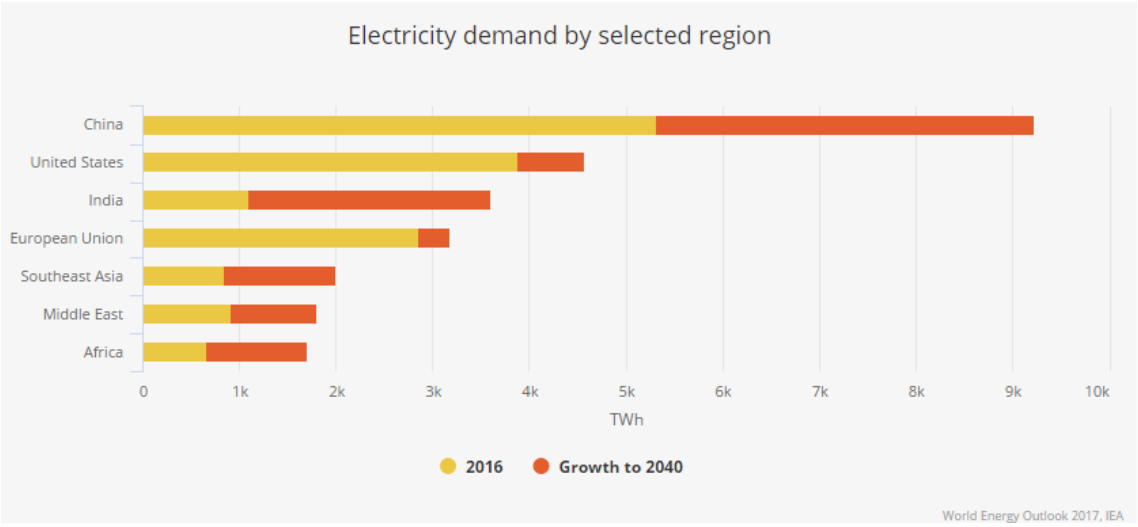

Figura 3: Demanda de electricidad mundial por región en TWh. [Fuente: Agencia Internacional de la Energía]

Del mismo modo, otro de los desafíos del sector eléctrico es cumplir con los objetivos a nivel mundial que consisten en disminuir las emisiones de CO_2. Dichos objetivos han sido adoptados por Europa a través de las medidas contra el cambio climático: los llamados

objetivos 20-20-20 (reducir las emisiones de gases de efecto invernadero en un 20%, ahorrar el 20% del consumo de energía mediante una mayor eficiencia energética, promover las energías renovables hasta el 20% del consumo energético). Para 2030, los objetivos son la reducción de al menos el 40% de las emisiones de gases de efecto invernadero con respecto a 1990, al menos el 27% del consumo total de energía procedente de energías renovables, e incremento de al menos el 27% de la eficiencia energética. Así mismo, los objetivos a largo plazo para 2050 de la UE son reducir sustancialmente sus emisiones —en un 80-95% con respecto a los niveles de 1990—, uniendo así sus esfuerzos a los del conjunto de los países desarrollados [3].

Igualmente, hay que tener en cuenta que las infraestructuras actuales tienen una capacidad de generación limitada y fueron diseñadas para operar en un escenario que dista mucho del actual. Centrándonos en el sistema eléctrico, disponemos de redes eléctricas que fueron diseñadas para operar de forma radial, soportando grandes instalaciones de generación que sirven a los consumidores por medio de un sistema de transmisión o transporte y distribución que funcionaba esencialmente en un solo sentido. Sin embargo, a las redes se les pide que acepten la electricidad de distintos tipos de fuentes de energía renovable de multitud de pequeños generadores (además de nuevas grandes instalaciones) distribuidos heterogéneamente sin consideración de ningún tipo de estructura jerarquizada. Así, la actual operación de las redes de distribución está condicionada por la explotación radial de las mismas, además de que a ese hecho hay que sumarle la poca información respecto a medidas con que cuentan los operadores para ejercer la gestión.

A estos cuatro hechos presentados, como son el crecimiento de la población, la necesidad de reducción del CO_2 que lleva aparejado las fuentes de energía renovable, la importancia del uso de la electricidad y la limitación de las infraestructuras, se les suman otros tres elementos que se postulan como las bases del futuro.

Por un lado, la aparición de nuevas tecnologías tanto de información y comunicaciones, como son el Internet de las Cosas, la sincronización, la seguridad y ciberseguridad, así como las nuevas tecnologías de potencia y almacenamiento. Por otro lado, la actividad a nivel regulatorio de los gobiernos e instituciones para alcanzar los objetivos de eficiencia y reducción de CO_2. Y, por último, la entrada en escena del usuario final con un rol activo en lo que respecta al consumo, a su interacción con el mercado, así como su nivel de concienciación en cuanto a la sostenibilidad del planeta.

En este contexto, surge el concepto de SmartGrid como solución para las redes eléctricas que se anuncia como pieza clave para el sector eléctrico actual.

1.2 Motivación y Objetivo de la Tesis

SmartGrid es un concepto que, como se verá más adelante, requiere de múltiples sistemas interaccionando en distintas capas. Los importantes progresos tecnológicos en el dominio del desarrollo software que se han realizado en los últimos años, hacen que gran parte de los esfuerzos de investigación y desarrollo en el campo de SmartGrid se centren en los sistemas y aplicaciones en las que la componente software es el elemento

predominante. Así, por ejemplo, el Sistema de Gestión de la Distribución, el Sistemas de Información Geográfica y el Sistema de Gestión Eléctrico son los verdaderos buques insignia de las empresas dominantes en el sector eléctrico. Además, dichas empresas están apostando por incluir en sus sistemas conceptos muy actuales como BigData, Analítica de Datos, Inteligencia Artificial, Internet de las Cosas (IoT), Virtualización, Machine Learning, Deep Learning, Digital Twin, etc., que no dejan de ser esencialmente software.

En este contexto, en el que la Digitalización se presenta como la próxima evolución de SmartGrid, los dispositivos y equipos englobados en el concepto de sistemas embebidos parecen carecer del más mínimo futuro.

En esta tesis, titulada “El futuro de los Sistemas Embebidos en SmartGrid: nuevas aportaciones en Unidades Terminales Remotas” se trata de poner de manifiesto la importancia de dichos sistemas embebidos, los cuales, aunque no suelen formar parte de las grandes campañas de marketing de las empresas dominantes del sector, juegan un papel indiscutible en la red eléctrica de hoy y del mañana. En este sentido, los sistemas embebidos, no solo son importantes como tecnología habilitadora para las mencionadas aplicaciones y sistemas, en lo que sería un papel secundario, sino que en ciertos dominios adoptan un papel protagonista en la venidera evolución de SmartGrid.

Por consiguiente, la presente tesis se centra en la RTU (Unidad Terminal Remota), que por sus características y versatilidad es el representante ideal de los sistemas embebidos en SmartGrid. Las RTUs se encuentran en las Subestaciones Eléctricas que, como se explicará más adelante, son la base fundamental del sistema eléctrico en su conjunto y son los elementos que lo vertebran.

Así pues, la RTU es el sistema embebido clave sobre el que se articulan las contribuciones a la evolución de SmartGrid que se presentan en la presente tesis y que versan sobre los tres aspectos siguientes, en el contexto de la Subestación eléctrica:

- Los sistemas de protección, donde se propone un “Nuevo Sistema de Protección Adaptativa Basado en el Estándar IEC61850”, que permita la reconfiguración dinámica de los dispositivos de protección para implementar soluciones avanzadas de tratamiento de faltas en la red eléctrica de distribución.
- Los sistemas de automatización con alta disponibilidad y seguridad, donde se avanza en “Nuevas Redes de Sincronismo Redundante de Precisión Basadas en Tecnología White-Rabbit para Subestaciones Confiables” que ofrezcan una mejora significativa de la precisión y disponibilidad.
- La “Concepción de un Nuevo Sistema de Gestión y Mantenimiento de Subestaciones Eléctricas Basado en Internet Social de las Cosas” en el que se redefina la interacción con las RTUs para adaptarse al nuevo mundo digital y que a su vez posibilite un acceso a la información más ágil y eficiente.

De esta forma, partiendo del estado del arte, se pretende estudiar tres ámbitos claves en el Sistema de Automatización de la Subestación, en los que se proponen contribuciones

científicas, con la RTU como denominador común, aportando nuevos elementos de diferenciación y valor añadido al mercado.

1.3 Organización de los Capítulos

La tesis se estructura de la siguiente forma. En primer lugar, en el “Capítulo 2” se exponen los conceptos de Smart Grid y Sistemas Embebidos, donde se justifica la elección de la RTU como representante más adecuado de los sistemas embebidos en SmartGrid.

A continuación, en el “Capítulo 3”, se expone el Estado del Arte de las tecnologías bajo estudio en la presente tesis, las cuales son clave para el futuro de los sistemas embebidos en el marco de SmartGrid y, por tanto, íntimamente relacionadas con la RTU. De esta forma, en primer lugar, se estudia el estándar IEC61850, se introducen los conceptos de seguridad y se estudian los sistemas de protección de la red eléctrica. Posteriormente, se introduce la sincronización en la RTU en el contexto de un Sistema de Automatización de Subestaciones. Seguidamente, se presenta el concepto del Internet Social de las Cosas, tomando como punto de partida el paradigma de Internet de las Cosas, las Redes Sociales y el Procesamiento de lenguaje Natural.

Los siguientes tres capítulos resumen la labor científica realizada, y presentan las principales contribuciones a SmartGrid desde el mundo de los sistemas embebidos.

En el “Capítulo 4” se presenta un “Nuevo Sistema de Protección Adaptativa Basado en el Estándar IEC61850”, donde las RTUs, actuando como Dispositivos Electrónicos Inteligentes de protección, implementan funciones que reducen el número y la duración de las interrupciones de suministro eléctrico. Además, para la implementación de dichas funciones, se hace un uso novedoso del estándar IEC61850, para lo cual se utilizan los servicios de intercambio de información de tiempo crítico a través de internet de dispositivos de campo de dicho estándar.

En el “Capítulo 5” se tratan las “Nuevas Redes de Sincronismo Redundante de Precisión Basadas en Tecnología White-Rabbit para Subestaciones Confiables”, donde se justifica que para poder operar eficientemente la red y realizar análisis rigurosos de la misma se requiere una referencia de tiempo común y determinista en los distintos sistemas que la componen y en particular en los sistemas embebidos. En este capítulo se estudia dicha necesidad, utilizando el caso de uso del Sistema de Automatización de Subestación, como elemento clave de SmartGrid, en donde los sistemas embebidos tienen un papel fundamental teniendo como pieza clave la RTU.

En el “Capítulo 6” se describe la “Concepción de un Nuevo Sistema de Gestión y Mantenimiento de Subestaciones Eléctricas Basado en Internet Social de las Cosas” y se presenta una implementación para mejorar la gestión y el mantenimiento de las Subestaciones eléctricas. La solución se basa en el paradigma de las redes sociales aplicado al mundo de Internet de las Cosas sobre la RTU, y ofrece un enfoque novedoso en el mundo del control en tiempo real de SmartGrid, yendo más allá del concepto clásico de comunicación Máquina a Máquina y Máquina a Humano en la interacción entre RTUs-usuarios.

En último término, se presentan las conclusiones derivadas de la labor científica realizada y el listado de las referencias utilizadas durante la elaboración de esta tesis.

1.4 Publicaciones Derivadas de la Investigación

A continuación se presentan el listado de publicaciones y trabajos relacionados con la tesis:

- Accurate Timing Networks for Dependable Smart Grid Applications. IEEE Transactions on Industrial Informatics, Volume 14, Issue 5 (Diciembre 2017). **Francisco Ramos** (Schneider Electric); José Luis Gutiérrez-Rivas (Seven Solutions); José López-Jiménez (Seven Solutions); Benito Caracuel (Schneider Electric); Javier Diaz (Seven Solutions)

  http://ieeexplore.ieee.org/document/8239829/

  IEEE Transactions on Industrial Informatics: La revista se enfoca en los siguientes temas principales: automatización flexible y colaborativa de fábrica, paradigmas computacionales y de control distribuido, sistemas de monitorización y control basados en Internet, software de control en tiempo real para procesos industriales, Java y Jini en entornos industriales, control de sensores inalámbricos y actuadores, interoperabilidad de sistemas e interfaz hombre-máquina.

  Factor de impacto: 6,764 JCR (Journal Citation Reports).

- IEC61850-based adaptive protection system for the MV distribution SmartGrid. ELSEVIER Sustainable Energy, Grids and Networks, ELSEVIER Magazine (October 2017). Amelia Alvarez de Sotomayor, **Francisco Ramos** (Schneider Electric), Davide Della Giustina, Alessio Dedè, Giovanni Massa, Antimo Barbato (Unareti SpA)

  http://www.sciencedirect.com/science/article/pii/S2352467716302077

  Sustainable Energy, Grids and Networks: publicación para investigación teórica y aplicada en el dominio de la energía, las redes de información y las redes de energía, incluidas las redes inteligentes.

  Factor de Impacto: 1.560 SNIP (Source Normalized Impact per Paper).

- Toward an Adaptive Protection System for the Distribution Grid by using the IEC 61850. Proc. of the IEEE International Conference on Industrial Electronics (ICIT-2015). Davide Della Giustina, Alessio Dedè (A2A Reti Elettriche SpA); Amelia Alvarez de Sotomayor, **Francisco Ramos** (Schneider Electric).

  http://ieeexplore.ieee.org/document/7125448

  IEEE International Conference on Industrial Technology es una de las conferencias anuales principales de la IEEE Industrial Electronics Society, dedicada a la difusión de nuevas ideas, investigaciones y trabajos en curso en los campos de los sistemas de control inteligente, robótica, comunicaciones y automatización en fábricas, fabricación flexible, adquisición de datos y procesamiento de señales, sistemas de visión y electrónica de potencia.

- Secure layer 2 tunneling over IP for GOOSE-based logic selectivity. IEEE International Conference on Industrial Technology (ICIT-2017). Peyman Jafary, Ontrei Raipala, Sami Repo, Mikko Salmenperä, Jari Seppälä, Hannu Koivisto (TUT), Seppo Horsmanheimo, Heli Kokkoniemi-Tarkkanen, Lotta Tuomimäki, (VTT), Amelia Alvarez, **Francisco Ramos** (Schneider Electric), Alessio Dede, Davide Della Giustina (Unareti)

  http://ieeexplore.ieee.org/document/7915428/

  IEEE International Conference on Industrial Technology es una de las conferencias anuales principales de la IEEE Industrial Electronics Society, dedicada a la difusión de nuevas ideas, investigaciones y trabajos en curso en los campos de los sistemas de control inteligente, robótica, comunicaciones y automatización en fábricas, fabricación flexible, adquisición de datos y procesamiento de señales, sistemas de visión y electrónica de potencia.

- Towards Industrial Internet vision: SIoT-based control system for Electric Substations. Jornadas SARTECO de la Sociedad de Arquitectura y Tecnología de Computadores (Septiembre 2015). **F. Ramos** (Schneider Electric), C. Luján-Martínez (US), J. Fuentes (US), L. Collar(US) and A. Torralba (US).

  Las Jornadas SARTECO, entre otras integra las VI Jornadas de Computación Empotrada (JCE2015). Las Jornadas de Computación Empotrada nacen con el espíritu de crear un foro de debate y cooperación entre investigadores y expertos del área para presentar los desarrollos más recientes en este campo.

- Smart Grid y los Sistemas Embebidos. Trabajo Fin de Master, Máster en Ingeniería de Computadores y Redes de la Universidad de Granada (Julio 2012). Autor: **Francisco Ramos Peñuela**. Tutores: Dr. Héctor Pomares Cintas y Dr. Miguel Damas Hermoso.

1.5 Patente Derivada de la Investigación

Título: “Method for setting up a Remote Terminal Unit for social networking”.

Referencia EP18305562.3.

Inventor: **Francisco Ramos**.

Depositada el 4 de mayo de 2018.

1.6 Proyectos de I+D Relacionados

El investigador de la presente tesis ha participado activamente en más de 50 proyectos de I+D colaborativos de ámbito nacional e internacional, estando relacionados con la labor científica aquí presentada cinco de ellos (EMC2, IDE4L, INFIERE, 3S-CS y SAGRA) cuya información general es presentada seguidamente. En dichos proyectos se ha participado activamente (definiendo los proyectos, investigando y dirigiendo los trabajos de Schneider Electric en los mismos), siendo el investigador principal del proyecto INFIERE.

- EMC2 (Embedded Multi-Core Systems for Mixed Criticality Applications in Dynamic and Changeable Real-Time Environments). El objetivo del proyecto EMC2 fue fomentar el desarrollo de los sistemas embebidos multinucleo a través de un enfoque hacia una arquitectura orientada a servicios innovadora y sostenible para aplicaciones con niveles mixtos de criticidad en entornos de tiempo real dinámicos y cambiantes. Este proyecto incluyó un demostrador enfocado a IoT en el dominio de SmartGrid.

  EMC2 fue parte de la estrategia industrial europea de los sistemas embebidos para mantener su posición líder proporcionando soluciones para:

  - Adaptabilidad dinámica en Sistemas Abiertos.
  - Utilización de costosas prestaciones del sistema solamente en la modalidad bajo demanda, para así reducir el coste total del sistema.
  - Manejo de aplicaciones con niveles mixtos de criticidad en entornos de tiempo real.
  - Escalabilidad y máxima flexibilidad.
  - Despliegue a gran escala y gestión de las cadenas integradas de herramientas, durante todo el ciclo de vida.
  - Retos en las fuentes de alimentación por los cambios operacionales en los sistemas en tiempo real MCMC (Multi-core / Many-core).

  Cofinanciado por ARTEMIS (Grant agreement: 621429) y Ministerio de Industria, Energía y Turismo (Ref: ART-010000-2014-1).

  Socios: 98 socios de la industria e investigación de los sistemas embebidos de 19 países europeos: Infineon, Schneider Electric, Siemens, EADS, Fraunhofer, Freescale, Rockwell, Thales, CEA, TECNALIA, TNO, TUDelft, Manchester Unv, KTH, ERICSSON, ABB, PHILIPS, BMW, VOLVO, NXP Airbus, SYSGO, TomTom, entre otros.

  Presupuesto: 93 millones de euros.

  Más información en: http://www.emc2-project.eu/

- IDE4L (Ideal Grid for All). Basándose en el desarrollo conceptual de Red de Distribución Activa, el proyecto IDE4L se centró en la integración de Recursos Energéticos Distribuidos en las redes de distribución con el fin de reducir las emisiones de CO_2, ahorrar energía, reducir las pérdidas, mejorar la monitorización y el control de la red, hacer un uso más eficiente de las redes existentes y mejorar

la visibilidad de los Recursos Energéticos Distribuidos en los operadores del sistema y los agregadores.

El objetivo del proyecto IDE4L fue el estudio de soluciones inteligentes para el diseño y operación de las redes de distribución con un alto grado de penetración de Recursos Energéticos Distribuidos, garantizando la continuidad y la calidad del suministro eléctrico.

Financiado por la Comisión Europea FP7. Grant agreement: 608860.

Socios: TUT, Schneider Electric, Dansmarks Tekniske Universitet, RWTH Aachen University, Univ. Carlos III of Madrid, KTH, Dansk Energi, IREC, Unión Fenosa Distribución, A2A Reti Electtriche SpA, Ostkraft.

Presupuesto: 8 millones de euros.

Más información en: http://ide4l.eu/

- INFIERE (INvestigation of the Future Intelligent Elements for Renewable Energy). El objetivo del proyecto consistió en la investigación de cómo aplicar el paradigma de Internet de las Cosas, las Redes Sociales Cooperativas y sus aspectos de topología a los dispositivos RTU en el contexto de SmartGrid.

  Financiado por INVEST IN SPAIN/ICEX y los Fondos de Desarrollo Regionales Europeos. Ref: 1/2014-007.

  Presupuesto: 200.000€.

  Más información en: https://www.schneider-electric.com/en/work/products/medium-voltage-switchgear-and-energy-automation/r-and-d-projects/infiere.jsp

- SAGRA (Sistema Avanzado para Gestión de Redes Aisladas). El objetivo del proyecto fue el desarrollo de un sistema avanzado para la gestión de redes aisladas con generación y almacenamiento distribuido e IoT. El proyecto se divide en tres pilares interrelacionados entre sí: Sistema de Monitorización Inteligente, Sistema de gestión de generación y almacenamiento en redes aisladas con emulación de la red basado en Hardware-in-the Loop (HIL), y Mantenimiento predictivo de los sistemas y equipos involucrados.

  Co-Financiado por CDTI y la Junta de Andalucía. Programa Innterconecta. Ref: ITC-20151067.

  Socios: Schneider Electric, GPtech, Irradia, Solar Services y Universidad de Sevilla

  Presupuesto: 1,88 millones de euros.

  Más información en: https://www.schneider-electric.com/en/work/products/medium-voltage-switchgear-and-energy-automation/r-and-d-projects/sagra.jsp

- 3S-CS (Standardization Security Synchronization Connected Substation) se centra en el desarrollo de un sistema de control global de Subestaciones basado en IEC61850 y provisto de comunicaciones IoT. El proyecto incluye el desarrollo de una herramienta de configuración y monitorización IEC61850.

  Co-Financiado por CDTI y la Junta de Andalucía. Programa Innterconecta. Ref: ITC-20161012.

  Socios: Schneider Electric, Endesa Distribución Eléctrica, Integrasys, Isotrol.

  Presupuesto: 2,28 millones de euros.

  Más información en: https://www.schneider-electric.com/en/work/products/medium-voltage-switchgear-and-energy-automation/r-and-d-projects/3s-cs.jsp

Capítulo 2. Conceptos SmartGrid y Sistemas Embebidos

El presente capítulo muestra los conceptos de SmartGrid y Sistemas Embebidos, así como el nexo de unión entre ambos, identificándose los dispositivos denominados Unidades Terminales Remotas como el sistema embebido clave en el dominio de SmartGrid y en su futura evolución.

2.1 Concepto de SmartGrid

El concepto de SmartGrid o Red inteligente consiste en una red eléctrica que incluye una pluralidad de sistemas y dispositivos de operación de la red y fuentes de energía como son los contadores inteligentes, dispositivos inteligentes, energía renovable y recursos energéticamente eficientes [4]. SmartGrid combina las infraestructuras de electricidad con las tecnologías de la información y comunicaciones para integrar e interconectar a los usuarios, con objeto de realizar un balance continuo y eficiente de la producción y la demanda sobre una red compleja. Además, el acondicionamiento electrónico de potencia y el control de la producción y distribución de electricidad son aspectos fundamentales de SmartGrid [4].

La política de SmartGrid está organizada en Europa por la "European Technology Platform on Smartgrids" [5], y la política en los Estados Unidos se describe en "U.S. Code, Title 42, Chapter 152, subchapter IX, 17381 Statement of policy on modernization of electricity grid".

Por otro lado, instituciones como la Comisión Europea tratan de fijar el alcance del concepto de SmartGrid además de resaltar su importancia. Seguidamente se presenta la "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Redes inteligentes: de la innovación a la implantación" [6].

La Estrategia Europa 2020 presenta un claro mensaje para Europa. El crecimiento económico y el empleo de la Unión Europea (UE) en el futuro dependerán cada vez más de la innovación en productos y servicios destinados a los ciudadanos y empresas de la UE. La innovación también contribuirá a abordar uno de los retos más difíciles que tiene planteados Europa, a saber, la utilización eficiente y sostenible de los recursos naturales. El desarrollo de nuestra futura infraestructura energética debe reflejar esta idea. Si no se procede a una profunda mejora de las redes y sistemas de medida existentes, la producción de energía renovable quedará frenada, la seguridad de las redes se verá comprometida, se perderán oportunidades en materia de ahorro energético y eficiencia energética, y el mercado interior de la energía se desarrollará a un ritmo mucho más lento.

Una red inteligente puede describirse como una red de electricidad mejorada a la que se ha añadido un sistema de comunicación digital bidireccional entre el proveedor y el consumidor y sistemas de control y de medición inteligentes. La medición inteligente es habitualmente algo inherente a las redes inteligentes.

Los beneficios de las redes inteligentes se reconocen generalmente. Las redes inteligentes permiten una comunicación e interacción directas entre consumidores, familias o empresas, otros usuarios de la red y proveedores de energía. Estas redes abren nuevas posibilidades para que los consumidores controlen y gestionen directamente sus hábitos de consumo, al mismo tiempo que proporcionan fuertes incentivos para una utilización eficiente de la energía si se combinan con una modulación de los precios de la electricidad en función del periodo horario en que se consuma. Una gestión mejorada y más selectiva de la red aumentará la seguridad de ésta y abaratará su gestión. Las redes inteligentes constituirán el armazón del futuro sistema energético hipocarbónico y permitirán la integración de grandes cantidades de energía renovable producida en tierra y en el mar y de vehículos eléctricos, manteniendo al mismo tiempo la capacidad de producción de energía convencional y la adecuación del sistema energético. Por otra parte, la implantación de redes inteligentes proporciona una oportunidad de promover en el futuro la competitividad y el liderazgo tecnológico a nivel mundial de los proveedores de tecnología de la UE, tales como la industria de ingeniería electrónica y eléctrica, compuesta principalmente por Pequeñas y Medianas Empresas (PYME). Por último, las redes inteligentes proporcionan una plataforma para que las empresas energéticas tradicionales o los nuevos operadores del mercado, tales como las empresas del sector de las Tecnologías de la Información y Comunicación, incluidas las PYME, desarrollen servicios energéticos nuevos e innovadores al mismo tiempo que garantizan la protección de datos y la seguridad informática. Esta dinámica deberá fomentar la competencia en el mercado minorista, incentivar la reducción de las emisiones de gases de efecto invernadero y proporcionar una oportunidad para el crecimiento económico.

En resumen, haciendo abstracción del concepto, el objetivo es desarrollar un sistema para que la distribución eléctrica se realice de forma eficaz, económica, automatizada y confiable, de modo que se contribuya a aumentar la capacidad del sistema sin invertir en nuevas infraestructuras, contribuyendo así directamente a reducir las emisiones de CO_2, de modo que se establezcan las bases para mejorar el servicio al usuario final y poder avanzar en el concepto de gestión de la demanda y en la reducción de los picos de consumo.

2.1.1 Transformación de la red eléctrica

La red eléctrica se encuentra en un proceso de transformación para convertirse en las redes interconectadas, automatizadas e inteligentes del futuro. La transformación avanza hacia la digitalización (Internet de las Cosas, Analítica de datos, Ciberseguridad) [7], la sensorización, el control en tiempo real, la autoreparación, entre otros muchos aspectos que se presentan en la siguiente tabla [8]:

Today's grid vs. the smart grid

Today's grid	The smart grid
Centralized, utility-controlled generation with traditional fossil fuels	Decentralized generation with emphasis on renewables and demand response
Blind operation of generation assets with only a forecast of demand	Real-time monitoring and advanced control of connected sources and loads for dynamic balance
One-way energy flows with little situational awareness and slow response to outages	Two-way energy flows that require automation, outage management, and awareness
Manually switching to restore power based on trial and error	Self-healing grid that automatically prevents or minimizes outages
Passive and uninformed energy consumers	Better informed consumers actively participating with utilities
Focus on adding infrastructure (power plants, transmission lines, etc.) to meet demand	Focus on adding efficiencies and control to meet demand without building infrastructure
Static operating modes with minimal integration of operational data	Flexible operating modes with full integration of information and operational data
Grid is vulnerable to cyberterrorism and damage caused by natural disasters	Grid is resilient and intelligent, virtually eliminating or mitigating all types of attacks

Tabla 1: El pasado vs futuro SmartGrid. [Fuente: Schneider Electric Ebook Powering an "always on" world]

En la siguiente figura se ilustra la transformación, el pasado de la red, el presente y el futuro:

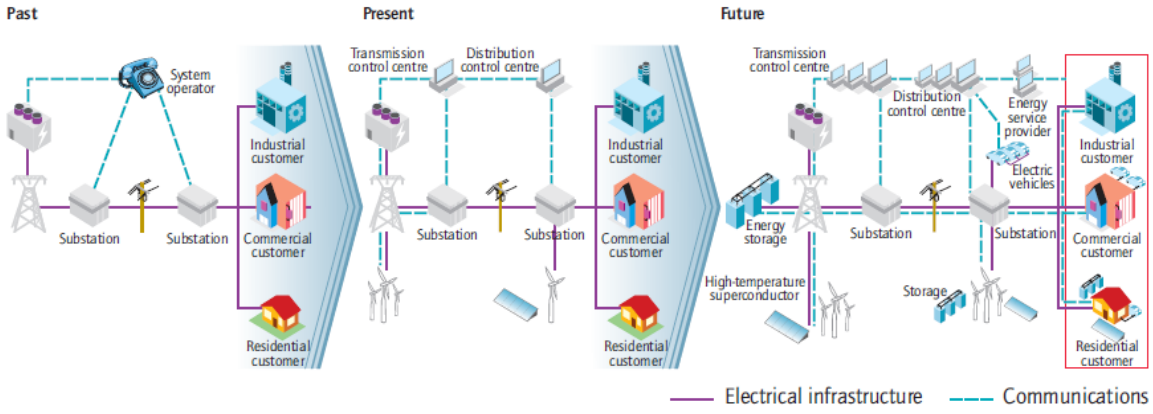

Figura 4: Representación del pasado, presente y futuro de la red eléctrica. [Fuente: Agencia Internacional de la Energía]

En la siguiente tabla, se representan las principales características que se implementarán en SmartGrid, realizando una comparación de dichas características con las equivalentes en la red eléctrica actual:

Característica	Red Eléctrica Actual	Smart Grid
Automatización.	Existencia muy limitada de elementos de monitorización, reservándose a la red de transporte.	Integración masiva de sensores, actuadores, tecnologías de medición y esquemas de automatización en todos los niveles de la red.
Inteligencia y control.	La red actual de distribución carece de inteligencia, implementando un control manual	Se enfatiza la creación de un sistema de información e inteligencia distribuidos en el sistema.
Autoajuste.	Se basa en la protección de dispositivos ante fallos del sistema.	Automáticamente detecta y responde a transmisiones actuales y problemas en la distribución. Su enfoque se basa en la prevención. Minimiza el impacto en el consumidor.
Participación del consumidor y generación distribuida.	Los consumidores están desinformados y no participan en la red. No se genera energía localmente, lo que implica un flujo energético unidireccional.	Incorporación masiva de generación distribuida, la que permite coordinarse a través de la red inteligente. En esta generación participa el usuario con la entrega del exceso energético generado localmente.
Resistencia ante ataques.	Infraestructuras totalmente vulnerables.	Resistente ante ataques y desastres naturales con una rápida capacidad de restauración.
Gestión de la demanda	No existe ningún tipo de gestión en la utilización de dispositivos eléctricos, en función de la franja horaria del día, o del estado de la red eléctrica.	Incorporación por parte de los usuarios de electrodomésticos y equipos eléctricos inteligentes, que permiten ajustarse a esquemas de eficiencia energética, señales de precio y seguimiento de programas de operación predefinidos.
Calidad eléctrica.	Solo se resuelven los cortes de suministro, ignorando los problemas de calidad eléctrica. De esta forma persisten problemas de huecos de tensión, perturbaciones, ruido eléctrico, etc.	Calidad eléctrica que satisface a industria y clientes. Identificación y resolución de problemas de calidad eléctrica. Varios tipos de tarifas para varios tipos de calidades eléctricas.
Vehículos eléctricos	Recientemente se están empezando a incorporar puntos de recarga eléctrica en la red, que sólo permiten la recarga de las baterías de los vehículos.	La incorporación de los vehículos eléctricos a la red, está demandando nuevas infraestructuras especializadas destinadas a la recarga y a permitir que cada vehículo pueda convertirse en pequeñas fuentes de generación.
Capacidad para todas las opciones de generación y almacenamiento.	Pocas grandes plantas generadoras. Existen muchos obstáculos para interconectar recursos energéticos distribuidos.	Gran número de diversos dispositivos generadores y almacenadores de energía, para completar a las grandes plantas generadoras. Conexiones "PlugAndPlay". Más enfocado en energías renovables.
Optimización del transporte eléctrico	En la actualidad se pierde una gran cantidad de energía debido a la poca eficiencia en el transporte eléctrico.	Sistemas de control inteligentes que permitan extender los servicios intercambiados entre los distintos agentes del mercado eléctrico y, asimismo, aprovechar eficientemente la capacidad de transmisión de la red.
Preparación de mercados.	Los mercados de venta al por mayor siguen trabajando para encontrar los mejores modelos de operación. No existe una buena integración entre éstos. La congestión en la transmisión separa compradores de vendedores.	Buena integración de los mercados al por mayor. Prósperos mercados al por menor. Congestiones de transmisión y limitaciones mínimas.
Optimización de bienes y funcionamiento eficiente.	Integración mínima de los datos de operación y la gestión de bienes. Mantenimiento basado en tiempo.	Sensado y medida de las condiciones de la red. Tecnologías integradas para la gestión de los bienes. Mantenimiento basado en las condiciones de la red.

Tabla 2: SmartGrid y la Evolución de la Red Eléctrica. [Fuente: Observatorio Industrial del Sector de la Electrónica, Tecnologías de la Información y Telecomunicaciones]

2.1.2 Arquitectura Global SmartGrid

Las distintas representaciones de la arquitectura de SmartGrid, incluyen básicamente: los centros de gestión y control, la generación clásica y la de fuentes renovables, elementos de almacenamiento, las redes de transmisión y distribución, los consumidores (industria, ciudades, oficinas, viviendas, contadores eléctricos, electrodomésticos, vehículo eléctrico, etc.), los aspectos relacionados con el entorno como por ejemplo la meteorología, entre otros.

En general se tratan las siguientes áreas tecnológicas:

- Gestión de la demanda.
- Almacenamiento.
- Distribución y transporte de la electricidad.
- Movilidad.
- Integración de renovables.

El Instituto Nacional de Estándares y Tecnologías de Estados Unidos (NIST: National Institute of Standards and Technology) ofrece una amplia representación en la que se estudian detalladamente los temas tecnológicos y de interrelaciones [9] como se presenta en la siguiente figura:

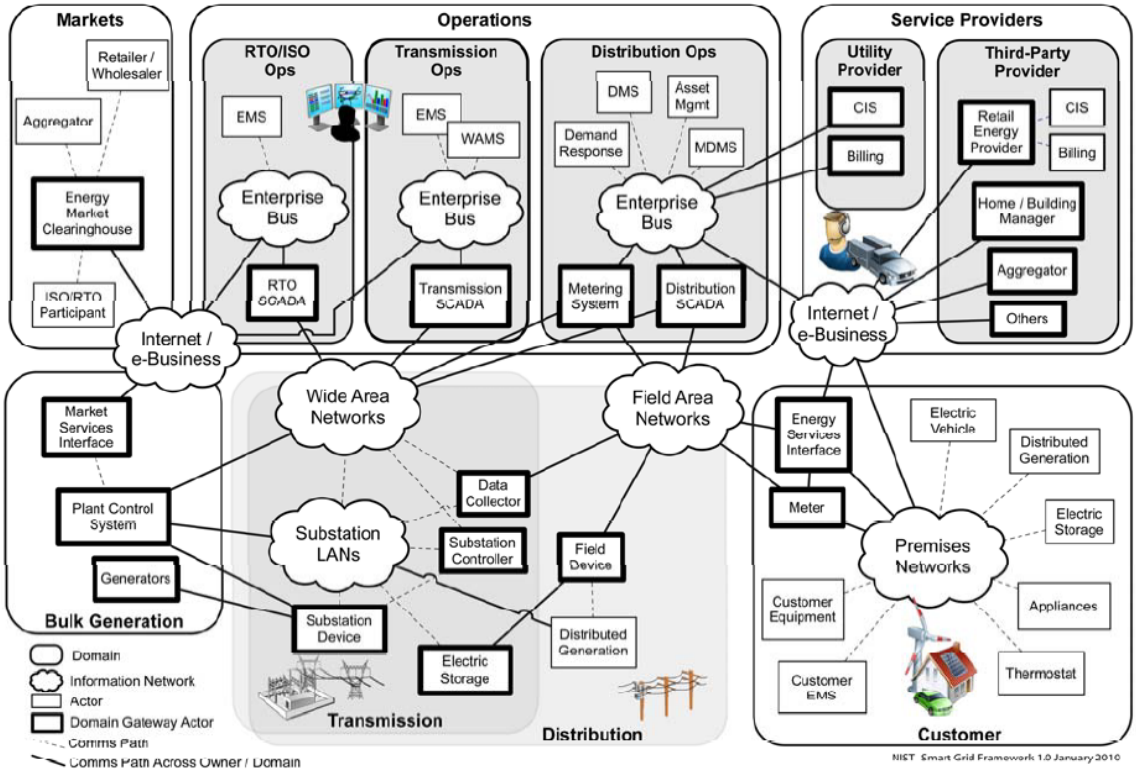

Figura 5: Diagrama conceptual de referencia para redes de información SmartGrid. [Fuente: Instituto Nacional de Estándares y Tecnologías de EE. UU.]

Por otro lado, el World Economic Forum [10] presenta una visión holística de SmartGrid, la cual se muestra seguidamente:

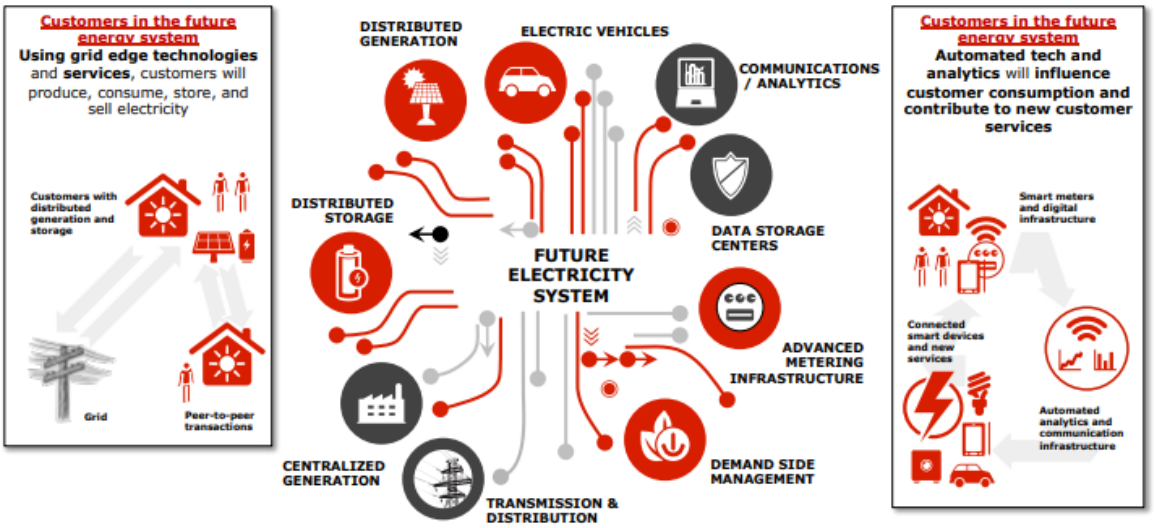

Figura 6: Representación holística de SmartGrid que incluye tanto generación como transmisión y distribución, así como el rol activo de los clientes del futuro. [Fuente: World Economic Forum]

2.2 Concepto de Sistemas Embebidos

Un sistema embebido consiste en un sistema de computación cuyo hardware y software están específicamente diseñados y optimizados para resolver un problema concreto eficientemente. El término "embebido" (también se le conoce como "empotrado") hace referencia al hecho que la electrónica o el sistema electrónico de control es una parte integral del sistema en que se encuentra. La característica principal que diferencia a los "embebidos" de los demás sistemas electrónicos es que, por estar insertados dentro del dispositivo que controlan, están sujetos en mayor medida a cumplir requisitos de tamaño, fiabilidad, consumo y coste, y su existencia puede no ser aparente [11].

ARTEMIS, plataforma tecnológica Europea de Sistemas Embebidos (www.artemis-ju.eu) introduce los sistemas embebidos como sigue:

"La mayoría de las personas no se dan cuenta de que, en la actualidad, la forma más común de computadora es la computadora embebida. De hecho, el 98% de los dispositivos de computación están embebidos en todo tipo de equipos electrónicos y máquinas. Las computadoras se encuentran en dispositivos cotidianos como tarjetas de crédito, teléfonos móviles, automóviles y aviones o lugares como casas, oficinas y fábricas. Los sistemas de computación embebidos están hechos de hardware (componentes nanoelectrónicos) y software."

Artemis fija el alcance de dichos sistemas tal como se muestra en la Figura 7, en donde representa tres dominios de investigación, como son: “arquitecturas y diseños de referencia”, “conectividad e Interoperabilidad” y “métodos y herramientas para el diseño de sistemas”, además de los contextos de aplicación: “industrial”, “entornos nómadas”, “espacios privados” e “infraestructuras públicas” [12].

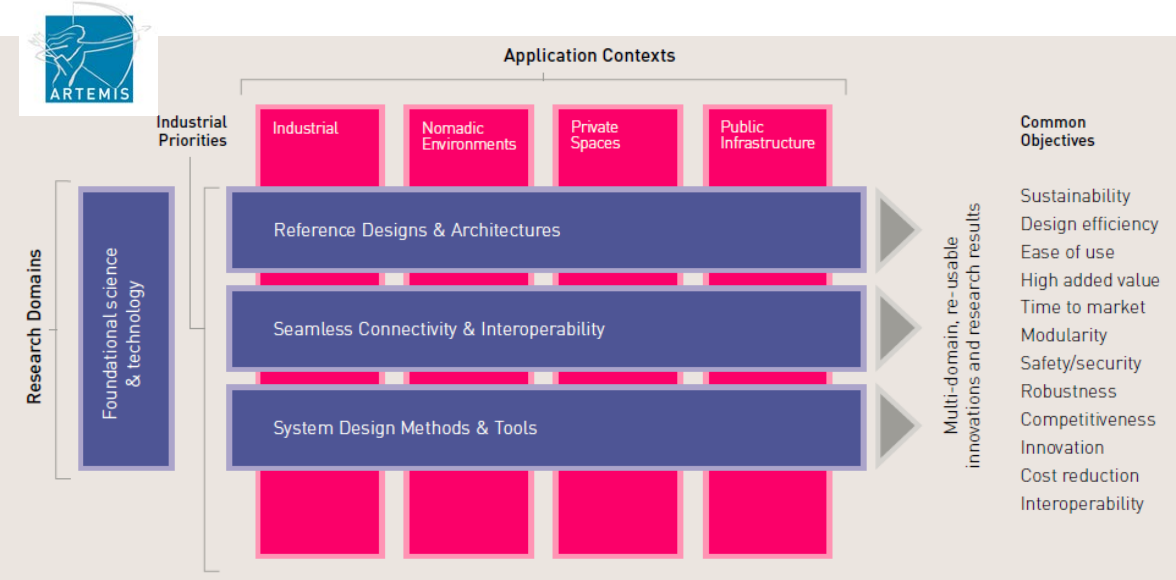

Figura 7: Representación de los dominios de investigación y los contextos de aplicación de los Sistemas Embebidos. [Fuente: Agenda Estratégica de Investigación de Artemis]

2.3 Los Sistemas Embebidos en SmartGrid

El concepto de SmartGrid es muy amplio y la solución que se ofrece al mercado está en plena evolución, las tecnologías necesarias siguen desarrollándose y optimizándose, estando otras en fase de investigación.

Si bien es verdad que actualmente el gran esfuerzo de la industria se está concentrando en las capas de las aplicaciones software de gestión de SmartGrid, no es menos cierto que los sistemas embebidos se presentan como elementos fundamentales. Sin unos sistemas embebidos adecuados la futura solución SmartGrid quedaría limitada y no podría desplegar todo su potencial.

De hecho, en un escenario en el que los sistemas embebidos no evolucionasen dentro de SmartGrid, los sistemas software de las capas de aplicación, a pesar de disponer de una gran capacidad de gestionar masivamente datos, y de ofrecer grandes posibilidades algorítmicas y de cálculo, se verían en cierta medida limitados. Dicha limitación vendría dada por no disponer a nivel de campo de los dispositivos con la necesaria capacidad para, por un lado, ejecutar de forma adecuada y con las condiciones temporales necesarias los comandos enviados por las aplicaciones software y, por otro lado, ofrecer la respuesta esperada a las solicitudes de información requeridas por los niveles superiores.

En el esquema que se presenta a continuación se ilustra la solución de SmartGrid donde se pueden observar los siguientes cinco niveles:

1. Empresa: aplicaciones empresariales clásicas de la *Utility*[1] como CRM (Customer Relationship Management), ERP (Enterprise Resource Planning), Mercado, etc.
2. Integración de datos: aplicaciones de valor añadido de la solución SmartGrid que se integran con las anteriores. Dichas aplicaciones software, que suelen trabajar sobre tecnología SCADA (Supervisory Control And Data Acquisition), son el Sistema de Gestión de Incidencias (OMS), el Sistema de Gestión de la Distribución (DMS), el Sistemas de Información Geográfica (GIS) y el Sistema de Gestión Eléctrico (EMS). A su vez se encuentra en este nivel la gestión de los sistemas de medida de contadores eléctricos Advanced Meter Infrastructure (AMI) y Meter Data Management (MDM), así como también la gestión de históricos.
3. Infraestructuras de Comunicaciones.
4. Dispositivos Electrónicos Inteligentes (IED) y sensores: Dispositivos Electrónicos Inteligentes que son los elementos inteligentes de los subsistemas de adquisición de datos y los propios sensores de campo. Fundamentalmente presentes en las Subestaciones y en las salidas de los alimentadores (feeders), así como en los contadores eléctricos inteligentes.
5. Red eléctrica: Generación, transmisión y distribución.

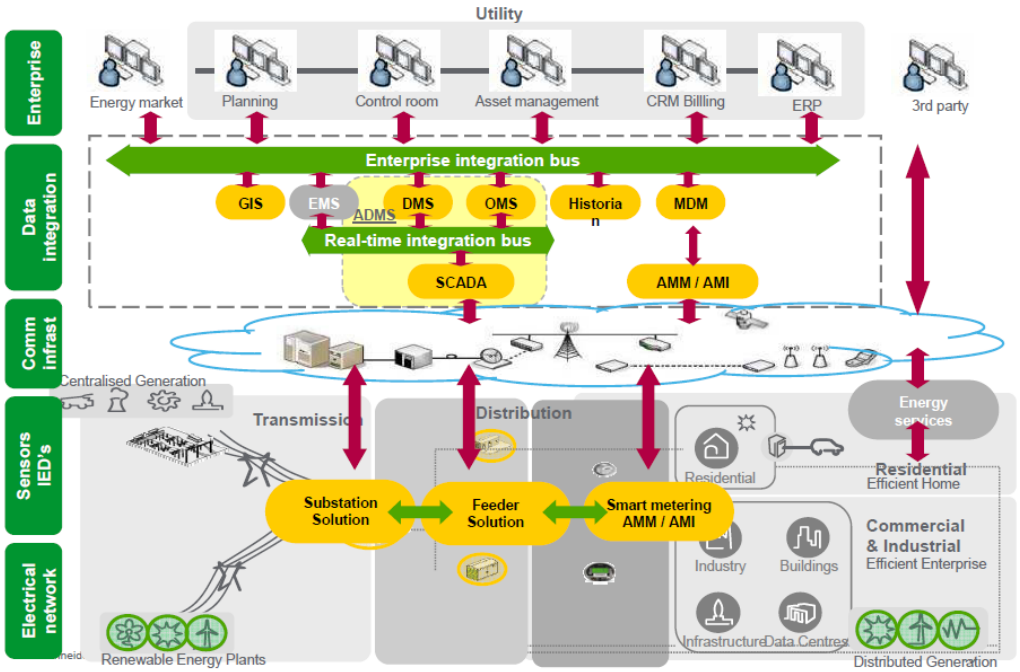

Figura 8: Representación en cinco capas del concepto de SmartGrid en cinco niveles. [Fuente: Schneider-Electric]

[1] Denominación genérica de aquellas compañías que ofrecen servicios públicos como electricidad, gas o agua

De esta forma vemos como los sistemas embebidos se encuentran claramente representados en el cuarto nivel de la Figura 8, y como se ha argumentado son parte integral de la solución como “habilitadores” y “capacitadores”.

Los sistemas embebidos en SmartGrid se basan fundamentalmente en elementos hardware con software embebido incluyendo capas de seguridad, monitorización, despliegue y configuración. Los principales dispositivos a nivel de Subestación eléctrica**,** de generación, transmisión y distribución ya sea primaria o secundaria, son las Protecciones, los Concentradores (Front-end), las Unidades de Control de Bahía, los Terminales Inteligentes y las Unidades Terminales Remotas. Por otro lado, en la red de distribución de baja tensión, los principales dispositivos son los contadores inteligentes.

Por tanto, la Subestación en sus distintas modalidades se presenta como el escenario natural donde los sistemas embebidos de SmartGrid se desarrollan y donde se producen los principales avances tecnológicos.

Seguidamente, se presenta el sistema eléctrico en su conjunto, desde la generación hasta el consumidor, pasando por los sistemas de transmisión y distribución en donde se pueden observar las Subestaciones eléctricas (ver Figura 9).

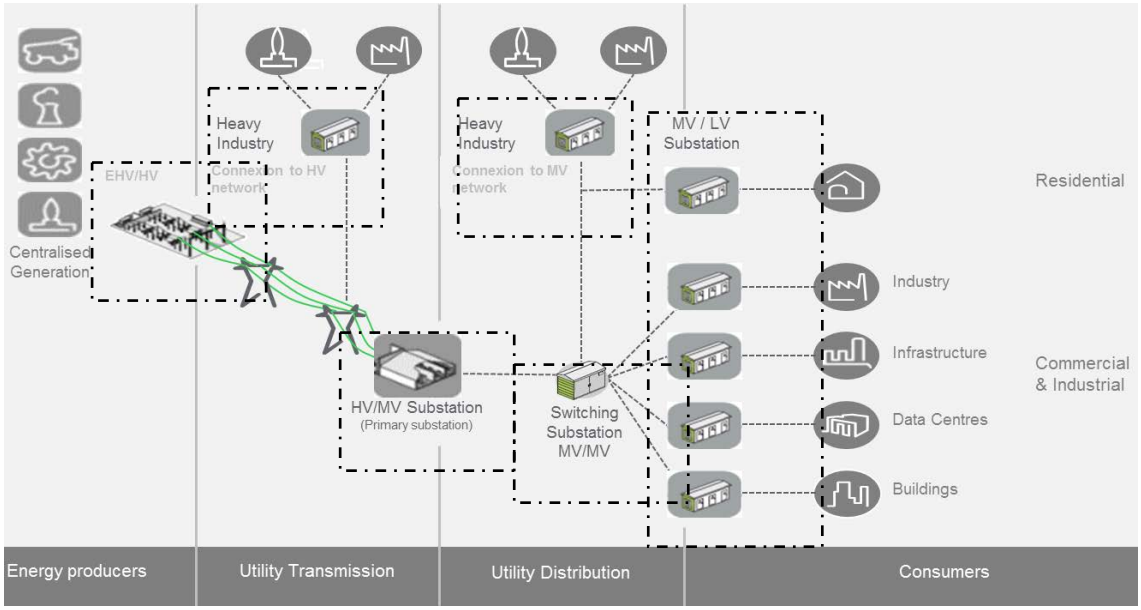

Figura 9: Situación de las Subestaciones en SmartGrid. Se resaltan con cuadros discontinuos, las Subestaciones de generación, transmisión y distribución, en sus distintos niveles de tensión. [Fuente: Schneider-Electric]

A continuación, por un lado, se presentan brevemente las principales características de los contadores inteligentes y por otro, a nivel de Subestación, las RTUs. Dado el posicionamiento y la versatilidad de las RTUs para actuar como Concentradores, Unidades de Control de Bahía, Terminales Inteligentes e incluso incluir funciones de protección, se puede afirmar que son el elemento clave del futuro desarrollo de los sistemas embebidos en SmartGrid.

2.3.1 Contadores Inteligentes

El equipo para la medida de la energía eléctrica consumida es un contador eléctrico o "meter" que consta de tres elementos principales, como son el sistema de medida, el elemento de memoria y el dispositivo de información.

Los equipos de medida de energía eléctrica pueden clasificarse según sus características:

- Tecnológicas, pudiendo ser contadores electromecánicos o electrónicos.
- Funcionales, como monofásicos o trifásicos.
- Energéticas, como contadores de activa y/o contadores de reactiva.
- Operativas, como dispositivo de tipo registrador o programables que permiten la telegestión.

Actualmente, los equipos de medida que están siendo desplegado masivamente son electrónicos, permiten registrar la medida de energía por intervalos de tiempo predefinidos inferiores a una hora. Dichos equipos se comunican con los concentradores bidireccionalmente y posibilitan la medida remota, lo que se denomina lectura automática de contadores.

En los últimos años, la tecnología de soporte a la telegestión de la demanda ha evolucionado, pasando por distintos estados que se conocen comúnmente por sus siglas en inglés:

- AMR (Automatic Meter Reading) o Lectura Automática de Contadores, se centra en la recolección automática de la información de consumos de contadores de los clientes, transfiriéndolos a una base de datos central desde la que se utilizan, sobre todo, para la facturación.
- AMM (Advanced Metering Management) o Gestión Avanzada de la Medida. Añade al punto anterior la focalización en la gestión de la información que se hace a lo largo de todo el proceso: captura, integración, validación, estimación y edición.
- AMI (Advanced Metering Infraestructure) o Infraestructura de Medida Avanzada. Es la aproximación tecnológica actual. Se centra en la telegestión del suministro, contemplando, adicionalmente a lo visto en los puntos anteriores, la gestión de la red mediante la recepción de información de alarmas y estados, así como el control de los elementos situados en la instalación del cliente: contador e interruptores de control de potencia. Requiere de la instalación de dispositivos avanzados o por su nomenclatura en inglés "Smart Meters" o "Advanced Meters".

Para permitir el intercambio de información en tiempo real, y monitorizar y notificar la calidad de servicio de la red, actualmente existen diferentes tecnologías PLC (Power Line Communications) basadas en distintos protocolos y estructuras: PLC SFSK, PRIME, G3-PLC y Meters & More. Aunque desafortunadamente hoy en día la interoperabilidad entre tecnologías no es posible [13], tanto PLC S-FSK, PRIME, G3-PLC como Meters & More están trabajando en esta dirección, lo cual permitirá la interoperabilidad entre todos los equipos y servicios de los distintos fabricantes (siempre de la misma tecnología).

El protocolo DLMS/COSEM (IEC 62056 / EN 13757-1) es muy utilizado en el sector comercial e industrial relacionado con los contadores eléctricos y tele gestionados que se comunican a través de la red telefónica conmutada pública, GSM, GPRS y Power Line. DLMS/COSEM es un estándar internacional ampliamente aceptado basado en dos conceptos: la modelización de los objetos de la capa de aplicación y en los modelos OSI (Open System Interconnection). Las tecnologías S-FSK, G3-PLC y PRIME usan DLMS como protocolo de capa de aplicación [13].

Por último, indicar que actualmente se está trabajando principalmente sobre tres soluciones Power Line con arquitectura de comunicaciones pública, abierta y no propietaria que están apoyadas por diferentes empresas: PRIME [14], G3 [15] y Meters and More [16].

2.3.2 Unidades Terminales Remotas

La RTU es un dispositivo electrónico controlado por microprocesador que conecta objetos en el mundo físico a un sistema de control distribuido o SCADA mediante la transmisión de datos de telemetría al sistema, y mediante el uso de mensajes del supervisor [17]. Las RTUs, por tanto, son dispositivos de adquisición y control de campo y supervisión que se encargan de procesar la información que reciben de los transmisores de campo y efectuar el procesamiento para control o seguridad de la aplicación donde se instalan. Tienen la capacidad de registrar, concentrar y comunicar toda la información para que ésta pueda ser utilizada por el operador o enviada a los distintos subsistemas de control que forman parte de la instalación. A continuación se representa la configuración típica [17]:

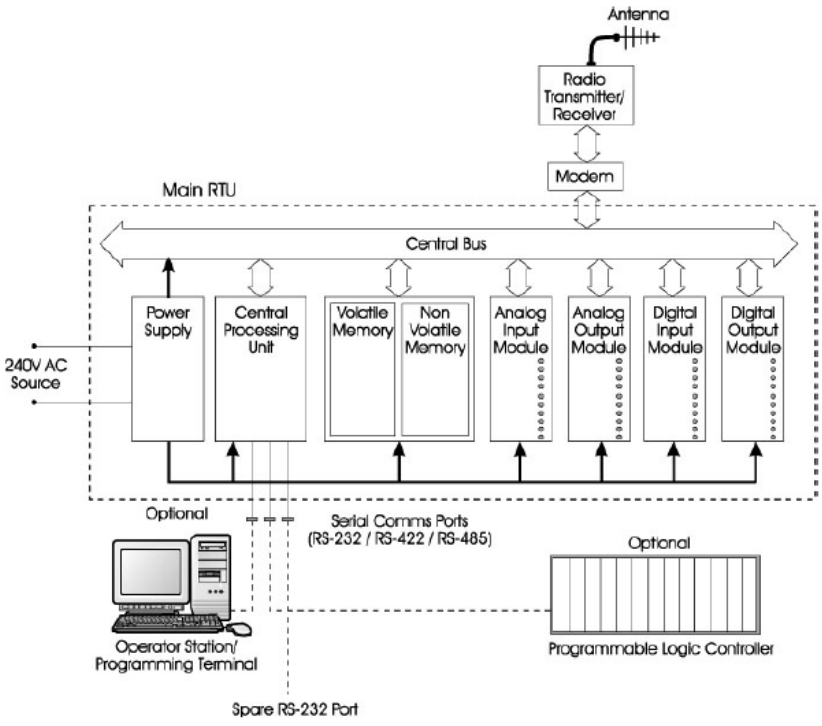

Figura 10: Configuración típica. [Fuente: Practical modern SCADA protocols: DNP3, 60870.5 and related systems Newnes [17]]

La arquitectura de una RTU consta básicamente de [18]:

- Fuente de alimentación: para suministrar la energía necesaria para operar a los distintos módulos que componen la RTU.
- Unidad central de procesamiento (CPU): es la encargada de centralizar la información adquirida por otros módulos del sistema y ejecutar los programas de control lógico, protocolos de comunicaciones y aplicaciones específicas de usuario. Las funciones de procesamiento de datos se definen en el software que se aloja en la CPU y los datos son guardados en módulos de memoria.
- Módulos de entradas/salidas: una RTU cuenta con módulos de entradas/salidas los cuales son conectados al sistema para adquirir, y, en determinadas circunstancias, preprocesar las señales, así como controlar y ejecutar las órdenes sobre los dispositivos de campo. Entre otros, se dispone de entradas y salidas digitales y analógicas y medidas directas.
- Módulo de sincronización de tiempo: para la ejecución del software y el establecimiento de comunicaciones es necesaria una sincronización que se lleva a cabo mediante este módulo.
- Software de control: a través de éste, la CPU ejecuta las instrucciones necesarias para el proceso. Con él se define la estrategia de control.
- Interfaz de comunicación: el módulo de comunicaciones se encarga de codificar la información recibida del campo para poder ser transmitida por los buses de comunicación; de igual manera la información recibida por los buses de comunicación es procesada por este módulo y decodificada para su uso por la CPU.

En la siguiente figura se puede observar un ejemplo de este tipo de arquitectura (RTU Saitel de Schneider-Electric):

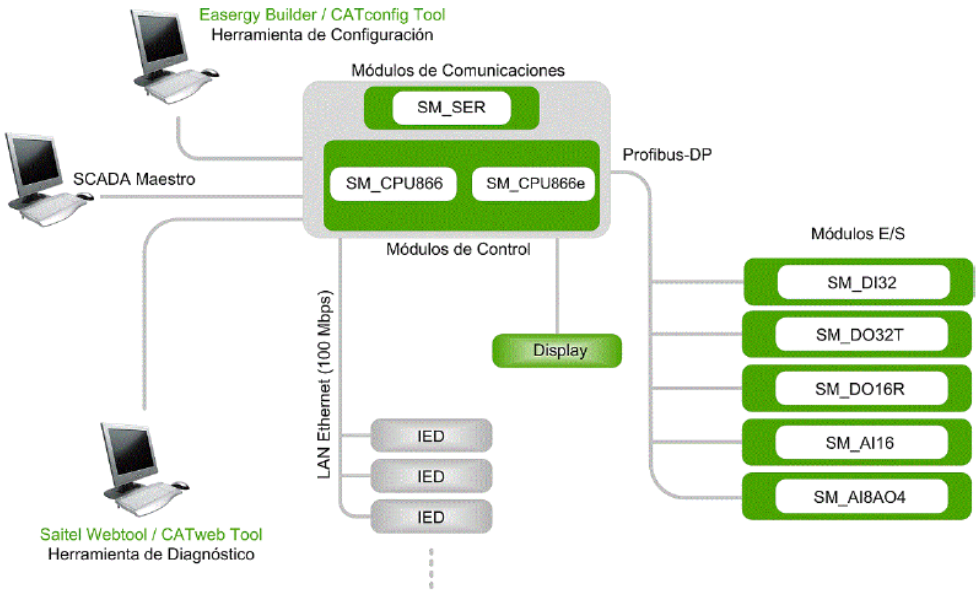

Figura 11: Arquitectura de RTU Saitel, incluyendo, módulos de control, comunicaciones, entrada salidas y herramientas de configuración y monitorización. [Fuente: Schneider-Electric [18]]

2.3.2.1 Protocolos de Comunicaciones

El mapa actual de protocolos de comunicación utilizados en el sistema eléctrico es muy extenso, y está regulado por el Comité Técnico 57 (TC57: Technical Committee 57: Power system control and associated communications) de la Comisión Electrotécnica Internacional (IEC: International Electrotechnical Commission). Así, TC57 aglutina varios grupos de trabajo para estandarizar las comunicaciones en el sistema eléctrico mediante el desarrollo de modelos de datos e interfaces genéricos y la utilización por los mismos de protocolos de comunicación ya existentes como TCP/IP (Transmission Control Protocol/Internet Protocol) o interfaces serie.

En la siguiente figura se puede observar la relación entre los distintos actores presentes en las redes eléctricas y los protocolos utilizados entre ellos para el intercambio de información [19]:

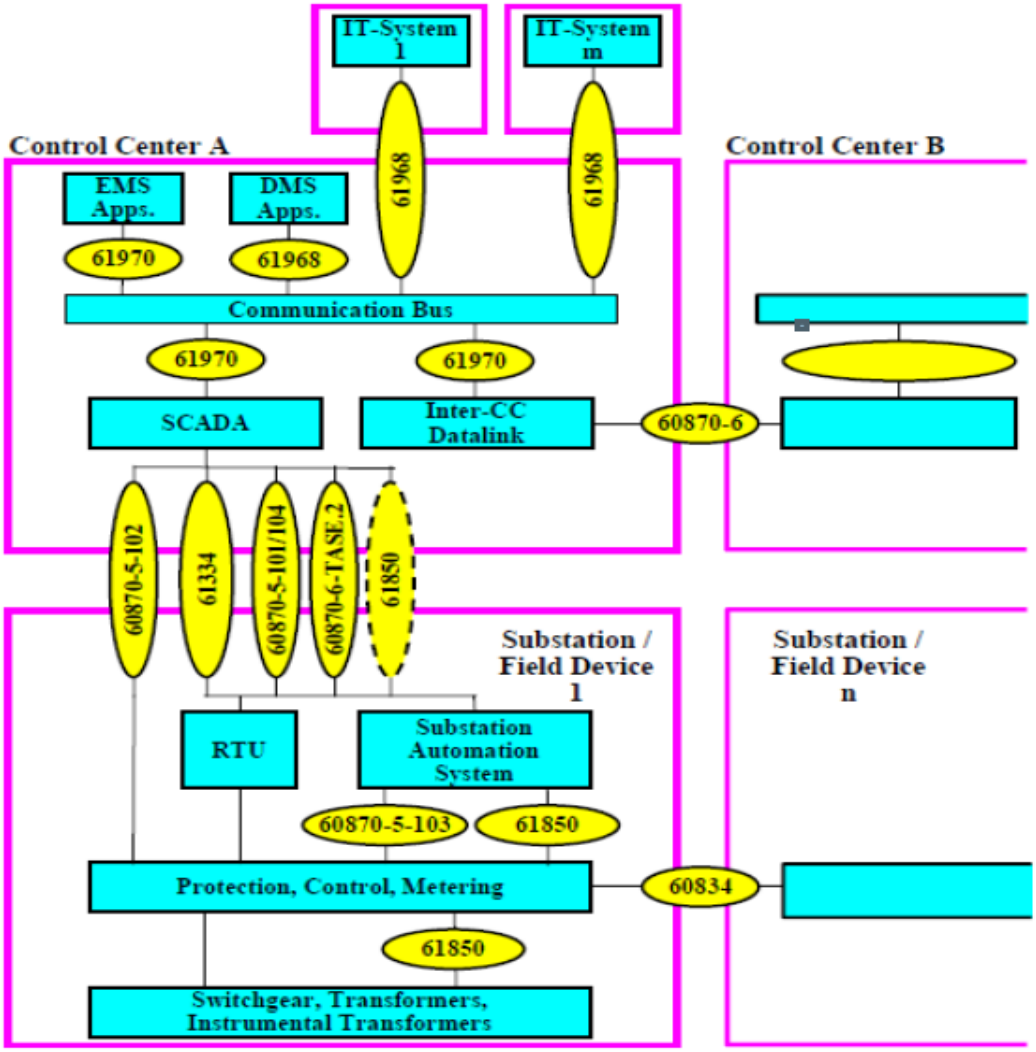

Figura 12: Utilización de protocolos en la red de distribución. [Fuente: Harmonization of CIM with IEC Standards [19]]

A continuación se presentan los principales protocolos de comunicaciones relacionados con RTU, que son IEC101, IEC103, IEC104, DNP3.0 y Modbus. Comentar que en el Capítulo 3 correspondiente al estado del arte y en el Capítulo 4 se estudiará el IEC61850 y sus protocolos de comunicaciones. A su vez, dichos protocolos, forman parte del caso de uso del Capítulo 5 y contrastan con las comunicaciones propuestas en el Capítulo 6, las cuales se basan en las redes sociales.

IEC 101

IEC 101 (IEC 60870-5-101) es un estándar internacional para los equipos y sistemas de telecontrol, centrado en transmisión de datos por serie para monitorizar y controlar procesos dispersos geográficamente del TC57 del IEC. Es compatible con las normas IEC 60870-5-1 y IEC 60870-5- 5 [20].

Entre las características generales de este protocolo se encuentran:

- Comunicación desbalanceada (sólo el maestro inicia el paso de mensajes) y balanceada (tanto maestro como esclavo pueden iniciar la comunicación) como modos de transferencia de datos.
- Dirección de enlace y direcciones ASDU (servicio de unidad de datos de la capa de aplicación), se proporcionan para la clasificación de la estación final y los elementos debajo de la misma.
- Los datos se clasifican en los diferentes objetos de información, cada uno de ellos se suministra con una dirección específica.
- Existen mecanismos para clasificar los datos en alta prioridad (clase 1) y baja prioridad (clase 2), así como la transferencia de los mismos a través de diferentes mecanismos.
- Se añade la posibilidad de clasificar los datos por grupos (1-16) para obtener dichos datos de acuerdo con el grupo mediante la transmisión de órdenes específicas de consulta de grupo por parte del maestro, y la obtención de datos en todos los grupos mediante la emisión de consultas genéricas.
- Se proveen esquemas de actualización espontánea y cíclica de datos.
- Facilidad para sincronización de tiempo.
- Esquemas de transferencia de archivos.

IEC 104

IEC 104 (IEC 60870-5-104) es un estándar internacional para los equipos y sistemas de telecontrol del TC57 del IEC. Las especificaciones de esta parte presentan una combinación de la capa de aplicación de IEC 60870-5-101 y las funciones de transporte proporcionadas por TCP/ IP [21].

El protocolo IEC 60870-5-104 define el uso de una red TCP/IP como medio de comunicación con las siguientes características:

- No es necesario software específico de red en los sistemas finales.
- No son necesarias funcionalidades de routing en los sistemas finales.

- No es necesaria la gestión de la red en los sistemas finales.
- Facilita que el sistema final lo suministre un especialista en telecontrol.
- Facilita que los routers los suministren especialistas en telecomunicaciones.
- Un cambio en el tipo de red requiere solo un cambio en el tipo de router, sin afectar a los sistemas finales.

IEC 103

IEC103 (IEC 60870-5-103) es un estándar internacional para los equipos y sistemas de telecontrol del TC57 del IEC. Se define un estándar que permite la interoperabilidad entre los equipos de protección y dispositivos de un sistema de control en una Subestación [22].

DNP 3.0

DNP3 fue el resultado de un esfuerzo integral para lograr la interoperabilidad basada en estándares abiertos entre las subestaciones eléctricas. Desde su creación, DNP3 también se ha utilizado en industrias adyacentes como el agua / aguas residuales, el transporte y la industria del petróleo y el gas [23]. El protocolo ha ganado aceptación mundial, incluyendo la formación de grupos de usuarios en China, América latina, y Australia, aunque en Europa predomina el uso de los protocolos IEC60870 101 e IEC60870 104.

En DNP, los datos se ordenan en tipos de datos. Cada tipo de datos es un grupo objeto, incluyendo:

- Entradas de información binaria (valores de un solo bit sólo lectura).
- Salidas binarias (valores de un solo bit cuyo estado puede ser leído, o que puede ser cambiado directamente o a través de operaciones tipo “select before operate”).
- Entradas de información analógicas (valores múltiples− sólo lectura).
- Salida analógica (valor múltiple−dígito cuyo estado puede ser leído, o que puede ser modificado directamente o a través de operaciones tipo “SBO: Select Before Operate”).
- Contadores.
- Hora y fecha.
- Objetos de transferencia de archivos.

Modbus

Introducido en 1979 por Schneider Electric (Modicon), el bus de campo Modbus® es un estándar de comunicación abierto, utilizado por una gran cantidad de productos y proveedores en el mercado actual. Con más de siete millones de nodos en América del Norte y Europa, Modbus es el estándar de facto en la integración de múltiples proveedores. En una red Modbus típica, los mensajes se envían a través de un enlace de comunicación serie RS232 / RS485. El protocolo Modbus se basa en un principio maestro / esclavo donde, por ejemplo, el maestro envía una solicitud y el esclavo direccionado envía una respuesta [24] . El protocolo Modbus define dos modos de transmisión: ASCII (American Standard Code for Information Interchange) y RTU [25].

2.3.2.2 Lógica de Procesamiento

Por último, es necesario estudiar la lógica de procesamiento que dota a las RTUs de inteligencia. Para dicha lógica, se adopta el estándar IEC61131-3 [26].

El objetivo del IEC61131-3 ha sido estandarizar los lenguajes de programación de los Controladores Lógicos Programable (PLC: Programmable Logic Controller) y RTUs. El estándar se subdivide en dos partes [27]:

- Elementos Comunes: El estándar define los aspectos básicos necesarios para lograr un software estructurado, encapsulación del software, control de ejecución y comportamiento secuencial. Esto cubre aspectos como variables, tipos de datos, direcciones de accesos, estructuración del software y Program Organization Units (POU).
- Lenguajes de programación: El estándar incluye la definición de 5 lenguajes distintos que pueden usarse para descomponer el software en elementos lógicos. Permite el uso modular y técnicas de software modernas lo que incrementa la reutilización, reduce costes e incrementa la eficiencia de programación y uso. También permite tanto la metodología de desarrollo top down como bottom up, donde es posible especificar la aplicación al completo y dividirla en sub bloques, declarar las variables, etc., o bien se puede comenzar a programar la aplicación desde la base, por ejemplo, vía funciones derivadas y funciones de bloque (PLCopen, 2004). Los lenguajes soportados son Sequential Function Chart (SFC), Ladder Diagram (LD), Function Block Diagram (FBD), Instruction List (IL) y Structured Text (ST).

PLCopen es una asociación mundial de software de automatización independiente de vendedores y productores (www.plcopen.org) creada en 1992 después de la publicación del estándar IEC61131. Su esfuerzo se enfoca principalmente en el IEC61131-3, que, como se ha indicado, define los lenguajes de programación estándar para la automatización industrial. La asociación ha trabajado desde entonces con la comunidad, manteniendo los esfuerzos enfocados en la independencia de fabricantes [27].

Es de notar que en ocasiones se utilizan PLCs que es un equipo electrónico programable, diseñado para controlar procesos secuenciales en tiempo real y en ambiente de tipo industrial. Un PLC trabaja en base a la información recibida por los captadores y el programa lógico interno, actuando sobre los accionadores de la instalación. Por tanto, respecto a la RTU, los PLCs presentan limitaciones a la hora de ejercer un control avanzado (que abarque adquisición, procesamiento y comunicación).

Capítulo 3. Estado del Arte

En este capítulo se expone el estado del arte de las tecnologías que se estudian en la presente tesis, que son clave para el futuro de los sistemas embebidos en el marco de SmartGrid, y que por tanto están íntimamente relacionadas con la RTU. De esta forma, en primer lugar, se estudia el estándar IEC61850, se introducen los conceptos de seguridad y se estudian los sistemas de protección de la red eléctrica. A continuación se estudian los principales estándares de seguridad. Posteriormente, la sincronización en la RTU en el contexto de un Sistema de Automatización de Subestaciones. Y, por último, se presenta el concepto del Internet Social de las Cosas, tomando como punto de partida el concepto de Internet de las Cosas, las Redes Sociales y el Procesamiento de lenguaje Natural.

3.1 IEC61850

En el capítulo anterior se presentaban los protocolos de comunicaciones estándares más extendidos y usados en la RTU y, por tanto, en el entorno de la Subestación eléctrica. En este apartado se presenta el estándar IEC61850 que posteriormente será referenciado tanto en el Capítulo 4 y en el Capítulo 5 como base de las contribuciones.

El estándar IEC61850 es hoy uno de los estándares principales para la automatización de Subestaciones [28], siendo su principal objetivo garantizar la interoperabilidad entre los dispositivos de automatización de diferentes proveedores [29], [30]. El estándar IEC61850 no es propiamente dicho un protocolo de comunicaciones, pero articula cómo debe realizarse la interoperabilidad entre equipos mediante el protocolo MMS (Manufacturing Message Specification) [31].

Se divide en diez partes y trata cuatro aspectos principales: un modelo funcional del dominio de aplicación de la Automatización de Subestaciones (Parte 5), un modelo de datos para sistemas de Automatización de Subestaciones (Parte 7), protocolos de comunicaciones y sus servicios (Partes 7, 8 y 9) y un lenguaje descriptivo de la configuración de Subestaciones (Parte 6), basado en XML [30], [32].

Define un conjunto de servicios de comunicación válido para la interconexión de equipos de distinta jerarquía dentro de la red eléctrica.

- Servicios de asociación/liberación entre cliente/servidor.
- Servicios de lectura/escritura de datos.
- Servicios de datasets, lectura y escritura de un conjunto de datos.
- Servicios de auto descripción, que permiten conocer el modelo de información completo del IED.
- Servicios de control, para operar sobre datos controlables (por ejemplo, abrir un interruptor). Existen servicios de control previa selección del objeto y servicios con seguridad, en los que se informa del estado final del objeto controlado.
- Servicios de ajustes y substitución.
- Servicios de informes de eventos, para el envío asíncrono de eventos y cambios de estado a un cliente que se suscribe.

- Servicios de registro (históricos), para el almacenamiento en la memoria del IED de eventos y cambios de estado y su posterior consulta.
- Servicios de transferencia de ficheros.
- Servicios de transmisión de eventos en tiempo real, para el envío rápido y fiable de eventos a varios receptores o transmisión de valores de medida muestreados, utilizando mensajes multicast sobre Ethernet.

Define un modelo de información jerárquico, basado en el modelado de funcionalidades o Nodos Lógicos (LN).

- Servidor, o elemento de más alto nivel que representa a una entidad con capacidad de comunicar. Puede contener uno o varios dispositivos lógicos.
- LD o Dispositivo Lógico, representa la modelización virtual de un dispositivo físico (por ejemplo, un inversor fotovoltaico o una unidad de generación compuesta por inversor, panel, baterías, etc.). Puede contener uno o varios Nodos Lógicos.
- LN o Nodo Lógico, que puede representar bien una funcionalidad (por ejemplo, control en un inversor fotovoltaico) o un componente (turbina de un aerogenerador) dentro de un equipo. Puede contener datos, data-sets, bloques de control de informes, ajustes e históricos.
- Dato, parte de información necesaria para cada función o componente modelizado mediante un Nodo Lógico (por ejemplo, para un inversor la tensión de bus). Cada dato puede estar formado por datos y/o atributos, por lo tanto, la definición de dato puede ser recursiva.
- Atributo, o contenedor final de la información (por ejemplo, valor, calidad, marca de tiempo de la tensión de bus).

Cada dispositivo compatible con la norma IEC61850 exportará su modelo de datos que comunicará hacia otros dispositivos IEC61850 según los servicios de comunicación que implemente el dispositivo.

Los distintos grupos de trabajo tratan de modelizar, bajo estas directrices, todos los elementos y funcionalidades que forman parte de cada dispositivo integrado en la red eléctrica. De esta manera, la nomenclatura y la semántica de los datos definidos serán comunes a todos los equipos desarrollados por los distintos fabricantes.

Los servicios de comunicación y los modelos de información son genéricos y no restrictivos, por lo que se dice que la norma IEC61850 es un estándar de mínimos:

- La mayor parte de Nodos Lógicos, datos y atributos son optativos, de manera que cada fabricante decidirá en la implementación final del estándar qué datos y servicios ofrecer, en función de la gama del equipo o del usuario final.
- IEC61850 define una interfaz abstracta de comunicaciones para independizar la capa de aplicación con todos sus servicios del protocolo de comunicación de nivel inferior utilizado (Servicios Web, DNP 3.0, etc.). Para cada servicio se define la semántica de los parámetros mínimos necesarios de las primitivas

Request/Response. Por el contrario, no establece cómo éstos deben ser implementados.

- Permite la utilización de las infraestructuras de comunicación existentes, ya que puede utilizarse sobre diversos protocolos de comunicación de nivel de aplicación OSI. IEC61850 define el mapeo de los servicios de comunicación y datos intercambiados a protocolos tales como MMS sobre TCP/IP, IEC101/104, DNP3.0 en función del medio físico, etc., pero está abierto a la definición de interfaces de mapeo sobre otros protocolos y sobre otras interfaces como radio, powerline, etc.
- La estandarización de los modelos de datos y de los servicios de comunicaciones, así como la definición de las capas de mapeo a protocolos de comunicación, permiten la interoperabilidad de equipos de distintos fabricantes.
- La definición del modelo de información se realiza mediante un modelo estándar basado en XML denominado SCL (Substation Configuration Language) [33], lo que implica una gran flexibilidad a la hora de implementar sistemas SCADA de adquisición y control. En la actualidad están surgiendo herramientas de configuración que se basan en SCL para configurar grandes entornos basados en IEC61850 como Subestaciones o parques eólicos.

Así pues, el estándar introduce un modelo abstracto que describe la información que puede intercambiarse entre los diversos dispositivos, introduce un conjunto de servicios, por ejemplo, las acciones que se pueden realizar en base a esta información, y propone protocolos para implementar el intercambio de información.

A) Modelo de datos

El modelo abstracto de un dispositivo se obtiene componiendo entidades básicas llamadas Nodos Lógicos. Cada Nodo Lógico describe un elemento específico en el sistema de automatización. Se definen varios grupos de Nodos Lógicos: control (C ---), medidas y medición (M ---), calidad de potencia (Q ---), funciones de protección (P ---), etc. Los grupos 'P ---' y 'R ---' son aquellos que agrupan Nodos Lógicos para funciones de protección y los propósitos relacionados con la protección.

Cada Nodo Lógico es una estructura compleja que contiene varios atributos llamados Objetos de Datos (DO, Data Objects). Cada uno de ellos tiene una clase específica llamada Clase de Datos Común (CDC, Common Data Class).

De esta forma, por ejemplo, el PTOC (protección de sobreintensidad) incluye el Objetos de Datos llamado “Str”' correspondiente al pico superior de la función de protección, que contiene una notificación general de que el fallo se ha detectado, junto con su marca de tiempo “t” y un atributo adicional de calidad “q” que indica si la notificación es confiable o no. Los elementos “t” y “q” se llaman Atributos de Datos (DA, Data Attributes) y son las “hojas” del modelo de datos de árbol IEC61850. A continuación se representa gráficamente la estructura de datos del estándar IEC61850 [34]:

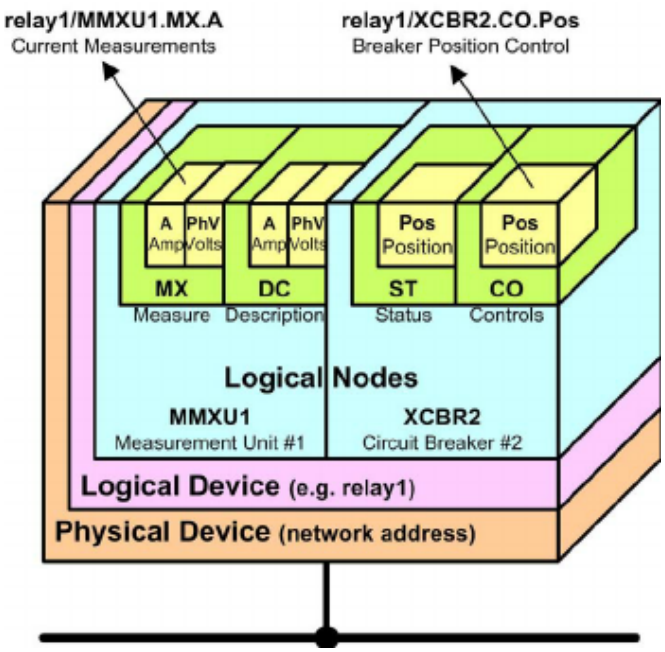

Figura 13: Estructura de Datos de IEC61850, donde se representa el dispositivo físico, el dispositivo lógico, los nodos lógicos, objetos de datos y atributos de datos. [Fuente: Communication Protocols and Networks for Power Systems Current Status and Future Trends [34]]

B) Servicios Abstractos

Una vez introducido el modelo de datos propuesto por el IEC61850, es importante analizar, primero los servicios que se aplican a la información y segundo los protocolos necesarios para realizar el intercambio de información.

Entre los servicios más comunes, se encuentra, el servicio de Informe (Report) que se utiliza para obtener información de un dispositivo con capacidades de medida. El servicio sigue un modelo de cliente/servidor basado en un envío periódico o por eventos. La contrapartida del Informe es el servicio Lectura (Read), en el cual, el cliente le pide al servidor que libere los datos una vez que se necesiten.

Otro importante grupo de servicios es el de realizar acciones de control (por ejemplo, un cliente cambia el estado de un interruptor actuando en el servidor conectado al elemento físico) y actualizar los parámetros de configuración. Hay cuatro modelos de control diferentes, cada uno de ellos combina de forma diferente los diversos servicios relacionados con el control (Seleccionar, Cancelar, Operar, etc.) para lograr un comportamiento diferente. Estos modelos también se pueden usar para cambiar el valor de los parámetros de los IEDs, a fin de actualizar las configuraciones de los mismos.

Por último, comentar el servicio de GOOSE (Generic Object-Oriented Substation Events), que se usa para intercambiar información en la que el tiempo es un factor crítico, como es lo relacionado con funciones de protección o errores y alarmas entre los diferentes IED a nivel de la Subestación. Los datos en el mensaje GOOSE se

organizan en una estructura denominada “Data-Set” según lo definido por el modelo de datos IEC61850 [35].

C) Implementación de Servicios

Cada uno de estos servicios están descritos de manera abstracta en el estándar. Sin embargo, también se propone una posible implementación al mapearlos en un protocolo específico.

Aunque recientemente se han propuesto nuevos mapeos de protocolos [36] y otros están siendo analizados para ser incluidos dentro de la norma, la forma más común de implementar dicho servicio es utilizar los protocolos MMS y GOOSE sobre Ethernet [37].

Mientras que el primero es un protocolo de aplicación basado en TCP/IP (ISO-OSI capa 3) y comunicación uno a uno, el segundo se mapea directamente en el nivel de Ethernet (ISO-OSI capa 2) como un protocolo multicast basado en un modelo de publicación/suscripción (publisher/subscriber). GOOSE sobre Ethernet tiene en general una estructura de paquete simple con poco “overhead”, lo que implica, en general, mayor velocidad de intercambio de información.

Por estas razones, el MMS es un buen candidato para implementar los servicios Report y SetValues, mientras que el protocolo GOOSE sobre Ethernet se debe usar para la Selectividad Lógica de la secuencia de localización de fallos, aislamiento y restablecimiento del servicio entre IEDs. En la Figura 14 se representan los distintos tipos de comunicaciones en el estándar IEC61850 [38].

D) Requisitos de Red

Teniendo en cuenta que el Sistema de Automatización se basa en la coordinación de los sistemas de protección con el fin de realizar una función de protección distribuida, se debe de usar el protocolo GOOSE sobre Ethernet, necesitando una amplia área de difusión. De hecho, un mensaje GOOSE tiene que llegar a todos los IEDs conectados a la misma red física (o virtual), lo que implica un gran uso del ancho de banda debido a la gran cantidad de pequeños paquetes que circulan en la infraestructura de comunicación.

Otra característica relevante de esta red de comunicación está relacionada con la priorización del tráfico, permitiendo la entrega de paquetes críticos a tiempo, incluso cuando haya un gran volumen de tráfico en dicho canal. De hecho, los diferentes servicios definidos por el estándar IEC61850 pueden requerir diferentes índices de rendimiento para la infraestructura de comunicación. Algunos requisitos comunes son la fiabilidad de la red, la latencia, el rendimiento y la precisión de la sincronización entre dispositivos y sistemas.

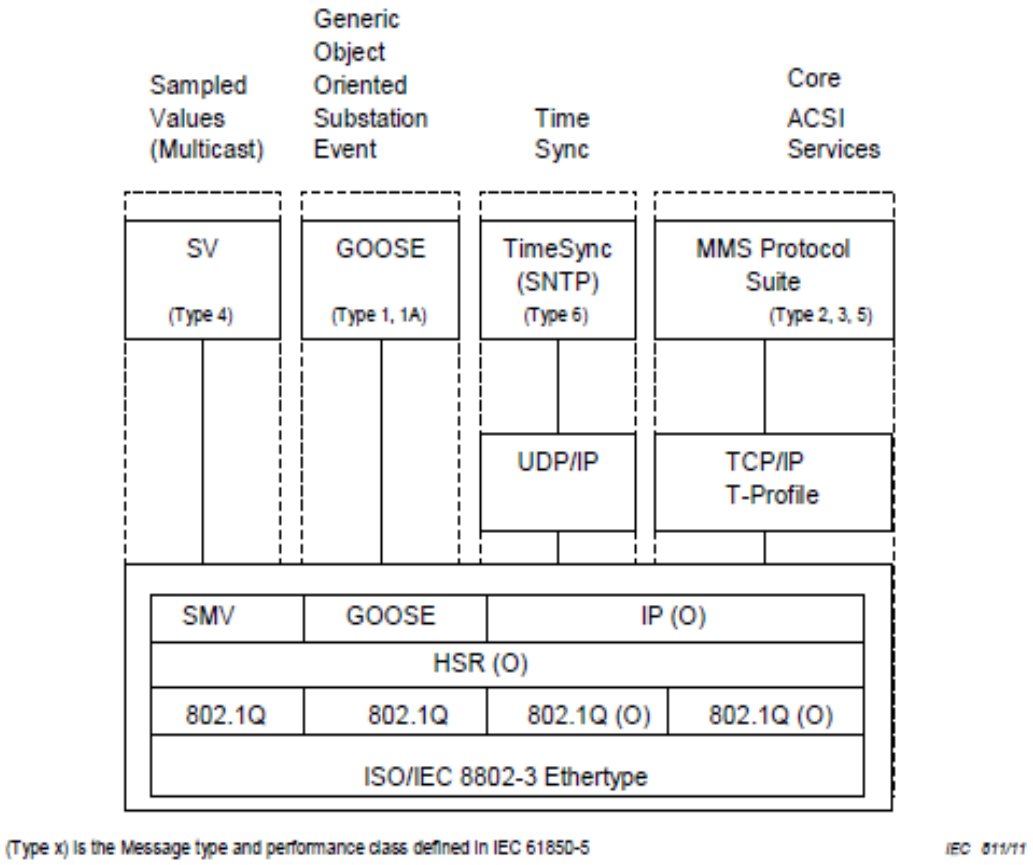

Figura 14: Representación Comunicaciones IEC61850, MMS, GOOSE y Sampled Values (SV). [Fuente: IEC 61850-8-1 Communication networks and systems for power utility automation – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3, Figura 1]

E) Configuración

La configuración de un IED en IE61850 se realiza en el archivo denominado CID (Configured IED Description). Un dispositivo totalmente compatible con IEC61850 debe configurarse solamente mediante este archivo respetando sus interfaces. Sin embargo, hasta ahora, los IED de muchos proveedores se pueden configurar solo en lo que respecta a las medidas y los comandos, mientras que la configuración de las funciones de protección se especifica en el IED mediante la descarga de un archivo de configuración específico del proveedor.

Cada vez que se necesita un cambio en la configuración de un dispositivo de protección o de la lógica de coordinación, se debe descargar el archivo en el IED. Este procedimiento, puede ser aceptable cuando los IED están limitados a Subestaciones Primarias, pues su número es limitado, pero no es admisible a nivel de Subestación Secundaria por el amplio despliegue de IEDs y el costo económico que implicaría dicha actualización. Por tanto, se necesita un modelo estándar para describir los parámetros de las funciones de protección y la lógica de coordinación entre los IED, junto con un sistema capaz de cambiar esos ajustes automáticamente cada vez que se produzca un cambio en la configuración de la red.

3.2 Seguridad

En lo que respecta a la seguridad, es necesario primero introducir dos de sus acepciones [39] que se exponen seguidamente:

- Security (en inglés), como el grado de resistencia o de protección frente a daños intencionados, que, en el contexto de la presente tesis, significaría el ámbito de la seguridad lógica, donde se utilizarían elementos como cortafuegos, antivirus, quedando fuera lo que respecta a la seguridad física, en donde se utilizan cámaras de vigilancia, sensores de presencia, etc., para proteger sistemas, máquinas físicas y otras infraestructuras frente a ataques en el ámbito de lo físico.
- Safety (en inglés), entendida como medidas que ayuden a evitar la ocurrencia de un accidente, que, en el contexto de la presente tesis, significaría prevención de daños a nivel de equipamiento, instalaciones, o personas.

En cuanto a la seguridad en su acepción “safety”, el estándar IEC61508 es el que generalmente es reconocido como el principal [40]. Dicho estándar IEC61508 “Seguridad funcional de los sistemas eléctricos/electrónicos programables relacionados con la seguridad" [41] cubre los aspectos relacionados con el Nivel de Integridad de Seguridad (SIL, Safety Integrity Level) de los sistemas.

Por tanto, SIL es la medida que define el estándar IEC61508 atendiendo a la probabilidad de fallo en una función o sistema de seguridad. SIL está intrínsecamente unido a un número que indica la probabilidad de que el dispositivo o sistema pueda fallar. Así se establecen cuatro niveles, siendo SIL 4 el más restrictivo y SIL 1 el menos. En la Figura 15, se representan los cuatro niveles con sus correspondientes probabilidades de fallo [42].

Safety Integrity Level	Probability of failure on demand, average (Low Demand mode of operation)	Risk Reduction Factor	Probability of dangerous failure per hour (Continuous mode of operation)
SIL 4	$>=10^{-5}$ to $<10^{-4}$	100000 to 10000	$>=10^{-9}$ to $<10^{-8}$
SIL 3	$>=10^{-4}$ to $<10^{-3}$	10000 to 1000	$>=10^{-8}$ to $<10^{-7}$
SIL 2	$>=10^{-3}$ to $<10^{-2}$	1000 to 100	$>=10^{-7}$ to $<10^{-6}$
SIL 1	$>=10^{-2}$ to $<10^{-1}$	100 to 10	$>=10^{-6}$ to $<10^{-5}$

Figura 15: Niveles de SIL con sus probabilidades de fallo y factor de riesgo en modo demanda y modo continuo. [Fuente: IEC 61508 Overview Report, Exida [42]]

Por otro lado, el IEC61508, define como las funciones de seguridad del sistema deben ser capaces de realizar diagnósticos y detección de fallos, así como reaccionar apropiadamente ante dichos fallos. También define métodos y procedimientos para el

desarrollo y gestión del proceso, reduciendo las probabilidades de aparición sistemática de fallos en el sistema.

Por último, el estándar define una aproximación del ciclo de vida del sistema: procedimientos usados para el diseño, desarrollo y validación del hardware y el software, gestión de seguridad funcional, documentación, análisis de riesgos y requisitos entre otros como se puede apreciar en la siguiente figura.

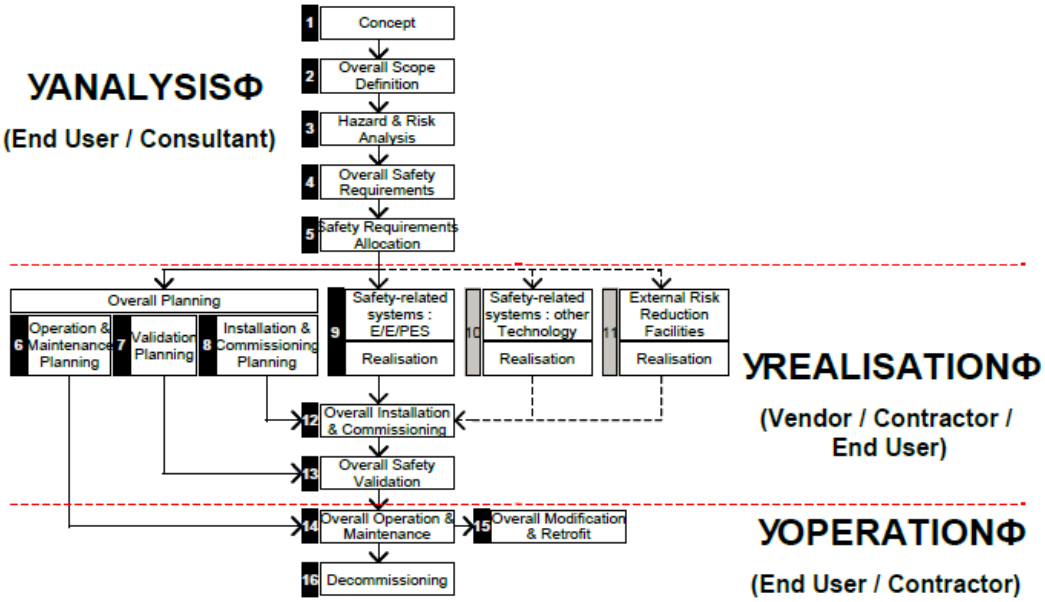

Figura 16: Ciclo de vida Safety del IEC61508 [Fuente: IEC 61508 Overview Report, Exida [42]]

En cuanto a la seguridad en su acepción “security”, existen un importante número de estándares relevantes para cubrir los distintos ámbitos de la seguridad en SmartGrid, como se puede observar en la Figura 17 [43]. Así pues, el estándar IEC62351 se dirige al sector de la energía, más específicamente a la automatización de Subestaciones, NERC-CIP generalmente se centra en los operadores de energía, mientras que ISO 27000 y NIST800-53 están dirigidos principalmente a entornos de tecnologías de la información (destinados a proteger la información) y otros estándares como ISA99 o IEEE1686 se centran en los sistemas de automatización industriales [43].

El alcance de la serie IEC62351 [44] se centra en la seguridad de la información para las operaciones de control de sistemas de potencia. Se desarrolla para manejar la seguridad de los protocolos del “Technical committee 57: Power system control and associated communications” del IEC, incluyendo las series IEC60870-5, IEC60870-6, IEC61850, IEC61970 y IEC61968. Los diferentes objetivos de seguridad incluyen autenticación en la transferencia de datos a través de firmas digitales, garantizando únicamente el acceso autenticado, la prevención de escucha, prevención de suplantación, o detección de intrusiones.

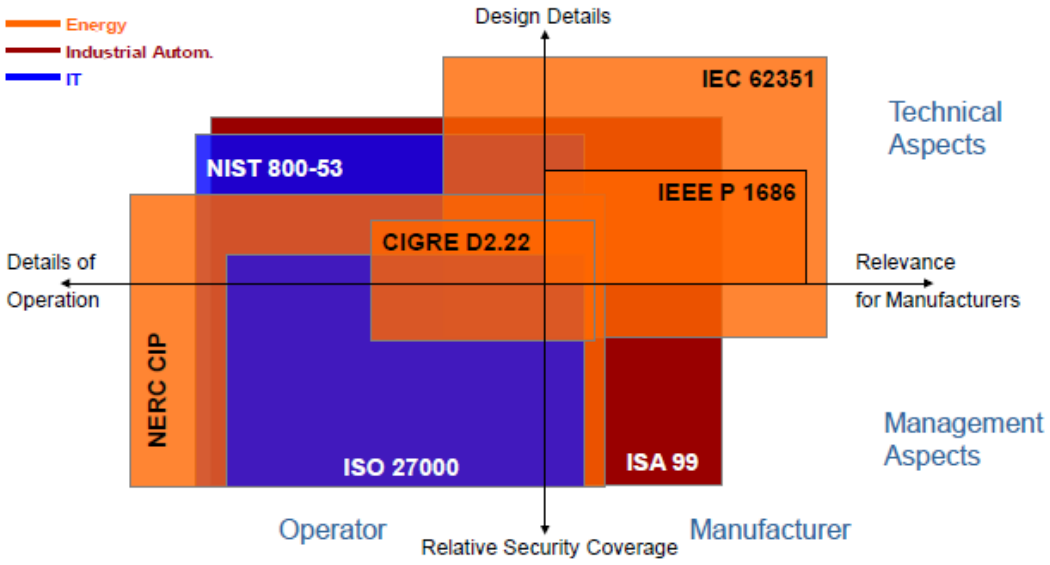

Figura 17: Representación gráfica de los estándares de aplicación en los dominios: energético, automatización y tecnologías de la información. [Fuente: IEC TR 62351-10:2012 [43]]

Por otro lado, el estándar IEEE1686-2013 "Estándar para capacidades de ciberseguridad de los dispositivos electrónicos inteligentes" [45], define las funciones y características a proporcionar en dispositivos electrónicos inteligentes para dar cabida a programas de protección de infraestructura crítica. Se aborda la seguridad con respecto al acceso, operación, configuración, revisión de firmware y recuperación de datos de los dispositivos electrónicos inteligentes.

Por último, en lo que respecta a la seguridad, es necesario mencionar al Internet Engineering Task Force (IETF) y su conjunto de estándares IPsec (Internet Protocol security). IPsec [46] es un protocolo de seguridad, ampliamente aceptado por prácticamente todos los fabricantes de dispositivos de red (cortafuegos, herramientas de administración remota, etc.). Entre sus principales características, proporciona nativamente confidencialidad, ocultando el contenido de la comunicación establecida, y autenticidad, verificando criptográficamente la validez de las operaciones realizadas.

3.3 Localización de Fallos, Aislamiento y Restablecimiento del Servicio

Como se ha indicado en el Capítulo 2 el concepto de SmartGrid implica la combinación de tecnologías e infraestructuras resultando un sistema complejo que puede ver sensiblemente afectado su funcionamiento por distintas razones, por ejemplo, factores externos como desastres naturales o fenómenos meteorológicos, o por el deterioro de su propia infraestructura y elementos que componen la red o el sistema de control y protección. Cuando uno de estos sucesos produce la interrupción del suministro, nos encontramos ante el evento que en este dominio se denomina “falta”. Por tanto, la localización de la falta y la pronta restauración del servicio es, sin duda, la principal misión en el dominio de la protección de la red.

Clásicamente, una vez que se produce una incidencia y ésta era comunicada o detectada, se emprendían las acciones necesarias para localizarla lo más precisamente posible. De esta forma se envían operadores que mediante inspección visual de la línea tratan de localizar el punto de origen de la incidencia, asilando sistemáticamente tramos de la red y re-energizando. Posteriormente, se realizan las maniobras necesarias para aislar el tramo afectado actuando sobre los interruptores y seccionadores necesarios en cada caso y restaurando el servicio al resto de la red, limitando lo máximo posible la interrupción del suministro. La secuencia completa de localización de fallos, aislamiento y restablecimiento del servicio se denomina FLISR (Fault Location Isolation & Supply Restoration), que es la clave para el proceso automatizado de auto curación o auto cicatrización de la red, también denominado self-healing.

Por lo tanto, una vez que aparece la falta, se debe pasar por las siguientes fases:

- **Detección**: tradicionalmente han existido dispositivos dedicados a la indicación del paso de falta. La integración de tecnologías de comunicaciones en dichos dispositivos ha significado una mejora importante en la detección de las faltas, ya que permite su configuración a distancia para adaptarse a las características de la red y la reducción del tiempo de detección.
  Por otro lado, existen dispositivos que realizan funciones de protección entre las que se encuentran las de detección de sobre corriente, el punto negativo se encuentra en su alto precio.
  Los dispositivos utilizan distintas técnicas en función de las fases implicadas, del método de puesta a tierra del sistema de distribución, y del tipo de falta, por ejemplo, faltas de alta impedancia.
  Uno de los problemas que surgen con la implantación de renovables y las topologías de redes malladas es que las faltas pueden producirse en los dos sentidos en una línea, cuando antes en la topología radial y con una fuente de generación bien determinada, la falta solo iba en un sentido. Por lo cual, hoy en día, es necesario que los dispositivos sean capaces de determinar lo que se denomina la “direccionalidad de la falta”.
- **Localización**: se trata de determinar en qué sección de la línea del feeder ha acaecido el evento que ha sido detectado como una falta.
  Clásicamente se aplicaba el método de “prueba y error” en donde se realimentaba desde la cabecera y progresivamente se actuaba sobre los seccionadores de la línea hasta recuperar el suministro y, por tanto, quedar abierto el seccionador del tramo afectado. Esto además de consumir mucho tiempo, reduce vida útil de elementos como interruptores al sufrir constantes reenganches y cortes hasta localizar el tramo afectado.
  Actualmente, se aplican técnicas basadas en algoritmos y tecnologías de comunicación que permiten realizar aproximaciones de inteligencia distribuida. Dichas técnicas, en función del tipo de datos que se utilicen se categorizan como las basadas en la componente fundamental de la frecuencia, las de ondas viajeras (onda que tiene un perfil que se mueve con el tiempo a través del medio) y componentes de altas frecuencias y las del conocimiento de la red.
- **Aislamiento y Restauración**: esta fase consiste en reconfigurar la topología de la red, con objeto de que el impacto de la interrupción del servicio sea mínimo y que por tanto el número de clientes afectados sea el menor posible. De esta

forma se realizan las maniobras posibles entre interruptores y seccionadores para que la zona afectada quede desconectada y en la mayor parte posible del resto se restablezca el suministro.

El proceso clásico de localización y restauración de servicio [47], se presenta en la siguiente figura.

Figura 18: Tiempo de investigación de la falta y restauración sin FLISR. [Fuente: Pacworld – Protection, Automation and Control World [47]]

Esta aproximación contrasta con la llevada a cabo por potentes sistemas de última generación. Las nuevas tecnologías han permitido la aparición de métodos y algoritmos capaces de estimar de forma más precisa la distancia hasta la falta y además han surgido potentes sistemas centralizados como el ADMS [48] que proporcionan un plan óptimo de acciones de control para detectar, localizar y aislar las faltas y restablecer el servicio.

A continuación se presenta el proceso de localización de falta, aislamiento y restauración de servicio por el ADMS (Advanced Distribution Management System):

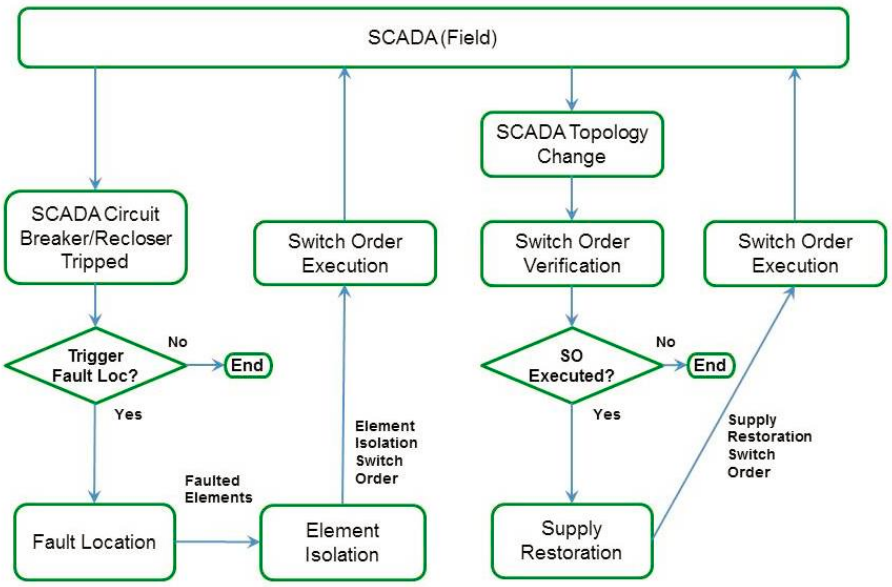

Figura 19: Ciclo automático de FLISR aplicado por el ADMS. [Fuente: Brochure ADMS FLISR, Schneider Electric [48]]

3.4 Sincronización

Los Sistemas de Automatización de Subestaciones son una tarea crítica en el concepto de SmartGrid, y las *Utilities* del sector eléctrico deben sincronizar la red eléctrica para garantizar una transferencia de potencia uniforme y mantener la integridad del suministro de energía [49]. Además, dependen cada vez más de la precisión de la sincronización del reloj para detectar la inestabilidad de la red y proteger la infraestructura [50].

Por lo tanto, se requiere una sincronización precisa para asegúrese de que los dispositivos de la Subestación tengan relojes precisos para el control del sistema y la adquisición de datos.

Desde sus inicios, los operadores de Subestaciones han tenido la necesidad de datar temporalmente todas las señales (cambios de estado, mandos, medidas, alarmas, etc.) involucradas en el sistema de control, siendo por tanto la sincronización temporal uno de los requisitos principales de dicho sistema. Para garantizar que las marcas de tiempo asociadas a los eventos de Subestación son coherentes, normalmente se requiere una sincronización temporal con una precisión inferior a un milisegundo (1ms).

No obstante, con la evolución hacia sistemas de Subestación más avanzados, se empiezan a requerir sistemas de sincronización más precisos, del orden de un microsegundo (1µs). Estos requisitos son necesarios, por ejemplo, para aplicaciones como monitorización de fasores (representación de oscilación sinusoidal) en redes WAN (Wide Area Network, Red de área extensa) o adquisición de mensajes IEC61850 para bus de proceso, donde se incluyen los mensajes GOOSE y Sampled Values (IEC61850-9-2).

Las tecnologías de sincronización empleadas pueden clasificarse en:

- Sistemas de sincronización temporal dedicados: Estos sistemas emplean cableados y repetidores independientes a la red del sistema de Subestación.
- Sincronización temporal integrada en redes de datos: Emplean para la transferencia de las señales de sincronización los propios cables y los switches de la red Ethernet de la Subestación, compartiendo el uso de los mismos con el tráfico de datos de otras aplicaciones de automatización y control.

3.4.1 Sistemas de Sincronización Dedicados

Históricamente en Subestaciones, para la sincronización temporal de los sistemas, se han venido usando sistemas independientes con su propio cableado para la distribución de la señal. Las tecnologías empleadas para el cableado de estos sistemas son generalmente cables coaxiales, fibra óptica o par trenzado. Para la codificación de la marca de tiempo en estos sistemas, encontramos varios métodos:

- IRIG-B (Inter Range Instrumentation Group - B): Los pulsos de sincronización proporcionan la sincronización además de la información relativa a la marca de tiempo.
- PPS (Pulso por segundo): Consiste en pulsos de sincronización muy precisos, transmitidos cada segundo. A diferencia de IRIG-B, estos pulsos no incorporan información sobre el día o la fecha del pulso.

El hecho de tener sistemas de control de Subestaciones con diferentes sistemas interconectados entre sí y con gran distancia entre ellos supone, para este tipo de métodos, un elevado coste asociado para el despliegue de la red de sincronización dedicada, en paralelo a la red de datos.

El uso de fibra óptica para este tipo de redes garantiza el aislamiento galvánico de los puertos de comunicación para la sincronización y permite eliminar interferencias, tanto inductivas como capacitivas. No obstante, el despliegue es más complicado y costoso al requerir repetidores de señal.

El retraso de propagación de la señal en cables de cobre o fibra óptica es aproximadamente de 5ns por metro. Este tiempo puede ser significativo en Subestaciones de grandes dimensiones, siendo necesario en estos casos que los propios sistemas de Subestación compensen el retraso.

3.4.2 Sincronización Temporal Integrada en Redes de Datos

Este tipo de sincronización hace uso de la red Ethernet, cuyo uso se está generalizando para la comunicación entre los Sistemas de Automatización de Subestación, con objeto de sincronizar los relojes internos de los dispositivos instalados a lo largo de la Subestación.

La ventaja de este método radica en que no se necesita el despliegue de un cableado adicional. Sin embargo, sí que se requiere el uso de protocolos apropiados y compatibles con todos los tipos de dispositivos conectados a una Subestación.

Así, para este tipo de sincronizaciones, encontramos los protocolos NTP (Network Time Protocol) y PTP (Precision Time Protocol) los cuales realizan el intercambio de mensajes de sincronización sobre una red Ethernet. El retraso en la sincronización debido a la propagación por la red es compensado por ambos protocolos mediante comunicaciones bidireccionales.

El uso del protocolo NTP se ha generalizado estando actualmente bastante extendido para la automatización de Subestaciones. No obstante, PTP ofrece mayor precisión y rendimiento gracias al despliegue de un hardware de red específico.

Para dotar de mayor redundancia y, por ende, fiabilidad a la red de sincronización temporal de la Subestación, ambos protocolos permiten la conexión de múltiples relojes maestros. Otra ventaja adicional de esta posibilidad es que permite la realización de labores de mantenimiento sin necesidad de interrumpir el servicio de sincronización temporal.

El protocolo PTP, definido en el estándar IEEE 1588, constituye un mecanismo de sincronización temporal de alta precisión a través del uso de un hardware Ethernet específico que permite registrar el momento exacto de recepción de un mensaje de sincronización PTP en la tarjeta de red Ethernet.

El protocolo plantea estrategias para compensar la incertidumbre temporal que pueda ser generada por el propio sistema operativo en tiempo real o cualquier otro retraso derivado del procesamiento de la señal tanto en el maestro de sincronización como en los dispositivos a sincronizar.

De este modo, el protocolo PTP, mediante el uso de equipos de red homologados y ya disponibles en el mercado, permite alcanzar precisiones en el marcado de las señales de hasta 10ns.

En la versión 2 del estándar, PTPv2, se presenta un tipo especial de switch Ethernet denominado “transparent clock” que permite alcanzar mayores precisiones en el marcado temporal midiendo el tiempo de latencia causado por la carga de tráfico y compensando el retraso. Esto lleva implícito que, a nivel de gestión de red, no sea necesario priorizar este tráfico de mensajes, simplificando así el diseño de la red.

Por otro lado, es importante destacar que el hardware específico para el marcado de tiempo según el protocolo PTP es independiente, por lo que no afecta al rendimiento de los dispositivos para el procesamiento de mensajes de otros protocolos, como IEC61850, DNP3.0, Modbus o IEC104, que se reciben en el mismo puerto Ethernet.

3.5 Internet Social de las Cosas

El arquetipo de Internet Social de las Cosas (SIoT, Social Internet of Things) define cómo las personas acceden y se integran con las cosas, llevando conceptos de Redes Sociales (SN, Social Networking) al ámbito del Internet de las Cosas. Las ventajas de este concepto son fundamentalmente [51]:

- Dotar a IoT de una estructura que se pueda configurar según sea necesario para garantizar la navegabilidad en la red, para que el descubrimiento de objetos y servicios se realice de forma efectiva y se garantice la escalabilidad, como en las Redes Sociales ”humanas” [52].
- Extender el uso de modelos inicialmente diseñados para estudiar redes sociales para abordar problemas relacionados con IoT (intrínsecamente relacionados con redes extensas de objetos interconectados).
- Crear un nivel de confiabilidad a partir del nivel de interacción entre las cosas en la red social aprovechando que, en dicha red, las cosas se siguen unas a otras y son "amigos" y por lo tanto existe un nivel de confianza entre ellas.
- Un enfoque distribuido, que se espera que garantice una mayor escalabilidad y una mejor reacción a los frecuentes cambios de estado que caracterizan los objetos implicados en el IoT [51].

3.5.1 Internet de las Cosas

El Internet de las Cosas es ya una realidad. En los últimos años ha crecido exponencialmente el número de artículos en relación con IoT.

Los productos cotidianos se han desarrollado hasta convertirse en elementos conectados. Primero fue el paso de teléfono móvil a smartphone. De éste surgió una evolución, un

producto que combinaba la versatilidad de un pc portátil con la movilidad de un teléfono móvil en la forma de una libreta, las tablets. Después, empezaron a surgir ideas como los smartwatches o los llamados wearables, otros casos del mismo fenómeno. El factor común de todas estas evoluciones es también la esencia del Internet de las Cosas: añadir valor a elementos dotándolos de un diseño inteligente que les permita interactuar con nuestro entorno virtual. El concepto básico es dotar a las cosas de conectividad a Internet. En este contexto, cuando se habla de “cosas” se está haciendo referencia a cualquier elemento susceptible de ser conectado.

Por otro lado, una vez los dispositivos conectados, lo verdaderamente relevante del concepto, es lo que se hace con los datos de las “cosas”. En este sentido existen las denominadas plataformas de IoT que básicamente son un software donde se recogen los datos de las “cosas” y se desarrollan aplicaciones para explotarlos, cruzándolos con datos de otras fuentes, aplicando algoritmos y representándolos. Por lo tanto, una plataforma de este tipo estaría constituida generalmente por los siguientes módulos: [53] (ver Figura 20): conectividad y normalización, gestión de dispositivos, base de datos, procesamiento y gestión, analítica, visualización, herramientas adicionales e interfaces externas.

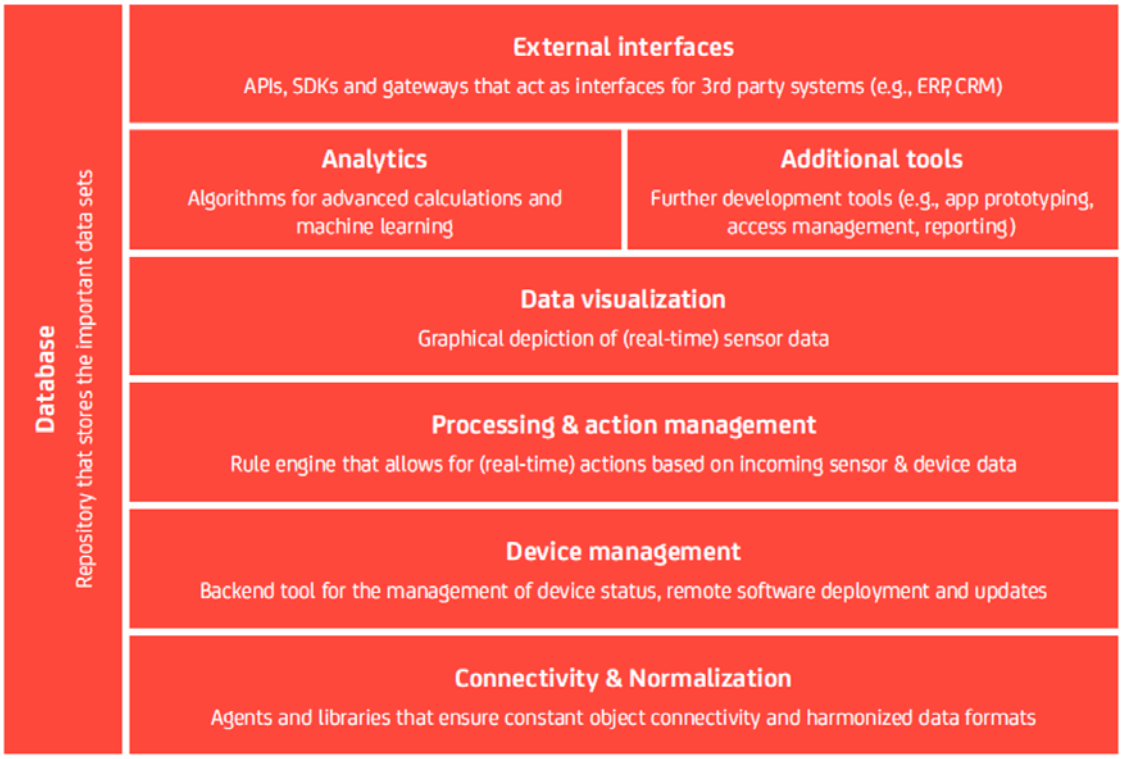

Figura 20: Elementos de una plataforma IoT. [Fuente: IoT Analytics https://iot-analytics.com/5-things-know-about-iot-platform/]

A continuación se presentan los protocolos y las plataformas IoT más relevantes.

3.5.1.1 Protocolos de Comunicación IoT

Seguidamente se indican los protocolos de comunicación IoT más usados, teniendo en cuenta sus prestaciones para una futura implementación en el escenario de la Subestación y más concretamente sobre un dispositivo RTU: AMQP, MQTT, OPC UA, STOMP, XMPP, CoAP, HTTP y DDS. Notar que dichos protocolos no suelen estar disponibles sobre las RTUs.

En el sector eléctrico el uso de dichos protocolos está en una fase muy prematura, aunque existen algunas referencias, como son las del uso de AMQP, MQTT en Volttrom [54], una plataforma de Pacific Northwest National Laboratory que conecta dispositivos, agentes y concentra señales de la red eléctrica, la cual se utiliza en Duke Energy [55]. También existen referencias de XMPP ya que el estándar de Subestaciones IEC61850 lo ha seleccionado como protocolo de control de recursos energéticos distribuidos [56], y del protocolo DDS, que es usado por varias empresas del sector como Siemens en sus soluciones aplicables a instalaciones de aerogeneradores [57]. Por último, OPC UA, para el que existen referencias en las que se establece un mapeo con el estándar IEC61850 [58], así como de su uso en comunicaciones con SCADA o DCS (Distributed Control System) [59].

Destacar también, el reciente artículo publicado en febrero de 2018 sobre “Substation sensing monitoring system based on power Internet of things” [60] donde un sistema de IoT realiza la monitorización en tiempo real de equipos de la Subestación, aplicando la correspondiente analítica de datos para la mejora de la operación y mantenimiento de la Subestación.

3.5.1.2 Plataformas IoT

A continuación se listan algunas de las plataformas de IoT más usadas, teniendo en cuenta sus prestaciones para una futura implementación en el escenario de la Subestación y más concretamente en comunicación con una RTU: Azure IoT Hub (compatible con los protocolos HTTP, AMQP, OPC UA y MQTT), CloudPlugs (MQTT y HTTP), Amazon AWS IoT (MQTT y HTTP), Fiware (MQTT, HTTP y CoAP), Google Cloud, Sofía2 (AMQP, HTTP y MQTT) y Oracle IoT Cloud Service (HTTP, MQTT).

La solución que propone Azure para IoT la usan empresas como TransAlta, eléctrica canadiense, para la gestión, validación y toma de decisiones sobre la actividad de sus generadores; o Hafslund, el mayor distribuidor eléctrico de noruega, para una solución diseñada de facturación, recolección y análisis de los datos proporcionados por los medidores inteligentes para una mayor eficiencia energética y operacional [61].

En lo que respecta a Fiware existen referencias de varias entidades como BD4BS, que ofrece soluciones Big Data para encontrar, predecir y eliminar pérdidas de energía a través de los dispositivos IoT, o Trafisense, que emplea Fiware para el mantenimiento predictivo de transformadores [62].

3.5.2 Redes Sociales

Una Red Social se define como un servicio que permite a las personas confeccionar un perfil público o semipúblico dentro de un sistema limitado, articular una lista de otros usuarios con quienes comparten una publicación, ver y recorrer su lista de publicaciones y las hechas por otros dentro del sistema. La naturaleza y la nomenclatura de estas publicaciones pueden variar de un sitio a otro [63].

El término se atribuye a los antropólogos británicos Alfred Radcliffe-Brown y John Barnes. Las redes sociales son parte de nuestra vida, son la forma en la que se estructuran las relaciones personales, estamos conectados mucho antes de tener conexión a Internet. En antropología y sociología, las redes sociales han sido materia de estudio en diferentes campos, desde el análisis de las relaciones de parentesco en grupos pequeños hasta las nuevas investigaciones sobre diásporas de inmigrantes en entornos multisituados. Pero el análisis de las redes sociales también ha sido llevado a cabo por otras especialidades que no pertenecen a las ciencias sociales. Por ejemplo, en matemáticas y ciencias de la computación, la teoría de grafos representa las redes sociales mediante nodos conectados por aristas, donde los nodos serían los individuos y las aristas las relaciones que les unen. Todo ello conforma un grafo, una estructura de datos que permite describir las propiedades de una red social. A través de esta teoría, se pueden analizar las redes sociales existentes entre los empleados de una empresa y, de igual manera, entre los amigos de Facebook [64].

Con la llegada de la Web 2.0 existe una revolución en cuando al concepto de red social, pasando de “solo lectura” a “lectura y escritura”. Aparecen los Social Media o medios sociales, definidos por los profesores de la Universidad de Indiana, Andreas M. Kaplan y Michel Haenlein, como “grupo de aplicaciones basadas en internet, desarrolladas sobre medios tecnológicos que permiten la creación e intercambio de contenidos generados por el usuario” [64].

Las redes sociales abren un mundo de posibilidades de uso, ya que la información compartida es muy diversa y existe una oportunidad para su explotación desde muchos puntos de vista. La capacidad de difusión con la que cuenta esta tecnología es enorme, ya que con un simple “clic” es posible que algo escrito, grabado o leído por el usuario sea transmitido casi al instante a millones de personas.

Esta forma de interconexión personal y profesional ha tenido tanto impacto que ya se ha convertido en una temática de estudio de análisis. Existen estudios sobre Análisis de Redes Sociales, también llamado análisis de datos reticulares o estructurales. Un ejemplo de este gran interés en el estudio de los Análisis de Redes Sociales es la conferencia internacional ASONAM (Advances in Social Networks Analysis and Mining) [65], celebrada desde 2009 y promotora de la investigación y desarrollo de nuevas técnicas de análisis en el contexto evolutivo de las redes sociales.

El auge de las redes sociales se puede explicar por distintos factores. Por un lado, el despliegue masivo de dispositivos móviles al que se le suma la facilidad de acceso a internet tanto desde hogares como desde los propios dispositivos móviles gracias a tarifas más asequibles de internet y datos móviles. Por otro lado, las posibilidades de compartir

fotos, videos y audios, así como de enriquecer o simplificar la expresión escrita con emoticonos y sticker, además de ser posible la realización de llamadas y videollamadas.

Al mismo tiempo, varias de las redes sociales y sus aplicaciones de mensajería más extendidas han desarrollado funciones para la interacción automatizada en función de ciertos parámetros, a través de APIs (Application Programming Interface) públicas y Bots (programa de envío de mensajes automáticos que interacciona con humanos y otros programas). Este modo de interacción permite desarrollar nuevos tipos de comunicación más allá de las tradicionales usuario-usuario y usuario-grupo, como por ejemplo modelos enfocados al comercio electrónico como consumidor-negocio (C2B), negocio-consumidor (B2C) o incluso otros más complejos que involucren a varios actores. Al aplicar la interacción automatizada a otros ámbitos, como el industrial, se pueden desarrollar sistemas de comunicación máquina-humano, o incluso máquina-máquina-humano, para la gestión de sistemas industriales.

3.5.2.1 Tendencias en el mercado de las Redes Sociales

Las redes sociales han experimentado un crecimiento exponencial. Facebook se ha mantenido líder [66], seguido de otras aplicaciones veteranas como Twitter. Sin embargo, estas plataformas han ralentizado su crecimiento en los últimos años, al mismo tiempo que ganaban protagonismo otras plataformas sociales más especializadas como Instagram, Vine, Pinterest, Periscope, etc.

A continuación se presentan las redes sociales más populares por países en el año 2017. En la Figura 21 están representadas las predominantes.

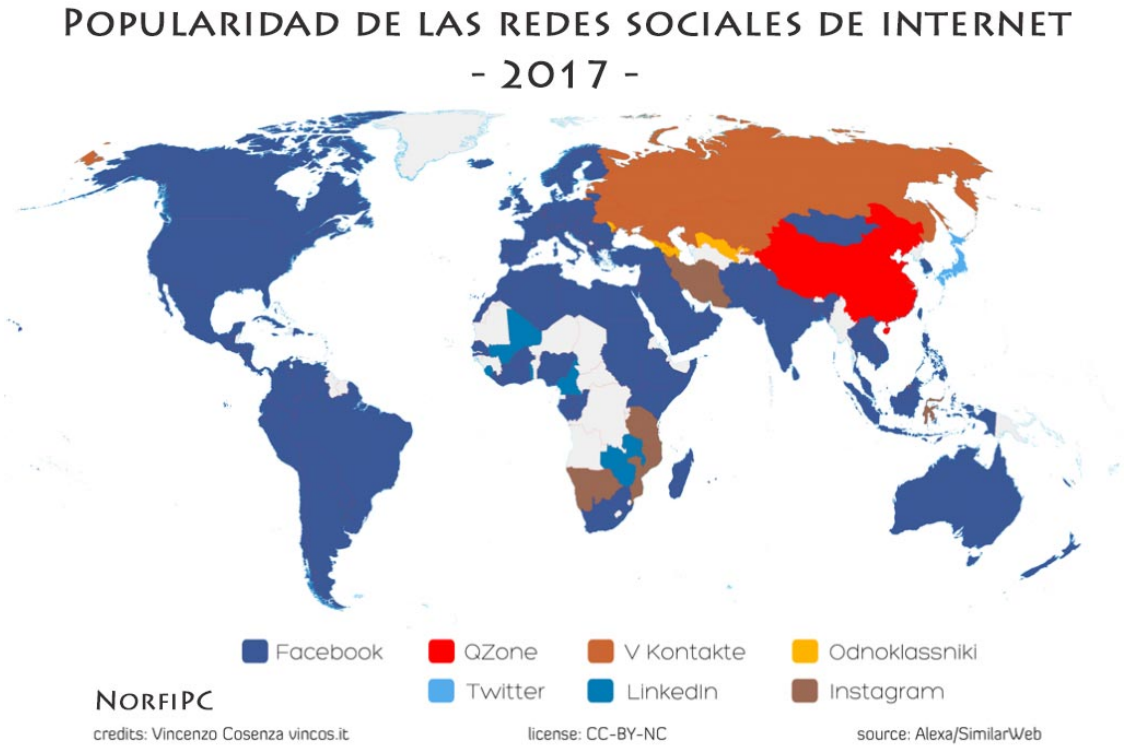

Figura 21: Popularidad de las Redes Sociales en 2017. [Fuente: Alexa/SimilarWeb/ [66]]

En la Figura 22 se presentan aquellas redes sociales que se sitúan en segunda posición en términos de uso.

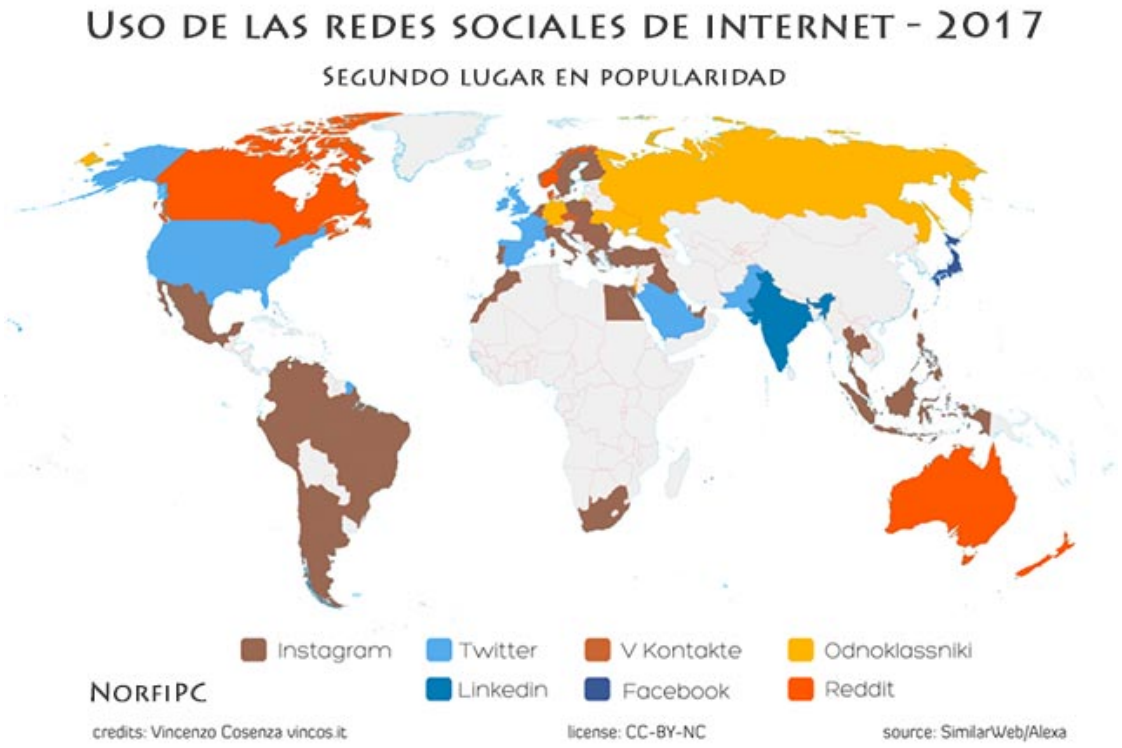

Figura 22: Segundo lugar de Popularidad de las Redes Sociales en 2017. [Fuente: Alexa/SimilarWeb/ [66]]

Por otro lado, el auge paralelo del uso de los dispositivos móviles ha provocado que las aplicaciones móviles ganasen en popularidad. En este contexto destacan las aplicaciones de mensajería instantánea. Aunque WhatsApp fue de las primeras en popularizarse, con el paso del tiempo han surgido otras alternativas en diferentes países como Telegram, Snapchat, Kik, LINE, WeChat, Viber, KakaoTalk, Wire, etc. Respecto a estas nuevas aplicaciones, cabe resaltar que Snapchat y Kik han ganado popularidad gracias a potenciar la privacidad y el anonimato mientras que Telegram ha apostado fuerte en la seguridad y los grupos. En este competitivo escenario, tanto las redes sociales tradicionales como las aplicaciones pioneras como WhatsApp han entendido que no pueden quedarse atrás, y han decido incorporar nuevas funcionalidades similares a las de sus más serios rivales, teniendo en cuenta su crecimiento.

Una funcionalidad interesante que están potenciando algunas plataformas como Telegram, Kik y también Facebook es el uso de Bots. Estos Bots simulan usuarios virtuales y permiten responder a preguntas básicas [67], [68].

En el mercado asiático el uso de Bots ya ha sido popularizado por aplicaciones como WeChat y LINE. Los Bots abren la puerta a un sinfín de posibilidades, por ejemplo, en el

ámbito del comercio electrónico y los servicios de atención al cliente. En una visión a futuro los Bots han sido clasificados como la próxima frontera y la interfaz mediante mensajes podrá incluso reemplazar a las actuales Apps [69].

Seguidamente, se presentan las redes sociales enfocadas a mensajería más destacadas. A nivel mundial, las aplicaciones de mensajería más utilizadas en 2016 según [70] son las siguientes:

1º: WhatsApp (+1.000 millones).
2º: Facebook Messenger (+900 millones).
3º: QQ (853 millones).
4º: WeChat (697 millones).
5º: Skype (300 millones).
6º: Viber (249 millones).
7º: LINE (215 millones).
8º: BlackBerry Messenger (100 millones).
9º: Telegram (100 millones).
10º: KakaoTalk (48 millones).

Y según el ranking de aplicaciones de mensajería más importantes en 2016 por país de SimilarWeb [71]:

1º: WhatsApp (primero en España, Alemania y otros 107 países).
2º: Facebook Messenger (primero en Estados Unidos, Francia y otros 47 países).
3º: Viber (primero en Ucrania y otros 14 países).
4º: Line (primero en Japón y otros 3 países).
5º: WeChat (primero en China y otros 2 países).
6º: Telegram (primero en Irán y Uzbekistán).
7º: KakaoTalk (primero en Corea del Sur).
8º: imo (primero en Cuba).
9º: Zalo (primero en Vietnam).
10º: BlackBerry Messenger (primero en Indonesia).
11º: ChatOn (primero en Eritrea).

3.5.3 Procesamiento de Lenguajes Naturales

El Lenguaje Natural es el medio que se utiliza habitualmente para establecer la comunicación con las demás personas. El Lenguaje Natural ha venido perfeccionándose a partir de la experiencia a tal punto que puede ser utilizado para analizar situaciones altamente complejas y razonar muy sutilmente. Los lenguajes naturales tienen un gran poder expresivo y un importante valor como herramienta de razonamiento. Por otro lado, la sintaxis de un Lenguaje Natural puede ser modelada fácilmente por un lenguaje formal, similar a los utilizados en las matemáticas y la lógica [72].

Una meta fundamental de la Inteligencia Artificial (IA) es la manipulación de lenguajes naturales usando herramientas de computación, donde los lenguajes de programación juegan un papel importante, ya que forman el enlace necesario entre los lenguajes naturales y su manipulación por una máquina [72].

El Procesamiento del Lenguaje Natural (PLN) es el campo que combina las tecnologías de la ciencia computacional (como la inteligencia artificial, el aprendizaje automático o la inferencia estadística) con la lingüística aplicada, con el objetivo de hacer posible la comprensión y el procesamiento asistidos por ordenador de información expresada en lenguaje humano para determinadas tareas, como la traducción automática, los sistemas de diálogo interactivos, el análisis de opiniones, etc. [73].

En los últimos años, las aportaciones al PLN han mejorado sustancialmente, permitiendo el procesamiento de ingentes cantidades de información en formato texto con un grado de eficacia muy aceptable. Muestra de ello es la aplicación de estas técnicas como una componente esencial en los motores de búsqueda web, en las herramientas de traducción automática, y especialmente en las aplicaciones de inteligencia artificial. En este último caso cabe destacar la irrupción de los asistentes de voz como Siri de Apple iOS o Cortana de Windows. La interfaz de usuario mediante mensajes, ya sean de voz o escritos, se ha establecido como una tendencia de futuro. En el ámbito de las redes sociales y aplicaciones de mensajerías cada vez existen más desarrollos orientados a implantar inteligencias artificiales que asistan a los usuarios y que comprendan los mensajes enviados por los mismos para darles una repuesta adecuada [74].

Debido al auge de la incorporación de inteligencia artificial en las aplicaciones han surgido varias iniciativas y compañías que ofrecen servicios de procesamiento de lenguaje natural y creación de Bots que permitan responder automáticamente a las necesidades y preguntas de los usuarios. Estas plataformas ofrecen APIs y librerías para implementar análisis de mensajes y enviar mensajes automáticos a través de diversas aplicaciones. Muchas de ellas incorporan el concepto de Machine Learning que permite a las aplicaciones aprender de las conversaciones previas para así proporcionar respuestas más adecuadas según el contexto. Algunos ejemplos de estas herramientas son [75], [76], [77], [78], [79]:

- wit.ai – API de Procesamiento de Lenguaje Natural, gratuita y de código abierto.
- Watson – API de Procesamiento de Lenguaje Natural de IBM.
- Language Understanding Intelligent Service - API de Procesamiento de Lenguaje Natural de Microsoft.
- Node/Natural – Librería de Procesamiento de Lenguaje Natural para node.js
- Natural Language Toolkit - Librería de Procesamiento de Lenguaje Natural para Python.

Por otro lado, también existen algunas librerías de Procesamiento de Lenguaje Natural para java, orientadas más al procesamiento general de textos que al contexto específico de una conversación. Entre los ejemplos de estas librerías se pueden destacar [80], [81], [82]:

- Apache OpenNLP
- Stanford NLP
- LingPipe

Como aspecto negativo, cabe comentar que las funcionalidades de estas últimas librerías para Java resultan bastante prefijadas y ofrecen limitadas posibilidades de personalización según el proyecto.

3.6 Conclusiones

En este capítulo se ha presentado el estado de las tecnologías de referencia para las aportaciones científicas de los siguientes capítulos. El apartado 3.1 “IEC61850”, servirá como punto de partida tanto para el Capítulo 4 como para el Capítulo 5, al ser el principal estándar del dominio de aplicación tratado en dichos capítulos. Además, el Capítulo 4 se basará en el apartado 3.3, mientras que en el Capítulo 5 se referenciará el apartado 3.2 “Seguridad”, 3.4 “Sincronización” y el subapartado 3.5.1 “Internet de las Cosas” por su relación con IoT. Este último subapartado junto con el resto de subapartados del apartado 3.5 “Internet Social de las Cosas” constituyen la base teórica del Capítulo 6.

Capítulo 4. Nuevo Sistema de Protección Adaptativa Basado en el Estándar IEC61850

En SmartGrid, la instalación de sistemas y dispositivos de protección en la red de Media Tensión es probablemente uno de los temas más relevantes. En particular en aquellos sitios, donde las distintas regulaciones de los sistemas de distribución incluyen incentivos basados en resultados ligados a la calidad de servicio para los Operadores de los Sistemas de Distribución.

Las aplicaciones, como la Selectividad Lógica (LS, Logic Selectivity), que reducen número de interrupciones y la duración de las mismas, pueden ser ejecutadas por las RTUs actuando en este caso como IEDs de protección. A su vez, pueden combinarse con el estándar IEC61850, en donde los mensajes GOOSE a través de internet entre RTUs pueden ser utilizados para la implementación de dicha Selectividad Lógica.

En este sentido, la seguridad debe ser tenida en cuenta, por lo que, para securizar las comunicaciones de Selectividad Lógica con GOOSE, en este capítulo se propone utilizar Tunelización Capa 2 (Layer 2 Tunneling) sobre el protocolo de seguridad IPsec, el cual ha sido introducido en el apartado 3.2.

Por otro lado, comentar que la principal limitación de la Selectividad Lógica es la configuración de las protecciones y las lógicas pues ambas se basan en la configuración estándar de la red de distribución de energía. De esta forma, cuando cambia la configuración de la red, la lógica y la configuración de las protecciones dejan de ser válidas, lo que se convierte en un problema importante. El presente capítulo muestra un enfoque innovador para la reconfiguración dinámica de los dispositivos de protección utilizados para implementar soluciones avanzadas de localización de faltas, aislamiento y restauración de servicio.

En este capítulo, partiendo del apartado 3.1 “IEC61850”, se incide en los aspectos relevantes de dicho estándar directamente relacionados con la contribución científica realizada, se estudia la funcionalidad de Selectividad Lógica profundizando en lo presentado en el apartado 3.3, y además se propone un método de securización. Asimismo, se presenta la estructura general de la arquitectura y la solución implementada, así como los resultados relevantes y las conclusiones.

La investigación descrita en el presente capítulo se realizó en el marco del proyecto europeo IDE4L [83].

4.1 Introducción

Las redes de distribución eléctrica afrontan varios desafíos en los últimos años. La cada vez más profunda penetración de los sistemas de generación distribuida, la llegada del vehículo eléctrico, así como las mayores exigencias de las normativas nacionales e internacionales en relación con la calidad de servicio, requieren una importante mejora en la gestión de la red de distribución, dado el aumento de su complejidad [84], [85], [86], particularmente cuando se produce un fallo en la misma [87]. En este escenario, la calidad de suministro, la confiabilidad y el coste de las sanciones administrativas se encuentran a

la vanguardia de las preocupaciones de las *Utilities*, ya que un coste significativo está relacionado con las interrupciones del servicio no programadas y la reputación de la empresa [88].

Los costos que soporta el consumidor final debido a las interrupciones de servicio y la baja confiabilidad de la red han crecido durante los últimos años, lo cual se debe a la importante relación entre la productividad y la confiabilidad. Seguidamente se presentan el impacto de interrupciones no programadas en 63 centros de datos de Estados Unidos comparando los años 2010, 2013 y 2016 [89]. Se puede observar como el coste producido por las interrupciones ha seguido aumentando en prácticamente todas las actividades analizadas, siendo muy significativo el asociado al negocio. Por tanto, se puede afirmar que la disminución de las interrupciones se traduce directamente en mejoras de la cuenta de resultados y justifica económicamente una oportunidad de negocio en este ámbito.

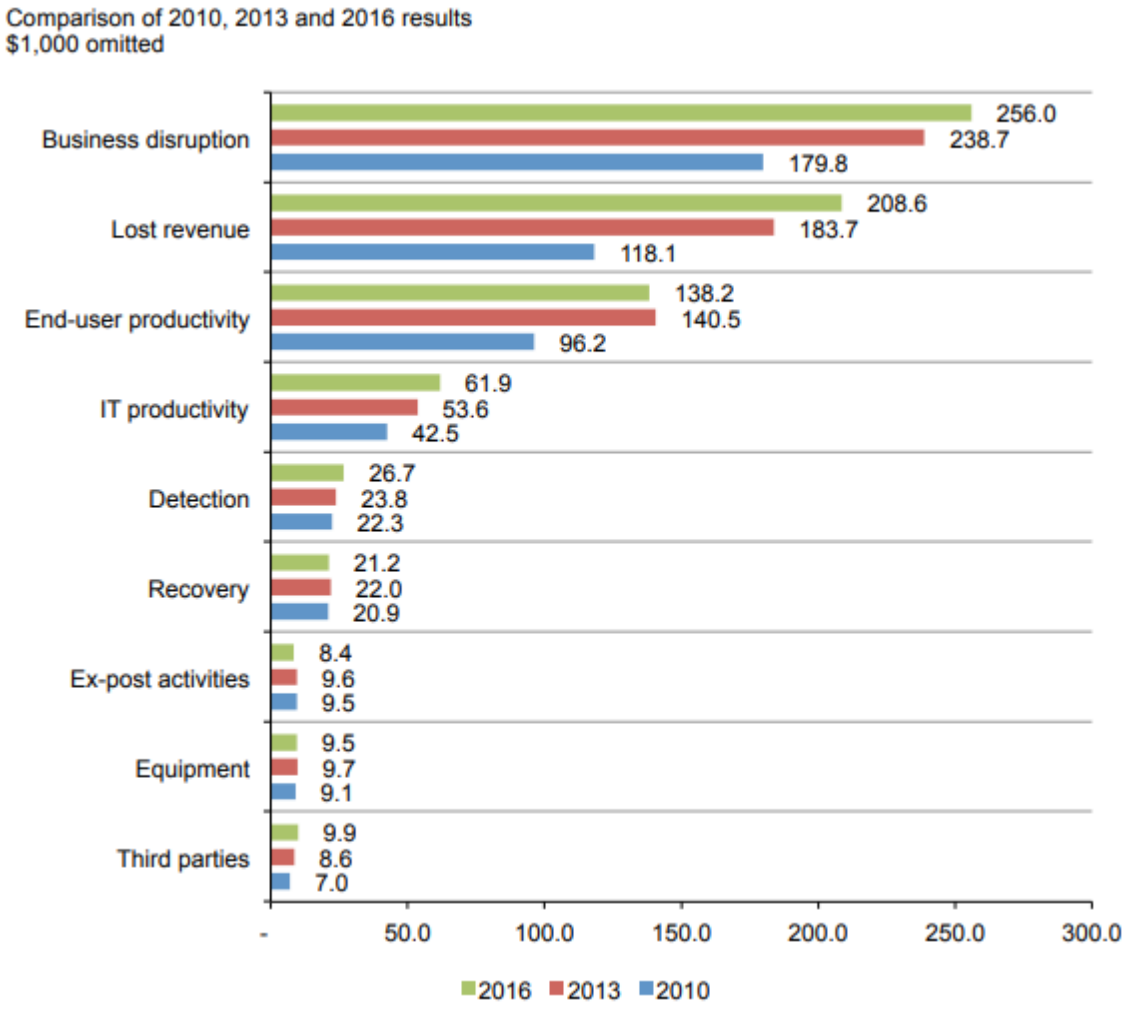

Figura 23: Comparación de costes de interrupciones no programadas en 63 centros de datos durante los años 2010, 2013 y 2016 en miles de dólares. [Fuente: Ponemon Institute, Cost of Data Center Outages January 2016 [89]]

Estos costes no solo están relacionados con la presencia de una perturbación, sino que también están relacionados con su gravedad en términos de varios parámetros, como la duración del problema. Con respecto a este aspecto, la siguiente figura muestra el vínculo existente entre la duración de una interrupción no planificada en un centro de datos y los costos asociados. Como se muestra, la media de los costes aumenta con la duración de la interrupción [89].

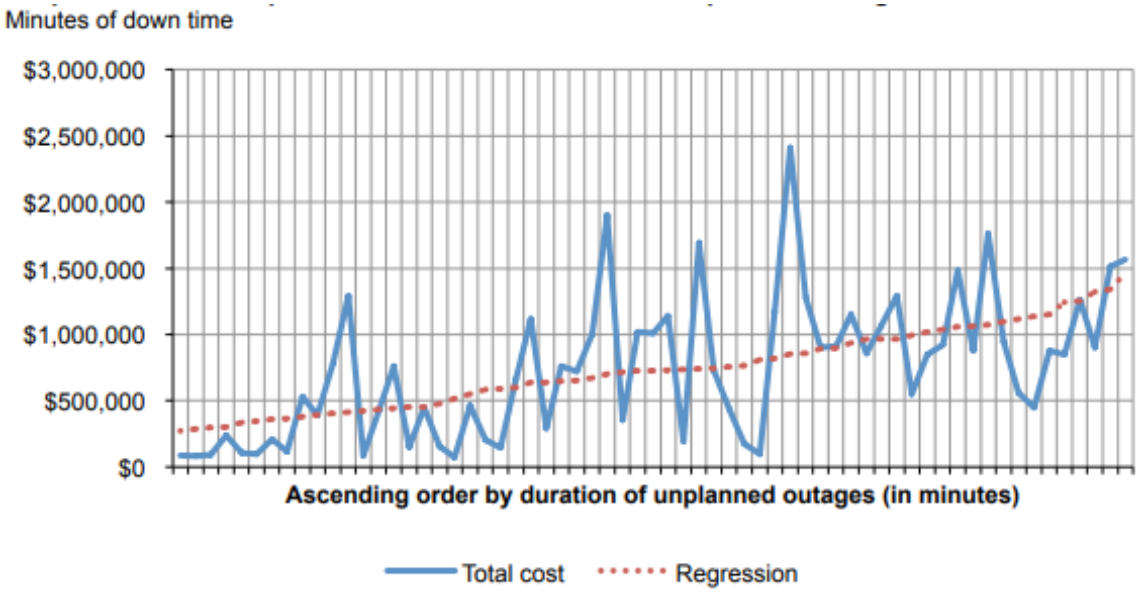

Figura 24: Coste de interrupciones no programadas vs el tiempo en minutos. [Fuente: Ponemon Institute, Cost of Data Center Outages January 2016 [89]]

Este tipo de costes afecta, prácticamente a todos los sectores industriales, como se muestra en la Figura 25 en la que se representa el impacto de las interrupciones de servicio no planificadas en 16 sectores industriales de Estados Unidos entre 2010 y 2016 [89]. Como se puede observar, existe un importante impacto en todos ellos siendo el más crítico el sector financiero. A su vez se aprecian diferencias significativas de dicho sector con respecto al sector público que viene a ser el menos afectado.

En este contexto, la madurez de las tecnologías de Automatización de la Distribución y la aparición de una importante variedad de tecnologías de comunicación brinda a las *Utilities* la oportunidad de reducir considerablemente las interrupciones de servicio no programadas [90]. Además, este enfoque viene reforzado por la reducción de costes de los interruptores de Media Tensión que son capaces de interrumpir las corrientes de cortocircuito. De hecho, en los últimos años, solo se utilizaron interruptores de carga, capaces de interrumpir corrientes cuyos valores eran como máximo el nominal [91].

De esta forma, las estrategias de auto-reparación indicadas en el apartado 3.3, también conocidas por FLISR, desempeñan un importante papel en la mejora de la red en cuanto a fiabilidad, aumento de energía suministrada y calidad de servicio [88], [92], [93], [94], [95], lo que al final resulta en un aumento de los beneficios económicos de las *Utilities* debido a la reducción de costes relacionados con las interrupciones de servicio de los

clientes, el aumento de la energía suministrada e incentivos de las autoridades reguladoras.

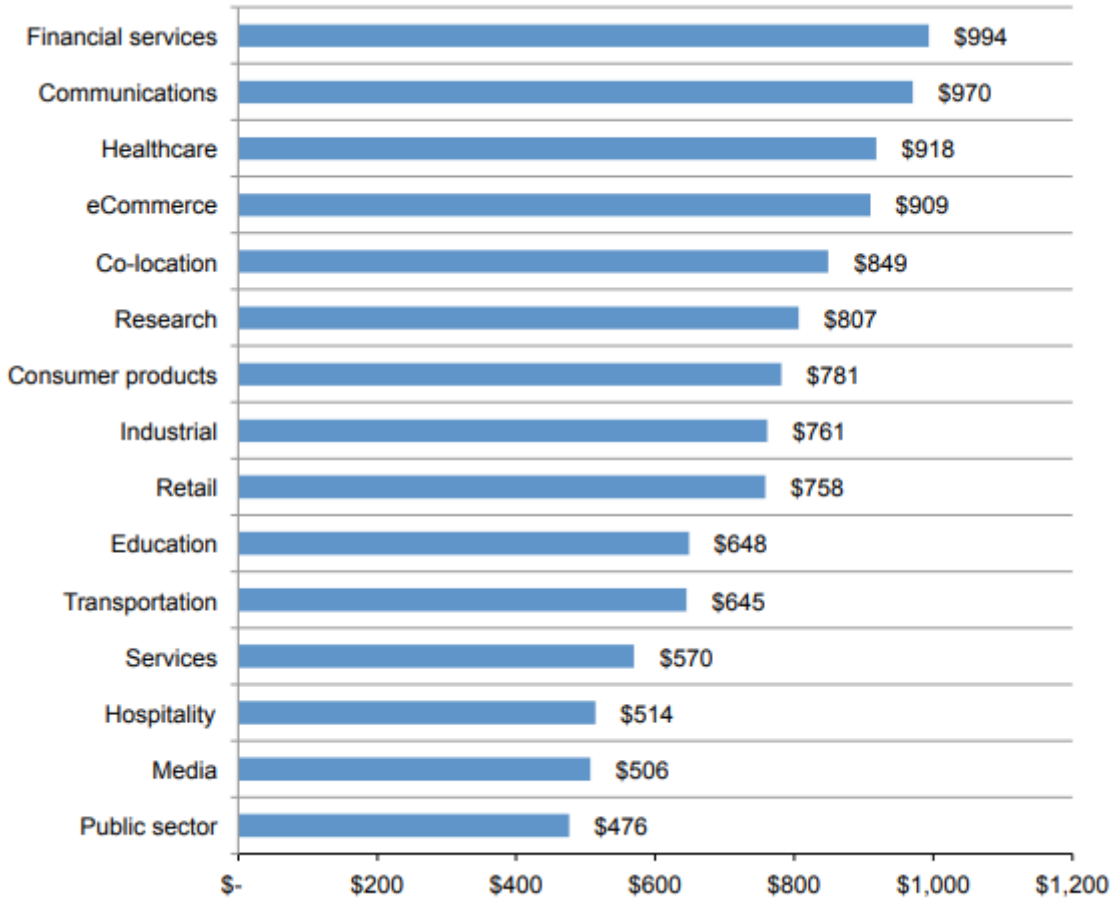

Figura 25: Impacto de la calidad en el sector industrial de Estados Unidos en miles de dólares. [Fuente: Ponemon Institute, Cost of Data Center Outages January 2016 [89]]

En lo que respecta a la detección de faltas (Fault Detection), existen varias técnicas que se usan dependiendo de los tipos de faltas que se detectan: monitorización de corriente o voltaje [96], técnicas avanzadas de detección transitoria como análisis de transformada Wavelet [84], asimetría de fase y componente de secuencia negativa [97] o fasores capturados por PMU (Phasor Measurement Unit) [98].

Por otro lado, en lo relativo a la localización de falta (Fault Location), en ausencia de generación distribuida, se supone que una falta se ubica entre el último componente que detecta la corriente de falta y el primer componente que no detecta la falta. Sin embargo, en el caso de una red activa con generación distribuida y con una configuración dinámica, los indicadores de faltas direccionales pueden ser útiles para la localización [99]. Así, se pueden aplicar diferentes métodos para determinar el punto donde se localiza la falta exactamente, los cuales utilizan datos como: componente de frecuencia fundamental [100] o medición de onda de alta frecuencia y desplazamiento [101], [102]. Además, se pueden aplicar técnicas como lógica difusa [103] o redes neuronales [104] aunque

requieren un gran conocimiento del sistema específico y un largo período de entrenamiento del modelo.

Por lo tanto, las investigaciones sobre FLISR son, hoy en día, de gran interés para la Automatización de la Distribución, de hecho, en los últimos años, se han propuesto una gran variedad de enfoques basados en distintas arquitecturas de automatización para estudiar los problemas relacionados con Automatización de la Distribución. Muchos de esos enfoques se basan en configuraciones FLISR centralizadas, donde la lógica principal se coloca en un servidor central desplegado como parte del Sistema de Gestión de la Distribución [94].

A su vez, se han presentado otras aproximaciones, como la descentralizada, en donde la lógica para la toma de decisiones se sitúa en la RTU a nivel de Subestación [105]. Y, por último, también tenemos la aproximación denominada semi-centralizada [105], que se basa en el uso tanto de las RTUs de Subestación, como del Centro de Control para el proceso de toma de decisiones. Dichas aproximaciones se ilustran en la siguiente figura, en donde se observa cómo se aplica a arquitecturas que van desde las más complejas hasta las más simples, y como disminuye el tiempo máximo de reacción, así como los sistemas involucrados:

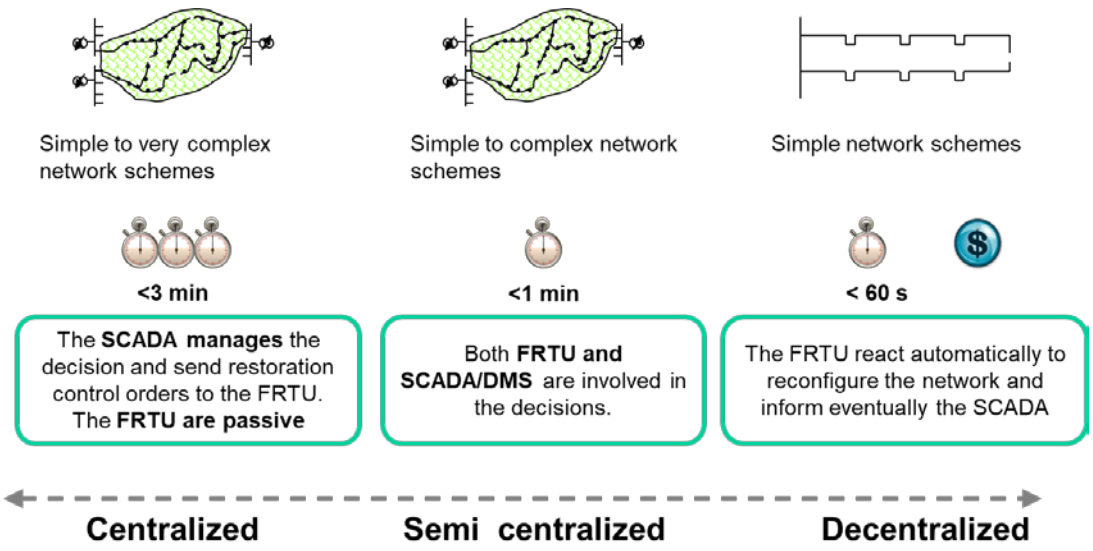

Figura 26: Aproximación centralizada, semi-centralizada y descentralizada. [Fuente: Proyecto IDE4L [83]]

En general, las aproximaciones semi-centralizadas y descentralizadas reducen el coste computacional y el tráfico de comunicaciones en el Centro de Control, permitiendo, asimismo, acelerar los procesos de self-healing a nivel local. Una solución puramente descentralizada se presenta en el artículo “Smart Grid Automation Based on IEC 61850: An Experimental Characterization” [106], en la que se describe el impacto en la calidad de servicio de una solución en la que, basándose en la instalación de interruptores en los feeders de la red de Media Tensión, los dispositivos de protección se coordinan usando el concepto de Selectividad Lógica para aislar selectivamente la falta [107]. Por lo tanto,

esta solución permite que la instalación de sistemas de protección en la red de Media Tensión se convierta en una de las soluciones de SmartGrid más rentables en aquellos sitios donde la regulación de los Operadores de los Sistemas de Distribución incluye incentivos basados en resultados.

Adicionalmente, la Selectividad Lógica [108] disminuye considerablemente el número de interrupciones y su duración, obteniendo beneficios de la automatización del feeder [109] y de las tecnologías de comunicación. A fin de obtener todos los beneficios de la Selectividad Lógica, se requiere invertir en seccionadores tele-controlables, IEDs y en la red de comunicación para el intercambiando mensajes entre los mismos.

Respecto a las comunicaciones, se investiga en los medios de comunicación necesarios para implementar soluciones basadas en Selectividad Lógica [110]. En “Hybrid Communication Network for the Smart Grid: Validation of a Field Test Experience” [111], se presenta una comparación entre las diferentes tecnologías, destacando los pros y los contras de cada una de ellas. Así pues, el intercambio de mensajes, pueden estar basados en protocolos propietarios [112] o en el estándar IEC61850 [113]. Cabe señalar a este respecto, que el borrador del estándar IEC61850-90-6 propone Nodos Lógicos aplicados a Selectividad Lógica, de forma que los mensajes GOOSE se intercambian entre IEDs en una Selectividad Lógica estandarizada [31].

El Internet inalámbrico (4G, LTE), cumple con los requisitos de automatización en tiempo real [114] y es una solución prometedora para el canal de comunicación de intercambio de mensajes GOOSE entre IEDs [114] y, por tanto, para la Selectividad Lógica. Los mensajes GOOSE utilizan tramas multicast a nivel de Capa 2 en el modelo de interconexión de sistemas abiertos.

Por otro lado, en cuanto a la seguridad, la Tunelización Capa 2 sobre IPsec para las comunicaciones de Selectividad Lógica con GOOSE garantiza la integridad y confidencialidad de la información. Además, los IEDs deben estar conectados a Internet de alta velocidad con baja latencia y comportamiento determinista, lo que garantiza la entrega a tiempo de mensajes GOOSE entre IEDs.

Así mismo, otra problemática aparece por los cambios de topología de la red de Media Tensión, que puede deberse a diferentes razones ligadas a la operación y mantenimiento como, por ejemplo, para mitigar las congestiones y reducir las pérdidas, para preparar la red para el correspondiente mantenimiento, para restaurar el servicio después de una falta, etc.

Los IEDs situados a lo largo de la red de distribución deben estar configurados para reaccionar ante los posibles problemas para una cierta tipología de la red. Los cambios que alteran la topología de la red y agregan nuevas fuentes de generación distribuida a la misma, resultan en un cambio significativo de las condiciones lo que implica que la configuración de los IEDs deja de ser válida [115]. Además, la relación entre un IED determinado y los anteriores o posteriores puede cambiar debido a los cambios mencionados.

Por lo tanto, los futuros sistemas embebidos de protección y los estándares de comunicación deben prever la integración de mecanismos para la reconfiguración remota

y automática de los parámetros operacionales, permitiendo el correcto funcionamiento del sistema de automatización de distribución sin interrupciones.

Así pues, en la presente introducción se ha puesto de manifiesto la problemática que se presenta en las redes de distribución y el impacto económico de las interrupciones, además de la complejidad extra que representa la introducción en la red de la generación distribuida, y por tanto la importancia de la investigación sobre FLISR utilizando aproximaciones descentralizadas y Selectividad Lógica.

A continuación se presentará el uso del modelo de datos del estándar IEC61850 para actualizar los parámetros de la función de protección, así como la jerarquía entre los dispositivos de protección. Esta aproximación permite implementar una solución FLISR totalmente descentralizada, para reducir la duración de las interrupciones y adaptar las configuraciones de los diferentes IED a las necesidades de la red de distribución de SmartGrid.

4.2 Arquitectura del Sistema de Protección Adaptativo

La estructura arquitectónica del sistema de protección adaptativo propuesto se presenta a continuación, a partir de la definición de las funciones de protección que se utilizarán y el mapeado de nodos lógicos.

A) Funciones de Protección

Desde los años 70, se han utilizado dispositivos digitales de protección específicos en redes de Alta y Media Tensión. Sin embargo, hasta ahora, el uso de estos dispositivos se ha limitado a Subestaciones Primarias o sistemas de transmisión de alta tensión. Con los cambios introducidos por la Directiva Europea sobre el mercado interior de electricidad [116], la gestión de Subestaciones Primarias se ha compartido entre Operadores de Sistemas de Transmisión y Distribución, de modo que la responsabilidad de los Operadores de los Sistemas de Distribución comienza desde el transformador de Alta/Media Tensión. Así, en la presente tesis, solo se tiene en cuenta el lado de la Media Tensión de los Operadores de los Sistemas de Distribución, mostrando cómo las funciones de protección más utilizadas, que fueron diseñadas para Subestaciones Primarias, también se pueden utilizar en la red de distribución de Media Tensión. Una lista de las funciones de protección más comunes se presenta en la siguiente tabla.

67N - protecciones de sobrecorriente direccional
50P – sobreintensidad o de velocidad de aumento de intensidad
51P – sobreintensidad temporizada
81O – sobre frecuencia
81U – sub frecuencia
81R – ratio de cambio de frecuencia
79 – reenganche

Tabla 3: Principales funciones de protección usadas en la red de Media Tensión.

A continuación se describirá brevemente cada una de estas funciones de protección:

"**67N**" se usa principalmente para detectar faltas de fase a tierra, tanto en sistemas de distribución que trabajan con configuraciones de neutro aislado, como en tramos de línea "largos", en donde sea importante la corriente capacitiva que puede remontar el ramal de línea. En el caso de una falta de fase a tierra, la corriente de falta es generada principalmente por el componente capacitivo del cable de Media Tensión. Por lo tanto, la corriente y la tensión tienen un retardo de fase en un rango específico. Esta característica es utilizada por la función de protección "67N", que mide el ángulo entre la corriente y la tensión, para detectar la falta.

"**50P**" se usa principalmente para detectar un cortocircuito de fase a fase, generado por corrientes de magnitud extremadamente alta, mientras que "**51P**" se usa para detectar situaciones de sobrecarga mantenidas durante un intervalo de tiempo predefinido.

"**81O/U** y **81R**" se utilizan para detectar sobre/sub frecuencias y derivadas de frecuencia provenientes de la alta tensión. En caso de un problema grave, algunos códigos de red exigen deslastrar la carga para reequilibrar la red de transmisión.

Después de abrir el interruptor, el reenganche automático "**79**", se usa a menudo para restaurar el servicio en caso de faltas temporales. Comúnmente, esta función es adecuada para el caso de líneas aéreas o si los clientes conectados a la Media Tensión son capaces de gestionar las faltas en su red interna.

Los dispositivos de protección instalados a lo largo de los feeders de Media Tensión también se pueden usar como sistemas de monitorización. En particular, las medidas de corriente, tensión y potencia se pueden almacenar localmente en cada Subestación, donde se encuentra una unidad de automatización dedicada a tal efecto.

B) Mapeado de los Nodos Lógicos IEC61850

El primer paso para la implementación de la solución propuesta es garantizar que todos los parámetros que caracterizan la protección puedan ser accesibles y reconfigurables. Esto se hace mapeando dichos parámetros en el modelo de datos IEC61850, concretamente en el archivo CID, como se ha comentado en la sección "E" del apartado 3.1. Es necesario señalar que la mayoría de estos parámetros, concretamente los relacionados con la configuración de la función de protección, fueron definidos por la primera edición de la norma IEC61850 parte 7-4. Por ejemplo:

- Las protecciones de sobrecorriente direccional (ANSI 67N) se deben mapear en tres Nodos Lógicos: i) un PTOC para definir la parte de sobrecorriente; ii) un PTOV (protección de sobretensión) para definir la parte de sobretensión; iii) un RDIR (elemento direccional) para especificar la dirección.
- Las protecciones de sobreintensidad temporizadas (ANSI 50P/51P) deben mapearse directamente con un PTOC del Nodo Lógico.
- Las protecciones de reenganche (ANSI 79) deben mapearse en un RREC (elemento de auto recierre) del Nodo Lógico.

La idea detrás de la Reconfiguración del Sistema de Protección es actualizar la configuración del IED después de que se despeje la falta y se restaure el servicio, de forma que se reconfigure adecuadamente la red. Para ello, es necesario que se puedan configurar dinámicamente los publicadores y suscriptores de la información en la red. Dicha posibilidad no está actualmente contemplada en el estándar IEC61850, ni siquiera es la segunda edición. Sin embargo, la norma complementaria IEC TR 62689-100:2016 [117], propone nuevos Nodos Lógicos para facilitar la integración de indicadores de paso de falta en el marco del IEC61850. Entre ellos, por simplicidad, se han seleccionado para este fin dos Nodos Lógicos dotados de algunas extensiones, que se presentan seguidamente:

- CLSF: Selectividad Lógica de la gestión de sección defectuosa de la Media Tensión. En este Nodo Lógico se modela el rol del IED que hace de controlador local en la Selectividad Lógica diseñada en el proyecto IDE4L [28], incluyendo la información que se publicará para ser utilizada por los pares que están suscritos a dicha información. En el estándar IEC TR 62689-100:2016 [117] se contempla el modelado de esquemas de Selectividad Lógica entre los indicadores de paso de faltas. Sin embargo, el proyecto IDE4L también contempla esquemas de Selectividad Lógica para controladores de interruptores que se puedan aplicar a las líneas de distribución donde las Subestaciones Secundarias estén equipadas con funciones de protección e interruptores.
- ALSM: Selectividad Lógica de la monitorización de la sección defectuosa de la Media Tensión. En este Nodo Lógico se modela la suscripción a la información publicada por pares remotos que esté relacionada con faltas. El objetivo es bloquear la operación local del controlador sobre el seccionador o interruptor que se activará. Con el propósito de habilitar/deshabilitar el mensaje de ”bloqueo” asociado a un IED, la instancia correspondiente de ALSM se suministra con un objeto de datos denominado “Downstream IED”. Cuando se configura a “1”, los mensajes GOOSE de pares IEDs son mensajes de “bloqueo”.

La representación completa del modelo de datos de IED propuesto se esquematiza en la siguiente figura:

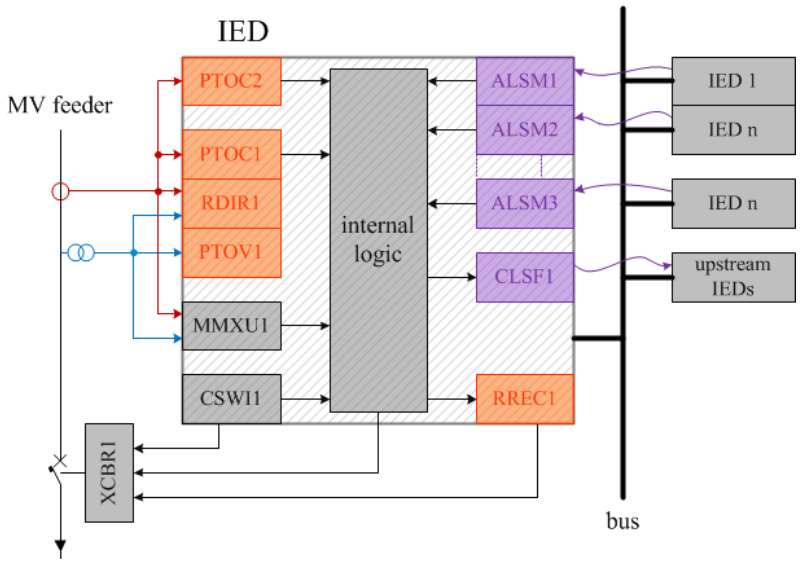

Figura 27: Diagrama de bloques simplificado de un dispositivo de protección y sus interfaces.

La información proporcionada por pares remotos en ALSMx es utilizada por la lógica interna cuando el bloqueo está habilitado para el IED. Por lo tanto, es posible bloquear la apertura de un seccionador o un interruptor comandado por funciones de protección.

En una red eléctrica radial o en bucle abierto, el bloqueo debe habilitarse solo para IEDs del mismo tipo ubicados aguas arriba. En caso de que haya una reconfiguración en la red que cause un flujo de potencia inverso, el esquema de bloqueo debe adaptarse a la nueva configuración para tener en cuenta los IEDs que se encuentran aguas abajo. Además, las configuraciones relacionadas con las funciones de protección, como el ángulo de referencia para la protección direccional o el umbral actual, pueden necesitar ser adaptadas a la nueva situación.

4.3 Implementación del Sistema de Protección Adaptativa

La presente sección describe el enfoque general de Selectividad Lógica y la Reconfiguración del Sistema de Protección, centrado especialmente en la implementación técnica de la solución desarrollada como parte del proyecto IDE4L.

A) FLISR

El nuevo enfoque propuesto para el aislamiento de faltas y la restauración del servicio se basa, por un lado, en la presencia de interruptores en algunas Subestaciones Secundarias y, por otro lado, en la distribución de las lógicas de control y monitorización a través de toda la red de Media Tensión. De hecho, esta solución de FLISR requiere que diferentes IEDs de protección instalados en ciertos puntos de un feeder de Media Tensión cooperen entre ellos y se coordinen con un IED situado en la Subestación Primaria. En particular, aprovechando GOOSE, cada IED instalado en el feeder puede comunicarse con los demás a través del modelo de publicación/ suscripción. Esta comunicación rápida se usa para intercambiar los eventos que se producen al detectar una falta con el fin de definir cuál de los IEDs es el más cercano a la falta.

Las fases de detección y aislamiento de la falta correspondientes al algoritmo FLISR se basan en el concepto de que cada IED se suscribe a los IED del mismo feeder instalados aguas abajo, que en este caso son sus publicadores. Cuando ocurre una falta en un punto del feeder, los dispositivos que lo detectan envían un mensaje GOOSE a sus suscriptores, de modo que el único que envía un GOOSE sin recibir al menos un mensaje de sus editores es el más cercano a la falta. Este IED es el único que dispara su interruptor para aislar la falta con el menor número de clientes involucrados [118].

Por otro lado, cuando se aísla la falta ocurrida, comienza la fase de restauración del suministro. Para dicho propósito, en el proyecto IDE4L [83] se utilizó la “Unidad de Automatización de Subestación” (SAU, Substation Automation Unit) [119]. El SAU supervisa la red de Media Tensión donde se realiza la Selectividad Lógica y actúa como suscriptor de cada uno de los IEDs instalados en sus feeders conectados a la Subestación Primaria, de modo que cada vez que se detecte y aísle una falta, conozca dónde está la falta y qué interruptor se ha abierto para despejarla. Su principal misión

es actualizar el sistema de protección durante el aislamiento de la falta, teniendo en cuenta la topología de la red. Además, en el proyecto IDE4L [83], esta Unidad se usa para monitorizar y controlar la red de dicha Subestación, a través de un conjunto de algoritmos (estimación / pronóstico de estado y flujo de potencia óptimo). Mediante dichos algoritmos de optimización se puede definir la mejor reconfiguración posible de la red considerando tanto la presencia de faltas como las restricciones de la red.

La aplicación de la secuencia para la reconfiguración de la red es administrada por la Unidad de Automatización de la Subestación coordinada con el centro de control. Esta coordinación es necesaria porque, en la actualidad, no todas las Subestaciones Secundarias están controladas de forma remota, por lo que algunas operaciones de reconfiguración necesitan la intervención humana que debe ser supervisada por los operadores del centro de control.

A continuación se ilustra la arquitectura básica tal como se ha descrito:

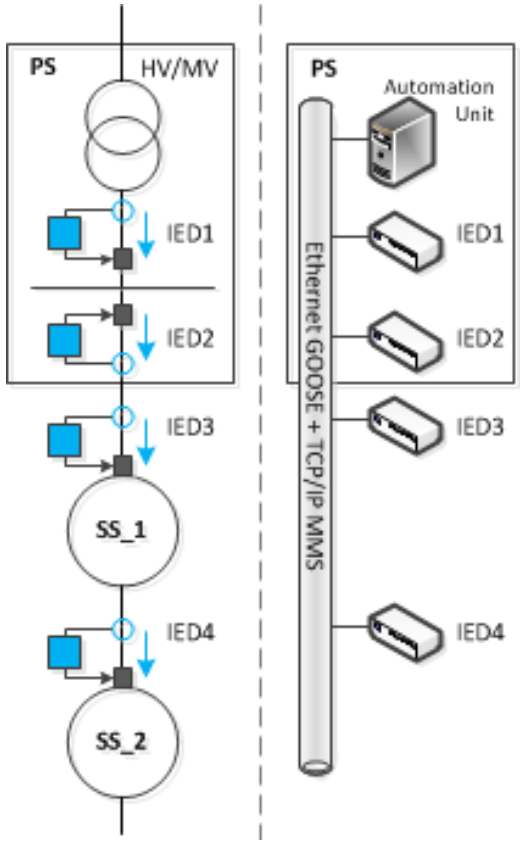

Figura 28: Arquitectura básica para el FLISR: a la izquierda se representan la perspectiva de la red eléctrica con cuatro IEDs y dos Subestaciones Secundarias (SS_1 y SS_2), a la derecha, se representa la red de comunicaciones TCP/IP con los cuatro IEDs y la Unidad de Automatización de Subestación.

Cada Unidad de Automatización de Subestación puede comunicarse con el nivel superior intercambiando comandos y medidas, y recopilar datos de los IEDs instalados en su área de control, almacenando medidas y alarmas en una base de datos local. La comunicación con los IEDs se realiza utilizando el protocolo MMS de IEC61850.

Los datos almacenados en la base de datos local son utilizados por algoritmos que realizan funciones de control y estimaciones. De esta forma se definen nuevos ajustes para los IEDs y para la Unidad de Automatización de Subestación. La interfaz utilizada para adquirir medidas y alarmas también se utiliza para enviar comandos y ajustes a los dispositivos. Dentro de la Unidad de Automatización de Subestación, se encuentra embebido un módulo específico para definir los nuevos umbrales de los dispositivos de protección, a fin de obtener una configuración del sistema de protección compatible con las condiciones vigentes y la configuración de la red de distribución de Media Tensión.

A continuación se ilustran la arquitectura de la Unidad de Automatización de Subestación con sus componentes:

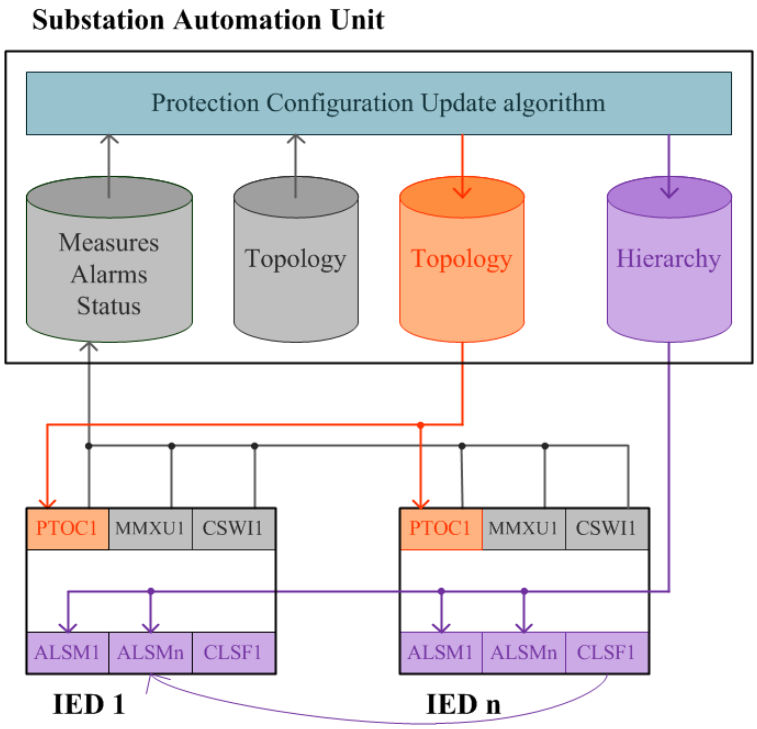

Figura 29: Arquitectura de la configuración del sistema de protección.

B) Selectividad Lógica

La aplicación de Selectividad Lógica es la base para llevar a cabo la solución adaptativa propuesta, implementando la coordinación entre los diferentes IEDs de acuerdo con el siguiente principio. Cuando ocurre una falta en una parte de la red, el IED más cercano aísla dicha zona para reducir el número de clientes afectados por la falta tanto como sea posible. Este IED envía un mensaje de bloque a aquellos IEDs situados aguas arriba a modo de indicación de que la falta ha sido aislada y por tanto el problema ya está resuelto.

En el ejemplo que se presenta en la siguiente figura, ocurre una falta aguas abajo del IED3 y se usa una función de protección direccional para identificar la presencia de la mencionada falta.

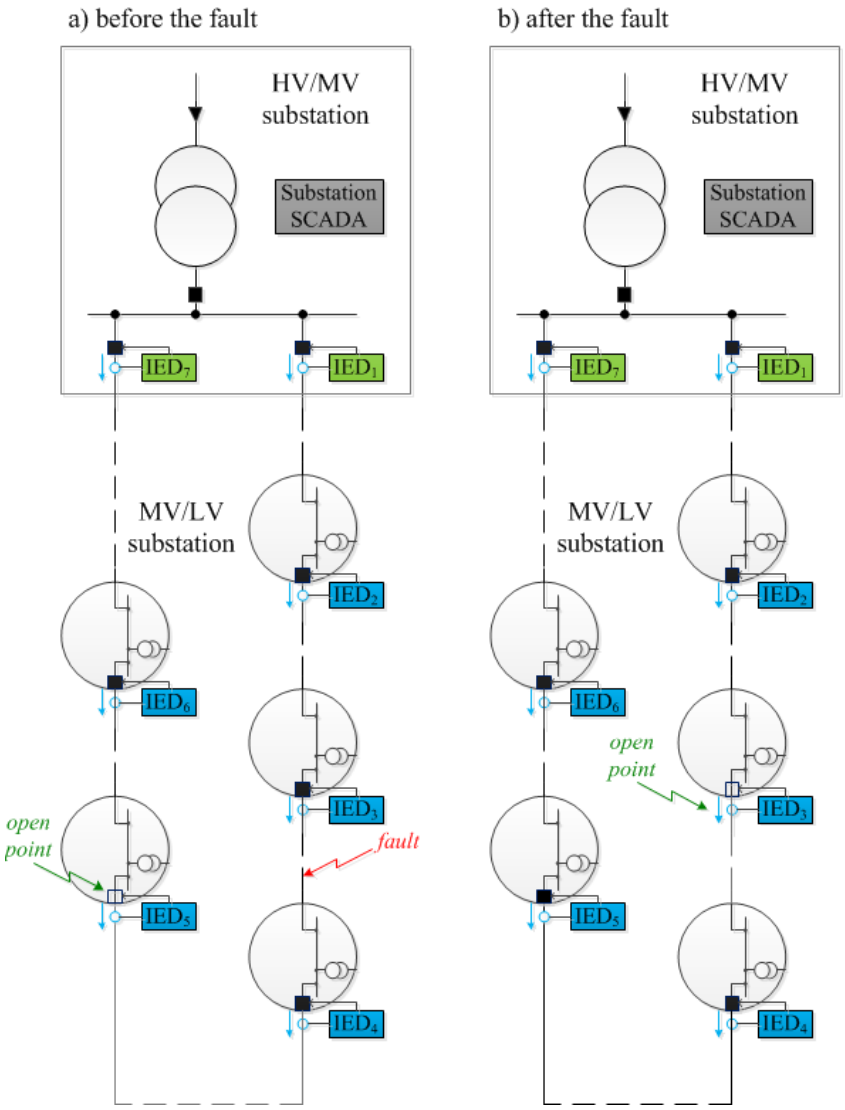

Figura 30: Esquema simplificado de una Subestación primaria con dos feeders de Media Tensión equipados con IEDs e interruptores: a) antes de la falta, está abierta la red entre el IED5 y el IED4; b) después del aislamiento de la falta y la restauración del servicio, el punto abierto se encuentra entre el IED3 y el IED 4.

De esta forma, se produce la siguiente secuencia:

- IED1, IED2 e IED3 detectan la falta y publican un mensaje de bloqueo en el bus de comunicación utilizando el protocolo GOOSE, esperando los mensajes de otros IEDs.
- IED4 no detecta ningún error porque la corriente de falta se produce en una dirección opuesta a la configurada para el IED4.
- El IED5 no detecta ninguna falta o corriente porque el interruptor está abierto y la Subestación Secundaria está desconectada. IED5 solo detecta una caída de tensión causada por la falta.
- IED6 e IED7 no detectan la falta ya que la red de Media Tensión está abierta en la Subestación Secundaria donde está instalado el IED5.

- Algunos IEDs, de acuerdo con los mensajes de bloqueo que se han publicado y la configuración de la siguiente tabla se suscriben al mensaje:

	IED1	IED2	IED3	IED4	IED5	IED6	IED7
IED1							
IED2	X						
IED3	X	X					
IED4	X	X	X				
IED5	X	X	X	X			
IED6							X
IED7							

Tabla 4: Mapeo de publicación / suscripción.

  - IED1 está configurado para suscribirse al bloqueo de mensajes de IED2 e IED3;
  - IED2 está configurado para suscribirse al mensaje de bloqueo de IED3,
  - IED3 está configurado para no suscribir ningún mensaje de bloqueo, dado que IED3 no suscribe ningún mensaje de bloqueo, dispara su interruptor para extinguir la falta.

En el caso de que existan indicadores de paso de falta en algunas Subestaciones Secundarias, se podría introducir un segundo paso para reducir aún más el área afectada por una falta.

C) Reconfiguración del Sistema de Protección

Con respecto a la Reconfiguración del Sistema de Protección, dicho sistema debe reconfigurarse de forma que esté preparado para operar en el caso de que se produzca una nueva falta, incluso, si la red no se encuentra en una configuración estándar. La versión actual del estándar IEC61850 no admite actualizaciones remotas de la configuración. Cualquier cambio debe realizarse cargando un nuevo archivo CID en cada IED. En el caso del ejemplo aquí presentado, este proceso implica editar siete archivos CID y detener el funcionamiento del FLISR para cargar cada archivo en los IEDs correspondientes.

La solución propuesta permite, por tanto, el intercambio de mensajes MMS con IEDs para asignar los nuevos valores a las configuraciones operativas que los necesiten como consecuencia de las reconfiguraciones de la red. Además, el nuevo esquema de comunicación, basado en GOOSE, no solo requiere cambiar los valores de configuración, sino que requiere cambios adicionales y más complejos en los archivos

CID. El haber añadido una configuración para habilitar o deshabilitar los mensajes de bloqueo de los pares IEDs, hace que no se requiera la edición de la suscripción GOOSE en los archivos CID. Así pues, el Nodo Lógico de Selectividad Lógica ha sido propuesto, incluyendo esta nueva configuración, para realizar remotamente los cambios del esquema de comunicación GOOSE sin interrupción del funcionamiento del FLISR. Estos Nodos Lógicos no están incluidos en la versión actual del estándar.

Para determinar la nueva configuración, se necesitan conocer principalmente dos datos:

- La topología de red, por ejemplo, en términos de cableado, transformadores, cargas, generación, etc., necesario para calcular la configuración de protección.
- La configuración de red, por ejemplo, la jerarquía entre la Subestación Primaria y las Subestaciones Secundarias. De acuerdo con esta jerarquía, la suscripción de mensajes GOOSE debe habilitarse / deshabilitarse para los distintos IEDs. Por ejemplo, el mapeo publicación/suscripción que se muestra en la tabla anterior, después de la reconfiguración de la red, debe actualizarse como se presenta en la siguiente tabla.

	IED1	IED2	IED3	IED4	IED5	IED6	IED7
IED1							
IED2	X						
IED3				X	X	X	X
IED4					X	X	X
IED5						X	X
IED6							X
IED7							

Tabla 5: Mapeo de publicación / suscripción después de la falta.

Los mapeos de publicación / suscripción que se muestran en las dos tablas anteriores están definidos de acuerdo con la ubicación del punto abierto y el flujo de potencia que llega a cada IED en condiciones normales.

D) Seguridad

El Protocolo estático de tunelización de capa 2 versión 3 (L2TPv3, Layer 2 Tunneling Protocol versión 3) [120], permite la integración de segmentos Ethernet sobre red IP enrutada. De esta forma, los segmentos LAN de automatización se pueden combinar en una sola LAN lógica. Por lo tanto, los mensajes GOOSE que están basados en la

comunicación de tipo Ethernet multicast se pueden extender a IEDs que se encuentran distantes entre ellos.

En caso de Selectividad Lógica, la tunelización de capa 2 permite conectar las Subestaciones entre sí, utilizando la infraestructura de red existente e incluso Internet. El protocolo de tunelización de capa 2 en sí mismo es una solución de red privada virtual (VPN: Virtual Private Network) sin cifrado y sin una fuerte autenticación, por ello se propone utilizar el protocolo IPsec [46] para mejorar estos aspectos, que como se ha comentado en el apartado 3.2, son dos de sus principales características.

Con objeto de demostrar la viabilidad de la propuesta del envío de GOOSE utilizando el protocolo de tunelización de capa 2 versión 3 sobre IPsec, se hace uso de un router Cisco 892 [121] y un Módem 4G/LTE Cisco 819 [122] que ofrecen la funcionalidad de tunelización IPsec, de forma que se manden los correspondientes mensajes GOOSE entre IEDs por esa vía, como se propone en [123].

Por otro lado, cabe notar que la utilización del protocolo de tunelización de capa 2 tendrá una influencia negativa en la calidad de las comunicaciones debido a los siguientes factores:

- El túnel requiere encabezados adicionales afectando a la cantidad máxima de carga útil (payload) y el tráfico de datos.
- Redes y routers causan retrasos indeterminados.
- La fiabilidad se disminuye especialmente en redes móviles.

Además, el protocolo de tunelización de capa 2 usa la transmisión basada en UDP/IP de información de túnel, lo que puede introducir problemas típicos de UDP, es decir, la pérdida de paquetes. Si además se utiliza IPsec, se introduce el correspondiente procesamiento y los encabezamientos adicionales, lo cual debe tener un mínimo impacto, ya que la mayoría de los equipos tienen hardware dedicado para procesamiento de cifrado y, por tanto, el costo en términos de rendimiento adicional debe ser insignificante.

4.4 Resultados

El FLISR y la reconfiguración del sistema de protección descritos anteriormente se han aplicado a un entorno operativo real en Brescia (en el norte de Italia). La red de Media Tensión, que se muestra en la figura siguiente, está compuesta por: una Subestación Media Tensión/Media Tensión, 3 líneas de Media Tensión, 40 Subestaciones Media Tensión/Baja Tensión y 9 clientes de Media Tensión.

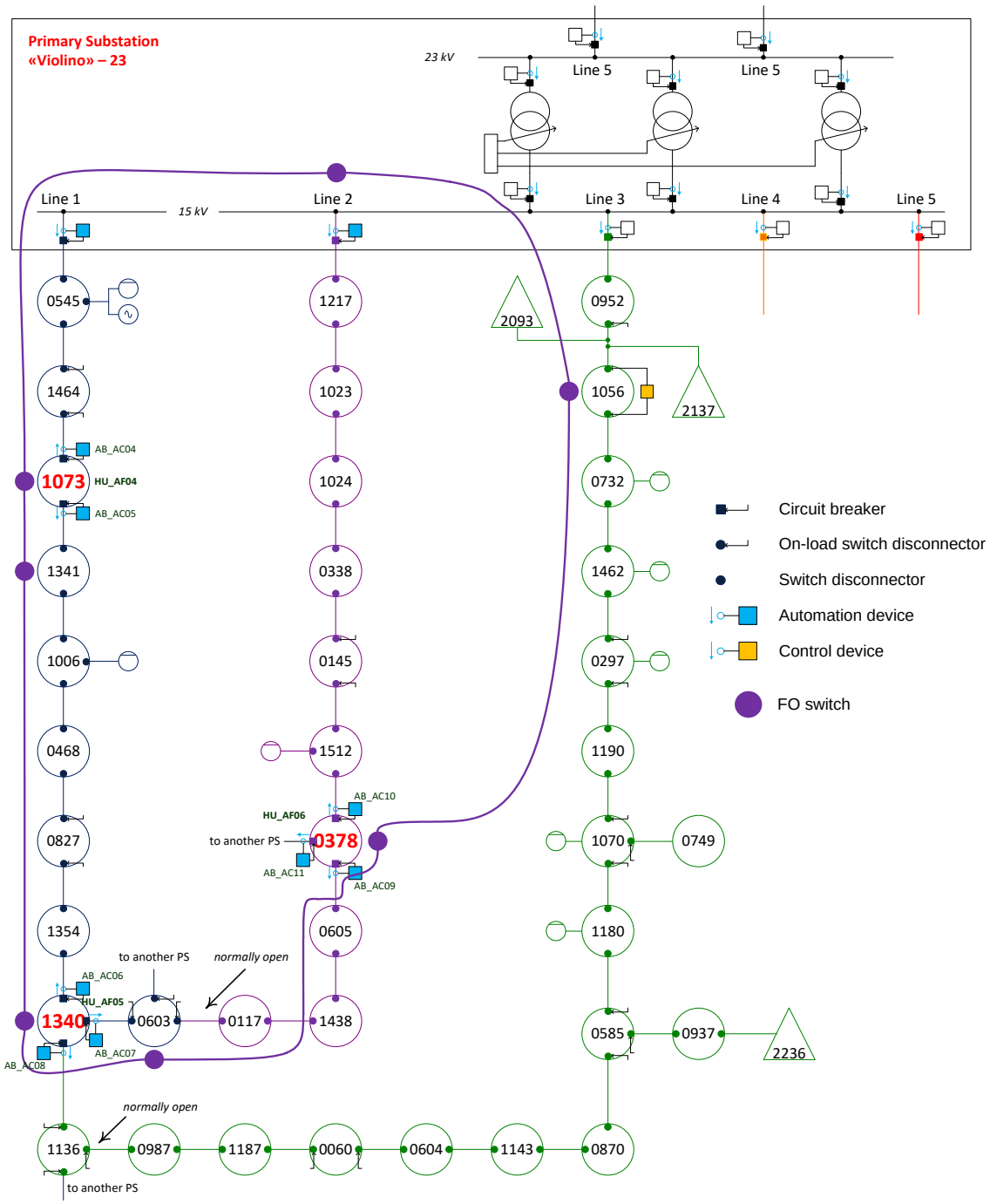

Figura 31: Entorno de pruebas de la red de Distribución en Brescia, Italia.

Las tres líneas forman dos anillos gestionados radialmente. Dos líneas de Media Tensión estarán completamente automatizadas con sistemas de monitorización, control, protección y simulación, mientras que la tercera línea estará dedicada principalmente a simulación y a la prueba de campo en Baja Tensión.

Como se ha expuesto anteriormente en el apartado 4.3, hay dos protocolos que se usan para Selectividad Lógica y la reconfiguración adaptativa del sistema de protección. El primero se basa en un intercambio de mensajes GOOSE y el segundo usa el MMS.

Con referencia a la pila de protocolos OSI, como se ha comentado en el “Capítulo 3 Estado del Arte”, GOOSE es un protocolo de capa 2. Los protocolos capa 2 se usan normalmente en redes de área local como las que se presentan dentro de una Subestación Primaria, que presentan un número limitado de nodos (no más de unos cientos, en el peor de los casos) y un área geográfica bien delimitada. Un nodo conectado a la red envía/recibe mensajes a/desde todos los demás nodos conectados en la misma red, lo que viene a ser una aproximación publicador/suscriptor.

Del mismo modo, MMS es un protocolo de aplicación basado en TCP/IP. En una red IP, denominada capa 3, cada nodo tiene una dirección IP, en caso de que la red se divida en varias subredes, los routers se encargan de recibir los paquetes de la subred y redirigirlos a los demás. Este tipo de redes son la opción más adecuada cuando el número de nodos es elevado, que es precisamente el caso de los Sistemas de Automatización, donde los IEDs están distribuidos geográficamente en un área de la ciudad que cubre varias Subestaciones Secundarias que, dicho sea de paso, son dos órdenes de magnitud más numerosas que las Subestaciones Primarias.

Para realizar la automatización de Media Tensión descrita en este capítulo se usa un enfoque mixto de capa 2/3 utilizando tanto MMS como GOOSE:

- Cada Subestación Secundaria se conecta mediante el uso de diversas tecnologías, como la fibra óptica, la línea de banda ancha sobre cables de Media Tensión y Wi-Fi (esta red es una extensión de la implementada para el Proyecto Europeo FP7 INTEGRIS) [124].
- Cada Subestación Secundaria ha sido equipada con un dispositivo switch/router configurado de tal manera que, por un lado, GOOSE pueda viajar a través de la red de comunicación como si viajara en una LAN y por otro lado, que el MMS viaje a través de las subredes de las Subestaciones Secundaria/Primaria.

En lo que respecta a la seguridad, gracias al envío de GOOSE utilizando el protocolo de tunelización de capa 2 versión 3 sobre IPsec, la integridad, confidencialidad y autenticación son aspectos garantizados para las mencionadas comunicaciones GOOSE.

4.4.1 Métricas

Con el objetivo de mostrar la efectividad del enfoque propuesto se definen las correspondientes métricas. Para ello, se compara un escenario de demostración en el que se despliegan los dispositivos que implementan el sistema de protección adaptativa, FLISR con Selectividad Lógica, frente al mismo escenario de demostración sin ningún elemento adicional, el cual es considerado como la referencia.

Las métricas consideradas serán los dos siguientes índices creados por el “Institute of Electrical Electronics Engineers” que son los generalmente utilizados para medir el rendimiento y fiabilidad del sistema de transmisión y distribución eléctrica [125], [126]:

- SAIFI (System Average Interruption Frequency Index): es una medida del número total de interrupciones experimentadas por los consumidores por número total de consumidores conectados a la red de distribución.
- SAIDI (System Average Interruption Duration Index): mide la media de tiempo que los consumidores están sin servicio por consumidor conectado a la red.

Nodo	Clientes	REF	FLISR	Localización de falta									SAIFI REF (%)	SAIFI FLISR (%)	SAIFI KPI (%)	SAIDI REF (min)	SAIDI FLISR (min)	SAIDI KPI (%)
PSLN01		x	x															
SS0545	102			x									100	100,0	0,00	86,44	51,7	40,19
SS1464	4				x								100	100,0	0,00	86,44	51,7	40,19
SS1073	22		x			x							100	100,0	0,00	86,44	51,7	40,19
SS1341	1						x						100	51,15	48,85	86,44	26,44	69,41
SS1006	18							x					100	51,15	48,85	86,44	26,44	69,41
SS0468	15								x				100	51,15	48,85	86,44	26,44	69,41
SS0827	39									x			100	51,15	48,85	86,44	26,44	69,41
SS1354	4										x		100	51,15	48,85	86,44	26,44	69,41
SS1340	38		x									x	100	51,15	48,85	86,44	26,44	69,41
SS0603	19											x	100	7,25	92,75	86,44	3,75	95,66
PSLN02		x	x															
SS1217	9			x									100	100,0	0,00	86,44	76,15	11,91
SS1023	187				x								100	100,0	0,00	86,44	76,15	11,91
SS1024	176					x							100	100,0	0,00	86,44	76,15	11,91
SS0338	419						x						100	100,0	0,00	86,44	76,15	11,91
SS0145	354							x					100	100,0	0,00	86,44	76,15	11,91
SS1512	94								x				100	100,0	0,00	86,44	76,15	11,91
SS0378	63		x							x			100	100,0	0,00	86,44	76,15	11,91
SS0605	84										x		100	18,11	81,89	86,44	9,36	89,17
SS1438	70											x	100	18,11	81,89	86,44	9,36	89,17
SS0117	134											x	100	18,11	81,89	86,44	9,36	89,17

Nodo	Clientes	REF	FLISR	Localización de falta	SAIFI REF (%)	SAIFI FLISR (%)	SAIFI KPI (%)	SAIDI REF (min)	SAIDI FLISR (min)	SAIDI KPI (%)
						Promedio	31,58			49,18

Tabla 6: Mejora en los índices SAIFI / SAIDI. Caso de referencia (REF) versus implementación con FLISR y Selectividad Lógica (FLISR).

Es necesario señalar, que estos resultados de la Tabla 6 fueron calculados bajo el supuesto de que la red siempre está en la configuración estándar y que el tiempo medio de las operaciones manuales es igual a 20 minutos.

Como se puede observar en esta tabla, la mejora promedio del indicador SAIFI es del 31,58%, mientras que la mejora promedio del indicador SAIDI es del 49,18%. Dichas mejoras tienen el correspondiente impacto económico, al estar ligadas al coste de las interrupciones que se han ilustrado a lo largo del apartado 4.1.

Además, dependiendo de la regulación vigente en cada país, las variaciones en estos índices pueden afectar directamente a la cuenta de resultados de los Operadores de los Sistemas de Distribución eléctrico, ya sean por penalizaciones ligadas a la interrupción de servicio o ya sea por perdida de incentivos ligados a la continuidad del servicio.

Un ejemplo es el caso de Suecia, en donde operan 170 Operadores de los Sistemas de Distribución, y en donde la regulación sueca, además de incentivos por la continuidad del servicio, establece el límite de ingresos de cada Operador del Sistema [127]. Así pues, en "Analyses of the Current Swedish Revenue Cap Regulation" [127] se demuestra el impacto de SAIDI y SAIFI en dichos límites de ingresos. En la siguiente figura se presenta el impacto que sufre el límite de ingresos (impacto revenue cap), desglosado por distintas categorías, cuando se duplican el SAIDI y el SAIFI [127]. Se puede observar que aunque la categoría comercial e industrial en número de clientes solo representen 6,4% y que en términos de consumo representen menos del 50%, sin embargo, el impacto en el límite de ingresos con un SAIDI y SAIFI duplicado representa el 88,4%.

Category	Number of customers	Energy consumption	Impact on revenue cap
Agriculture	1.2 %	2.6 %	4.2 %
Industry	0.8 %	22.9 %	30.9 %
Commercial	5.6 %	24.5 %	57.5 %
Public service	2.3 %	8.3 %	5.6 %
Household	90.2 %	41.8 %	1.7 %

Figura 32: Impacto del límite de ingresos en los Operadores del Sistema Eléctrico de Suecia ante una duplicación de SAIDI y SAIFI desglosado en las categorías de Agricultura, Industria, Comercial, Servicio Público y Residencial. [Fuente: Analyses of the Current Swedish Revenue Cap Regulation [127]]

El ejemplo de Suecia supone una demostración tangible de como la mejora de SAIDI y SAIFI puede mejorar las cuentas de resultados de los Operador del Sistema eléctrico sueco.

Por otro lado, en términos más globales, en el informe del Worl Bank sobre “Tarifas de electricidad, interrupciones de energía y rendimiento de la empresa” [128], en el que se analizan 142 economías del mundo, se presenta una correlación directa entre SAIDI y la renta nacional per cápita (GNI per capita, Gross National Income per capita) y se afirma que el nivel de ingresos de un país está asociado al desarrollo de las infraestructuras. Para que dicho nivel de ingresos aumente, el desarrollo de las infraestructuras debe estar dirigido a aumentar confiabilidad del servicio, que es precisamente lo que determinan índices como el SAIDI y el SAIFI.

En la siguiente figura se puede observar como aquellos países con un SAIDI muy elevado tienen un bajo GNI per cápita y, al contrario.

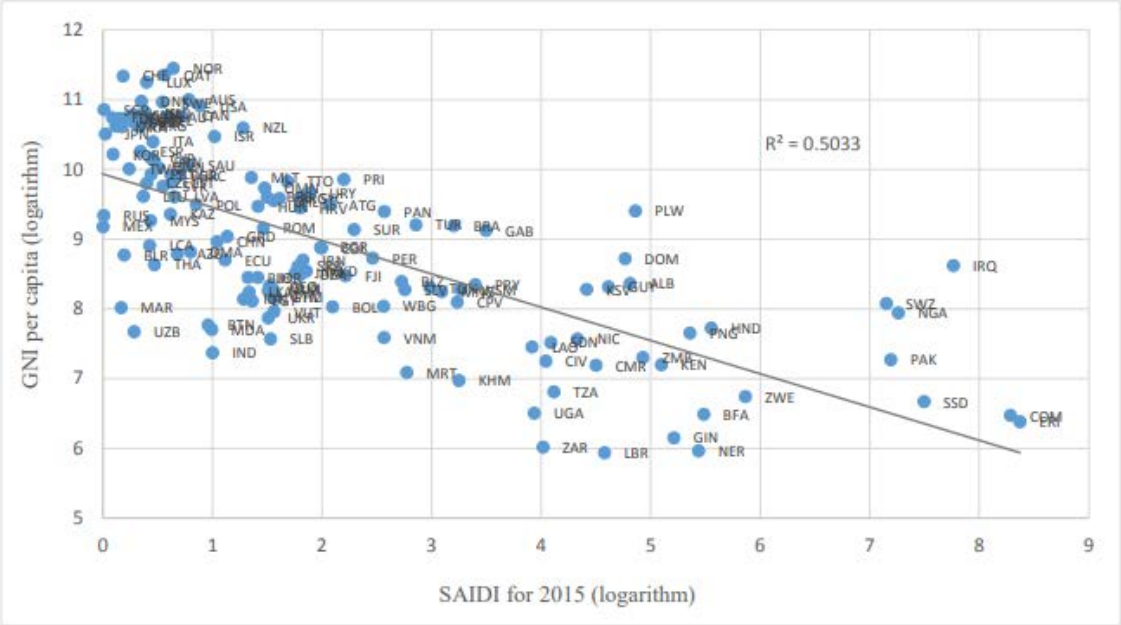

Figura 33: World Development indicators 2015, 142 economies [Fuente: Doing Business database. World Bank [128]]

Así pues, las mejoras en los índices SAIDI y SAIFI tienen su correspondiente huella, no solo en las cuentas de resultados de las eléctricas sino también en las economías de los países, y por tanto en las economías de empresas y ciudadanos.

4.5 Conclusiones

En el presente capítulo se ha presentado y demostrado, en una infraestructura real, una aproximación innovadora respecto al enfoque clásico de automatización y protección. La principal contribución consiste en la reconfiguración dinámica de los dispositivos de

protección utilizados para implementar soluciones avanzadas de localización de faltas, aislamiento y restauración de servicio, utilizando para ello el estándar IEC61850, lo que supone una novedad y confiere al sistema de un importante valor añadido.

Se ha propuesto un posible mapeo de Nodos Lógicos en IEC61850 para funciones de uso común en la red de Media Tensión, se han descrito los requisitos y la configuración de dicha solución, y se han definido y calculado métricas relevantes para demostrar la eficacia de la solución adaptativa.

En este sentido, ante la detección de una falta y la necesaria reconfiguración del sistema, se ha demostrado, que la utilización del sistema de reconfiguración dinámica propuesto mejora sustancialmente los indicadores SAIFI y SAIDI, los cuales son claves para el negocio de los operadores del sistema eléctrico y se traducen en variables económicas que impactan directamente en la cuenta de resultados de las empresas.

Al mismo tiempo, la tendencia creciente de instalar dispositivos electrónicos inteligentes e interruptores a lo largo de la Media Tensión, refuerza la viabilidad del sistema presentado y las posibilidades reales de una implantación futura.

Por último, en lo que respecta a la seguridad, la utilización del protocolo de tunelización de capa 2 versión 3 sobre IPsec garantiza la integridad, confidencialidad y autenticación para las comunicaciones GOOSE, mitigando así una posible barrera a la implantación del sistema debido a las posibles dudas en cuanto a la seguridad del sistema.

Capítulo 5. Nuevas Redes de Sincronismo Redundante de Precisión Basadas en Tecnología White-Rabbit para Subestaciones Confiables

SmartGrid, como se ha indicado en el apartado 3.3, es un sistema complejo e interconectado donde las acciones y eventos en una parte del sistema afectan a las operaciones en otros lugares del mismo. Es por ello, que para poder operar eficientemente la red y realizar análisis rigurosos de la misma se requiere una referencia de tiempo común y determinista en los distintos sistemas que la componen y en particular en los sistemas embebidos.

En este capítulo se estudia dicha necesidad, utilizando para ello el Sistema de Automatización de Subestación como caso de uso, que como se ha comentado en el apartado 3.4 son un elemento crítico en el concepto de SmartGrid. Además, en los Sistemas de Automatización de Subestación los sistemas embebidos juegan un papel fundamental, siendo la RTU una pieza clave. Cabe señalar, que en dichos sistemas históricamente las compañías eléctricas han optado por un reloj satélite que proporciona una señal de temporización y diferentes formas de distribuirlo a través de la Subestación. En este capítulo se propone una solución de redes de sincronismo precisas para aplicaciones confiables en SmartGrid en la Subestación, presentándose los detalles de la implementación, el análisis de la confiabilidad del sistema y de la seguridad, junto con prometedores resultados y novedosos mecanismos para proporcionar el tiempo en la red.

El capítulo está organizado de la siguiente manera, una vez introducido el problema, se describe el caso de uso, a continuación se presentan los detalles de implementación, y por último se muestran los resultados, así como el análisis de la precisión, confiabilidad, escalabilidad y seguridad del sistema. Finalmente, se presenta la discusión y las conclusiones de estos resultados.

La investigación descrita en el presente capítulo se realizó en el marco del proyecto europeo EMC2 [129].

5.1 Introducción

Como se ha mencionado en el apartado 2.1.1, la transformación que trae consigo SmartGrid está convirtiendo lo que hasta ahora era la clásica red eléctrica centralizada, en una red inteligente e interactiva, cambiando a su vez la cadena de valor de la energía. SmartGrid es una infraestructura compleja, que como se indicaba en el apartado 2.3, está compuesta por un importante número de sistemas y dispositivos electrónicos de diferente naturaleza, desde los Sistemas Empresariales de Planificación, pasando por los Sistemas de Gestión de la Distribución y los SCADA hasta los dispositivos inteligentes como RTUs, para finalizar en sensores y actuadores. La complejidad de SmartGrid aumenta continuamente debido a la incorporación de nuevos actores como los recursos de energía

distribuida, típicamente en forma de paneles fotovoltaicos y aerogeneradores, el vehículo eléctrico [84], microredes y el concepto de prosumer (productor y consumidor de energía) [130]. Además, debido a la naturaleza crítica de estas infraestructuras, al proporcionar servicios esenciales como energía eléctrica, la red inteligente debe ser segura y confiable [131], [132], [133].

Los Sistemas de Automatización de Subestación tales como SCADA, Unidad Terminal Remota y Dispositivo Electrónico Inteligente se consideran componentes clave de la red eléctrica a nivel de transmisión y distribución. La Automatización de Subestaciones es una tarea considerada de misión crítica y, además, dichos sistemas funcionan en condiciones de tiempo real. Igualmente, los Sistemas de Automatización de Subestaciones proporcionan una base sólida para futuros desarrollos de SmartGrid en las instalaciones eléctricas [134].

Debido a la naturaleza distribuida de los diferentes dispositivos de SmartGrid, la utilización adecuada de una infraestructura de red es fundamental para proporcionar un medio de comunicación seguro y confiable para los diferentes sistemas, dispositivos, actuadores y sensores.

Por un lado, los datos permiten conocer correctamente el estado de la red eléctrica, lo que a su vez permite el control y la optimización de los diferentes parámetros de operación, con objeto de conseguir una distribución y uso de recursos eficiente.

Por otro lado, es fundamental garantizar la presencia de elementos y funciones de protección para evitar la destrucción de equipos e instalaciones debido a fallos o faltas y garantizar la seguridad de las personas. Para ello, se utilizan entre otros elementos interruptores y seccionadores que permiten aislar el fallo, minimizar la zona afectada y restaurar el servicio, tal como se ha estudiado en el apartado 3.3 y a todo lo largo del Capítulo 4.

Al mismo tiempo, es primordial dotar al sistema de una referencia de tiempo global que permita realizar un análisis forense de la red, después de haber sufrido algún tipo de fallo, lo cual requiere un mecanismo de sincronización de red para trabajar en áreas extensas de una manera determinista. Estas características requieren una infraestructura de red confiable que incluya equipos fiables, topologías de red redundantes con recuperación a tiempo cero, referencias de tiempo confiables y comunicaciones seguras que puedan garantizar el funcionamiento correcto de la red.

La distribución del tiempo exacto es esencial para asegurar un correcto sistema de control y protección automático de SmartGrid, el cual, en último término, permite el uso óptimo de los recursos de la red eléctrica. El tiempo se convierte en un parámetro crucial para garantizar el correcto funcionamiento de la Subestación, de igual importancia que el propio marcado de tiempo, las funciones de protección y el análisis forense que se realiza después de una falta. En la presente tesis, se ha utilizado un nuevo protocolo de transferencia de tiempo basado en Ethernet conocido como White-Rabbit (WR) [135], [136], [137]. White-Rabbit se ha propuesto como un nuevo perfil de alta precisión para el estándar IEEE 1588 y permite la sincronización totalmente determinística de subnanosegundos [138]. Toda la información relativa a este proyecto White-Rabbit puede ser consultada en el repositorio de hardware abierto del CERN [139].

Con relación a la confiabilidad de la red, es importante destacar que el protocolo de redundancia HSR (High-availability Seamless Redundancy) y el PRP (Parallel Redundancy Protocol), redactados en el estándar IEC62439-3 [140], han sido adoptados para la Automatización de Subestaciones en el marco del estándar descrito anteriormente en el apartado 3.1 para la automatización de Subestaciones [141], [142], [143].

La importancia de los protocolos de comunicación de red, así como sus tiempos de recuperación ante una pérdida de enlace, se considera crítica en sistemas como el de Automatización de Subestación dadas sus necesidades a nivel de control y protección. Los protocolos tradicionales, cuando se comunica un fallo en un enlace, actúan recalculando todo el camino. Sin embargo, los algoritmos de recuperación de estos protocolos de red son transparentes a las capas superiores, aunque el tiempo que tardan en recalcular los enlaces repercute en el tiempo de transmisión de un mensaje. Para un evento crítico, incrementar el retardo en milisegundos, puede equipararse en gravedad a la pérdida de información. Los márgenes o la ventana de exposición de un dispositivo, cuando nos encontramos con un sistema de protección deben tender a “cero” o dejarían de ser sistemas de protección [144]. En la siguiente tabla se clasifican los tipos de sistemas por tiempos esperados de respuesta:

Criticidad	**Tiempos esperados de respuesta**	**Tipo de sistema**	**Red**
No críticos	>10s	Corporativo, Negocio	Negocio
Normal	<800ms	SCADA, historian, HMI, Edificios	Supervisión
Alto	<100ms	Control de procesos	Control
Crítico	<10ms -> “cero”	Sistemas de protección, control de robots industriales, Subestaciones	Control de actuadores críticos

Tabla 7: Relación entre tipo de sistema, criticidad y tiempos aceptables de recepción de mensajes. [Fuente: PRP y HSR: Protocolos redundantes INCIBE [144]]

Parallel Redundancy Protocol es un protocolo diseñado para asegurar alta disponibilidad y reducir el tiempo de recuperación de red. Se basa en la utilización de dos redes LAN independientes (LAN A y LAN B, ver en la siguiente figura) a través de las cuales se envía el mismo mensaje. Dicho mensaje es enviado por dos puertos diferentes, pero con la misma dirección MAC (Media Access Control) e IP (Internet Protocol).

Los nodos del Parallel Redundancy Protocol, denominados DANs (Double Attached Nodes), son responsables del envío en paralelo de las tramas por ambas redes. Dichos nodos, actúan a su vez en el destino, donde tomando el rol de nodos receptores aceptarán la primera de las dos tramas en llegar y descartarán la segunda. En la siguiente figura se ilustran las redes y las distintas conexiones con los nodos.

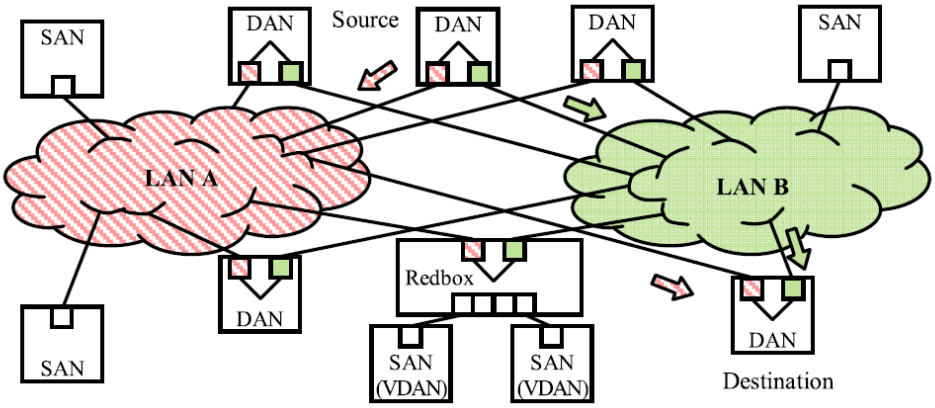

Figura 34: Representación de la red Parallel Redundancy Protocol, incluyendo dos redes LAN independientes (LAN A y LAN B). [Fuente: PRP and HSR for high availability networks in power utility automation: A method for redundant frames discarding [145]]

High-availability Seamless Redundancy es igualmente un protocolo diseñado para asegurar la alta disponibilidad y reducir el tiempo de recuperación de red. HSR opera de forma similar al anteriormente descrito PRP, pero usa una sola LAN. La topología básica utilizada, en este caso, es una red en anillo, en donde los DANs del HSR envían tramas HSR idénticas por los dos puertos del dispositivo en sentidos opuestos, como se muestra en la siguiente figura.

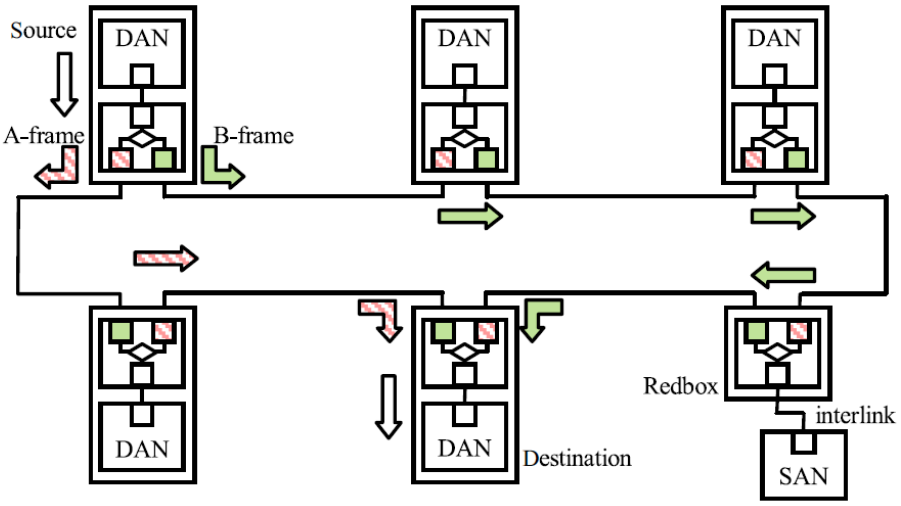

Figura 35: Representación de la red High-availability Seamless Redundancy, incluyendo el flujo de las tramas (A y B). [Fuente: PRP and HSR for high availability networks in power utility automation: A method for redundant frames discarding [145]]

Por tanto, HSR y PRP son protocolos de redundancia que proporcionan una alta disponibilidad de información de temporización y protección que son esenciales para este tipo de sistemas críticos que han sido recientemente adoptados por las compañías eléctricas [145].

Además, otro de los aspectos a tener en cuenta, es la seguridad en sus dos acepciones mencionadas en el apartado 3.2. Así pues, como se comentó en dicho apartado se considera el estándar IEC61508 “Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad" [41] para cubrir los aspectos relacionados con el nivel de integridad de seguridad del sistema y el estándar IEEE1686-2013 "Estándar para capacidades de ciberseguridad de los dispositivos electrónicos inteligentes" [45] para cubrir los aspectos de ciberseguridad, los cuales se aplicarán más adelante en el presente capítulo.

Así, la combinación de los Sistemas de Automatización de Subestaciones, junto con los requisitos de tiempo, interoperabilidad, disponibilidad y seguridad, pone de manifiesto la necesidad de contar con un caso de uso adecuado que sirva como punto de partida del presente capítulo que, como el conjunto de la tesis, se centra en los dispositivos embebidos en SmartGrid. A este respecto, como se describe en el siguiente apartado, se implementó una red redundante con distintos dispositivos de entradas y salidas que representan sensores y actuadores en el escenario de la Subestación eléctrica como caso de uso.

Por otro lado, para analizar globalmente las características de confiabilidad requeridas, se utilizó una herramienta específica destinada a evaluar características clave de los dispositivos embebidos del caso de uso de la Subestación, como son: la seguridad, la capacidad de certificación basadas en el estándar IEC61508 (teniendo como objetivo el nivel de SIL) y la confiabilidad respecto a los fallos. Para ello, se usa el Análisis de Diagnósticos, Efectos y Modos de Fallo (FMEDA) [146] que valora la solución propuesta, obteniéndose de esta forma una solución altamente confiable para los elementos de los casos de uso de la Subestación en el dominio SmartGrid.

Esta investigación se realizó en el marco del proyecto europeo colaborativo EMC2 (Embedded Multi-Core systems for Mixed Criticality applications in dynamic and changeable real-time environments) que es un proyecto de la ARTEMIS Joint Undertaking en el Programa piloto de innovación 'Plataformas computacionales para sistemas embebidos” [129].

5.2 Caso de Uso de la Subestación

En el concepto de SmartGrid, la Subestación es uno de los elementos claves. Como se puede apreciar en la Figura 36, el sistema eléctrico está dividido en generación, transporte y distribución, existiendo distintos tipos de Subestaciones que, en función de su nivel de tensión, pueden ser básicamente de alta, media o baja tensión. Dichas Subestaciones forman la columna vertebral del sistema eléctrico en su conjunto.

Como ya se ha indicado previamente en el apartado 3.4, los principales elementos de la red de distribución eléctrica son los Sistemas de Automatización de la Subestación [147], que controlan la infraestructura eléctrica.

Una Subestación eléctrica es un nodo de interconexión de circuitos, de manera directa o mediante transformación, que conecta redes a distintos niveles de tensión. La función principal de las Subestaciones es conseguir mallar adecuadamente el sistema eléctrico.

De esta manera, se pueden asegurar unos niveles óptimos de calidad, continuidad y seguridad del suministro eléctrico, minimizando pérdidas de transporte y facilitando labores de mantenimiento. Desde el punto de vista de la operación del sistema, se puede definir una Subestación como el conjunto de los elementos que se utilizan para regular los parámetros eléctricos (tensión, frecuencia y flujos de carga, potencias activa y reactiva) [148].

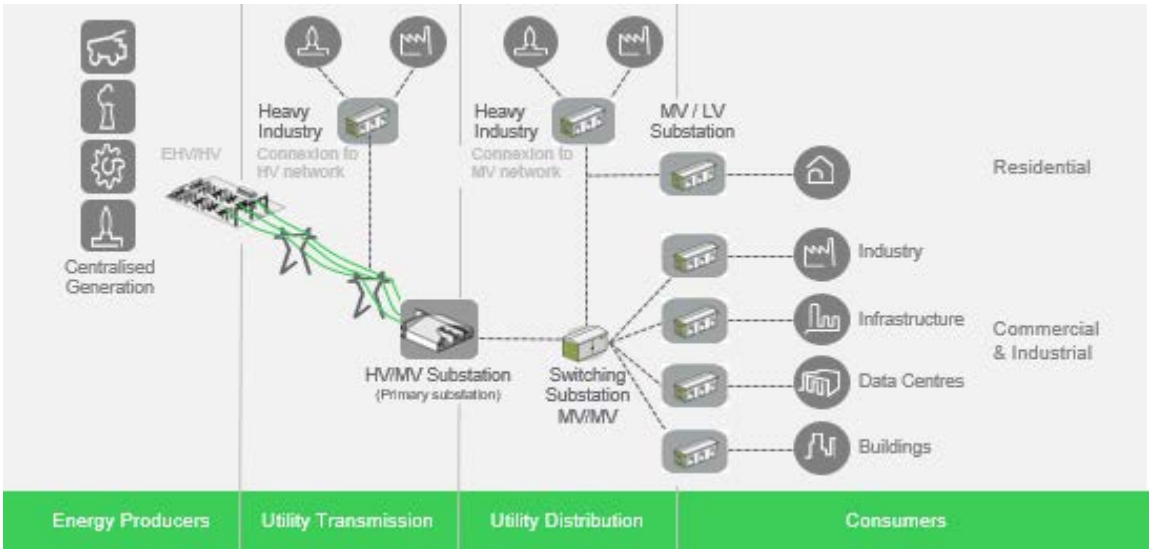

Figura 36: Flujo de electricidad comenzando desde la producción de la electricidad, pasando por los sistemas de transmisión y transporte, siguiendo por los sistemas de distribución, hasta los consumidores en sus distintas modalidades: industria pesada, industria, infraestructuras, centros de datos, edificios comerciales y residenciales [Fuente: Presentación Corporativa, Schneider Electric]

Un SCADA, típicamente situado en un centro de control, se comunica con la Subestación y la gestiona remotamente, recibiendo datos y enviando ordenes de actuación. El sistema de control de una Subestación eléctrica se compone de los siguientes elementos principales [149]:

- Interfaz Hombre Máquina que, a nivel local, permite visualizar mediante gráficos y/o datos el conjunto del sistema de control. Dicha interfaz puede estar embebida en la RTU.
- Concentrador de datos y comunicaciones (Front-end) que recopila los datos de los elementos de control y comunica con el SCADA o los SCADAs del nivel superior. Este elemento puede ser también una RTU.
- RTU de adquisición, conectada con sensores y actuadores aguas abajo y que aguas arriba comunica con el concentrador/Front-end o eventualmente con el SCADA directamente.
- IED que son los responsables de la protección del sistema.

A continuación se ilustra el sistema descrito [149]:

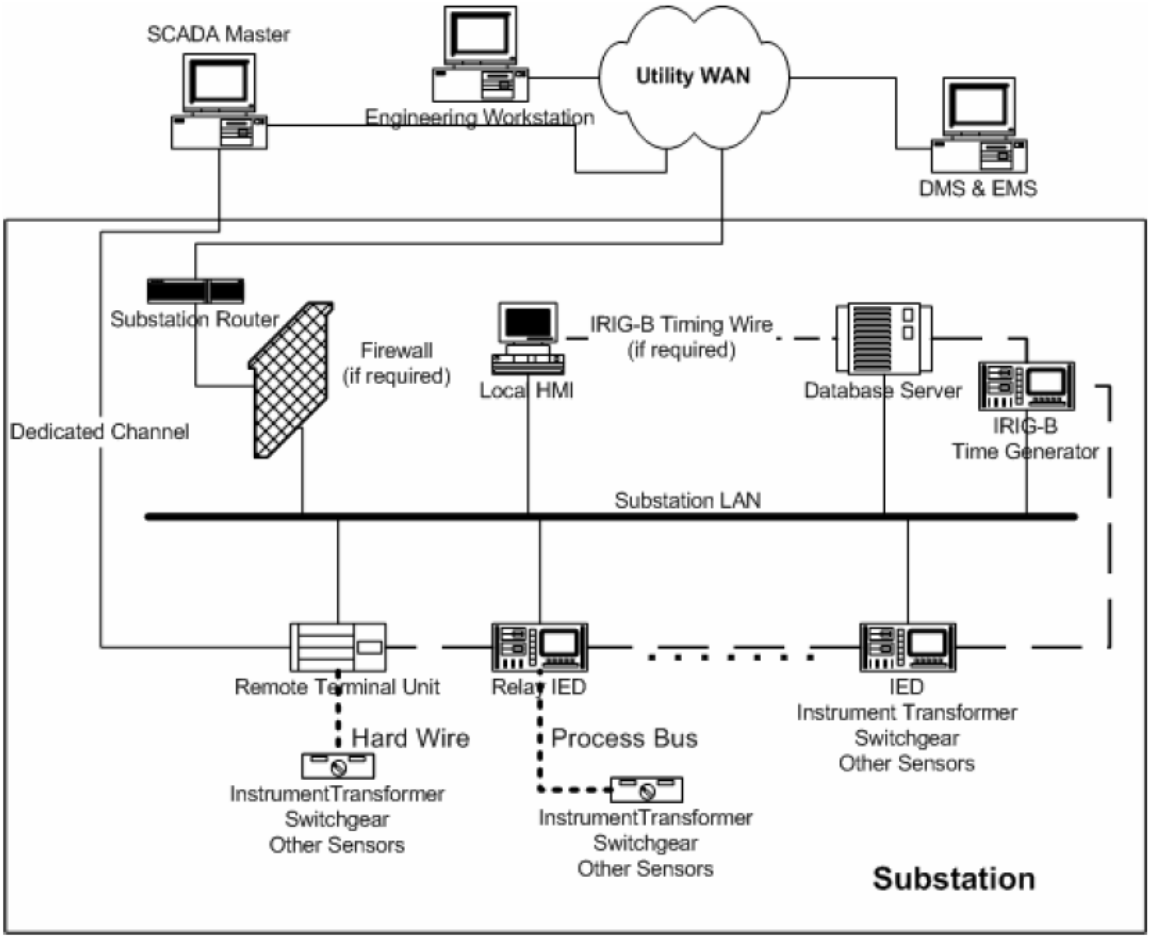

Figura 37: Ejemplo de arquitectura de sistema de automatización de Subestación. [Fuente: IEEE Standard for SCADA and Automation Systems. IEEE Std C37.1-2007]

Como se puede observar, en la Figura 37 los sistemas embebidos predominan en este contexto y además como se ha indicado en el apartado 2.3 están ampliamente representados por la RTU, al poder este elemento actuar como Concentrador o Front-end y unidad de adquisición, además de realizar funciones de protección y dar soporte para la Interfaz Hombre Máquina.

Por todo ello, se plantea la arquitectura basada en tres niveles, que por otro lado es la más común y más representativa en la Subestación eléctrica y que se muestra en la Tabla 8.

El nivel más alto, desde el punto de vista jerárquico, es el Centro de Control. Este incluye el sistema SCADA, que está alojado en las instalaciones de la empresa, y recibe los datos de las Subestaciones eléctricas. Además, controla la infraestructura y envía las correspondientes órdenes o comandos. El sistema SCADA presenta la información en pantallas gráficas donde se representan el sistema que se está controlando y sus alarmas, tendencias e histórico de datos.

En el segundo nivel se encuentra el Concentrador. Está dotado de las tecnologías de comunicaciones y almacenamiento necesarias para recibir y almacenar la información de los niveles de adquisición de campo y el centro de control. Las unidades terminales

remotas de Front-end están equipadas con protocolos industriales (por ejemplo, IEC101, IEC104, DNP3, Modbus, descritos anteriormente en el apartado 2.3.2.1) y comunicaciones Ethernet y Serie. En este nivel se suelen implementar arquitecturas redundantes de comunicaciones, de almacenamiento y procesamiento de datos.

Centro de Control SCADA	 Nivel-3
Subastación – Concentrador Front-end RTU	 Nivel-2
Subastación - Adquisición o campo RTU, Controladores de bahía, Control y Protecciones IED	 Nivel-1

Tabla 8: Sistemas de Automatización de Subestación en 3 niveles: centro de control, nivel de concentrador de Subestación y nivel de campo, ilustrado con dispositivos RTUs de la familia de productos Saitel de Schneider Electric.

El nivel jerárquico inferior, también denominado nivel de adquisición o de campo, tiene como misión recopilar los datos de los sensores y tramitar las órdenes o comandos que deben efectuar los actuadores. Estos dispositivos son activos críticos, equipados con señales de entrada y salida que proporcionan funciones de control, monitorización y recopilación de datos de las Subestaciones.

El caso de uso seleccionado, desarrollado durante el proyecto EMC2 [129], se basó en la arquitectura jerárquica clásica descrita para Sistemas de Automatización de Subestaciones, con el fin de proporcionar un escenario de validación representativo. El caso de uso incluye dispositivos RTU de las familias Saitel DP y Saitel DR de Schneider Electric [150] configurados respectivamente como maestro y esclavo, de forma que una RTU Saitel DP situada en el nivel jerárquico superior actúe como Front-end y una RTU Saitel DR y otra Saitel DP actúen como RTUs de adquisición a nivel de campo en conexión con los sensores y actuadores. Por un lado, el nivel superior envía comandos para ser ejecutados en el nivel de campo y, por otro lado, los datos se envían desde el nivel de campo al Front-end.

Las RTUs de adquisición se componen de dispositivos de control SM_CPU866e y HU_A y dispositivos de adquisición de entrada/salida SM_DO32T, SM_DI32, AB_DI, AB_DO, todos ellos pertenecientes a la familia de productos Saitel de Schneider Electric. Por otra parte, la RTU que actúa de Front-end está compuesta del dispositivo de control SM_CPU866e.

El Front-end incluye un programa de lógica, desarrollada siguiendo el estándar IEC61131-3, que fue descrito en el apartado 2.3.2.2. Dicha lógica envía regularmente comandos a las RTU de adquisición. Desde el nivel de campo, las señales de adquisición son enviadas aguas arriba por protocolos de control industrial tales como IEC 60870-5-104 [151], DNP3 y Modbus. Además, PTPv2 (IEEE 1588-2008) e IRIG-B [152], comentados en el apartado 3.4, se utilizan como fuentes de sincronización para el sistema de control.

En el contexto de los Sistemas de Automatización de la Subestación, en lo que se refiere al tiempo, es necesario disponer de una sincronización precisa entre los distintos elementos que componen el sistema en su conjunto, de forma que responda a las necesidades del sistema de control, del sistema de adquisición y del sistema de reconstrucción de eventos, que es utilizado después de suceder algún tipo de fallo. Para ello es de vital importancia la precisión de las marcas de tiempo en las distintas señales de adquisición.

Al mismo tiempo, la sincronización de tiempo es especialmente importante para los dispositivos denominados PMU o sincrofasores [153], ya mencionados en el apartado 4.1 como parte del sistema de detección de faltas. Dichos dispositivos miden ángulos y fase de las ondas de las redes eléctricas comparándolas en distintos puntos y alertando de una desincronización que concluya con una inestabilidad del sistema, y en último caso, con una interrupción del suministro. Aunque, clásicamente, los PMUs son utilizados en las redes de transmisión, se plantea su posible aplicación en los sistemas de distribución eléctrica [154], siendo considerados como uno de los más importantes dispositivos en el futuro de sistemas de energía eléctrica [155].

Las tecnologías utilizadas para sincronizar los Sistemas de Automatización de Subestación son el sistema de posicionamiento geográfico (GPS: Global Positioning System), IRIG-B y Pulso por Segundo. Por otro lado, para la sincronización a nivel de la red de área local, como se ha mencionado en el apartado 3.4.2, se utilizan el protocolo NTP y el protocolo SNTP (Simple Network Time Protocol), así como el PTP en sus dos versiones, PTPv1 (IEEE1588-2002) y PTPv2 (IEEE 1588-2008) que son, en general, requisitos necesarios para cumplir con el estándar de Bus de proceso IEC61850-9-2 o el de Sincrofasores IEEEC37.118-2005 [49].

Así pues, para analizar correctamente las perturbaciones del sistema, es necesario un marcado de tiempo de los eventos muy preciso. Algunas RTUs tienen la capacidad necesaria para marcar los eventos con una precisión por debajo del milisegundo [156], aunque generalmente, el requisito para el etiquetado de tiempo de los eventos es de un milisegundo de precisión [157], lo cual es crucial para una adecuada reconstrucción y análisis forense de una eventual perturbación en la red eléctrica [158].

En términos de las nuevas necesidades del Sistema de Automatización de Subestación, las mencionadas PMU están demandando precisiones de sincronización de decenas de nanosegundos que están lejos de la precisión del milisegundo que, clásicamente, se requería en el sector eléctrico [159], [160], [161].

En cuanto a la distribución del tiempo, el caso de uso incluye dispositivos White-Rabbit que proporcionan una sincronización determinista por debajo de los nanosegundos. En primer lugar, en el nivel jerárquico superior, se utiliza un Switch White-Rabbit (WRS) [162] configurado como maestro de sincronización (GM: Grand Master) de la red. En segundo lugar, se dispone de otros cinco WRS con tecnología HSR, que junto con el anterior WRS forman una red central en anillo redundante. Dichos WRS pueden suministrar el tiempo usando tanto White-Rabbit como PTPv2.

Además de estos Switches White-Rabbit, una cascada de varios nodos específicos White-Rabbit, los denominados White-Rabbit-LEN (WR-LEN) [163], propagan el tiempo desde el centro de la red hasta su periferia. Los WR-LEN pueden propagar el tiempo usando tanto tecnología White-Rabbit como PTP e IRIG-B. Asimismo, se utilizan como interfaces para los dispositivos RTU de Front-end y adquisición, convirtiendo de White-Rabbit a PTP e IRIG-B de forma que las mencionadas RTUs se sincronicen con el Maestro de Sincronización de la red.

En la Figura 38 se representa la implantación del caso de uso, formado por un Maestro de Sincronización (que es un Switch White-Rabbit) conectado a un anillo HSR de Ethernet (formado por 6 Switches White-Rabbit), que envía de forma redundante el tiempo y las tramas de datos.

El sistema de adquisición se distribuye a lo largo del anillo, lo que asegura la recepción de la referencia de tiempo del maestro, y la comunicación entre nodos (tramas de datos y control), hasta la conexión en cadena de 12 nodos. Las tecnologías usadas son White-Rabbit, PTPv2 e IRIG-B.

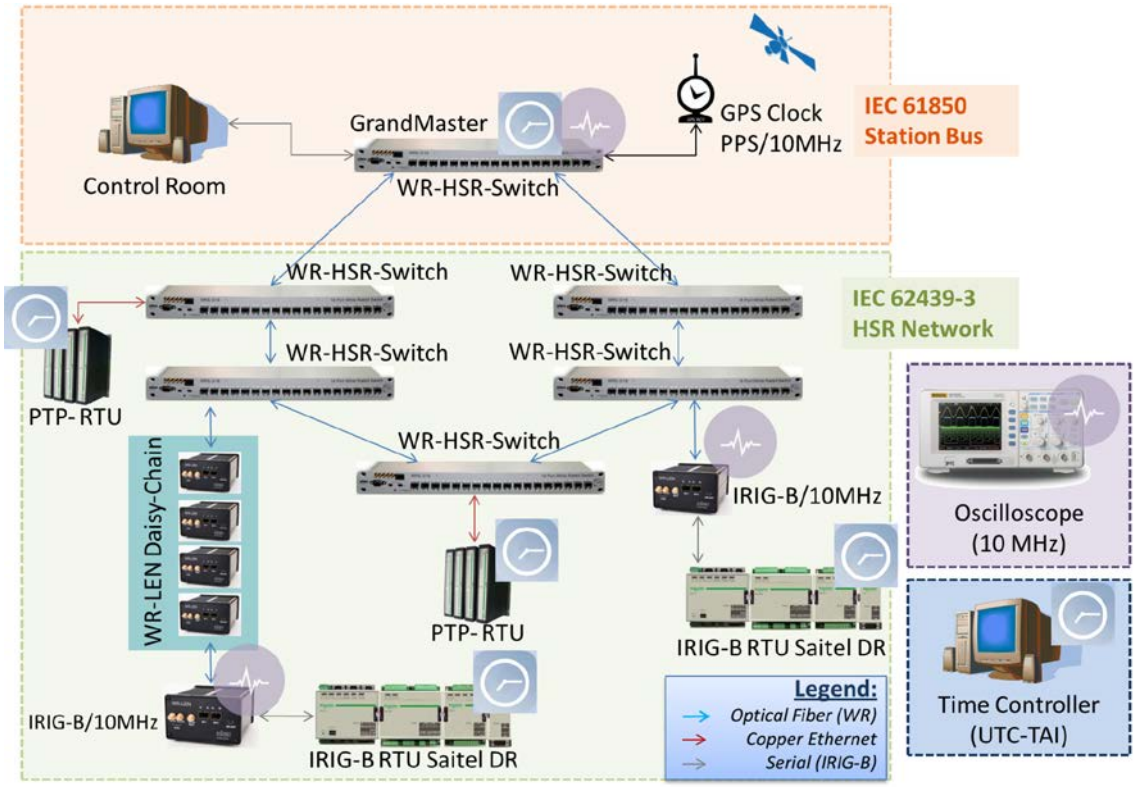

Figura 38: Implementación del caso de uso de Subestación. Incluye un WRS como Maestro de Sincronización, 5 WRS para formar un anillo HSR al que se conecta la RTU que actúa como Front-end, varios WR-LEN en cascada que proveen sincronización mediante IRIG-B a la RTU de adquisición.

Finalmente, como se verá más adelante en el siguiente apartado, para analizar globalmente las características de confiabilidad requeridas y evaluar el nivel de seguridad del sistema, se integró en el caso de uso una herramienta de evaluación específica de seguridad (security y safety), basada en los estándares IEC61508 e IEEE1686-2013 descritos anteriormente en el apartado 3.2.

El caso de uso propuesto valida los requisitos para futuras aplicaciones en el dominio de la Subestación eléctrica, tanto de redes industriales como de Internet de las Cosas (ámbito que se estudiará en el Capítulo 6). A continuación se listan y describen los requisitos [164]:

A) Transferencia de tiempo y frecuencia deterministas de alta precisión y compatibilidad industrial de distribución de tiempo.

La utilización de nuevos protocolos Ethernet que ofrecen una mejor precisión de sincronización redunda a su vez en una mejora de sistemas de control en Sistemas de Automatización de Subestación con respecto a la detección de eventos, registro y adquisición de datos [159], [160], [161]. Además, con el objetivo de operar con un único tiempo en la red es necesario que los diferentes protocolos industriales que lo suministran sean compatibles [141].

B) Tiempo confiable y transferencia de datos.

La implementación de protocolos de redundancia como HSR y PRP, descritos anteriormente, aumenta la robustez y la tolerancia a fallos, ya que evita la situación en la que un fallo simple en la red culmine con una interrupción del suministro y, al mismo tiempo, la duplicación de tramas asegura la recepción de paquetes críticos en el nodo de destino. Por otra parte, esto aumenta la disponibilidad de cualquiera de los servicios en una red White-Rabbit incluyendo el tiempo, que es considerado crítico en el contexto de SmartGrid.

C) Escalabilidad de tiempo.

En los Sistemas de Automatización de Subestación se presentan, por naturaleza, múltiples nodos interconectados en configuraciones en cascada y en paralelo. Estos nodos deben ser sincronizados con la misma referencia temporal, suministrada por el Maestro de Sincronización de la red y, por lo tanto, se debe tener en cuenta la precisión de la sincronización para determinar el máximo número posible de saltos.

D) Seguridad (safety y security).

La evaluación del nivel de SIL y la seguridad del sistema debe llevarse a cabo utilizando herramientas específicas basadas en estándares IEC6150 [41], IEEE1686-2013 [45].

En el siguiente apartado se presenta la implementación detallada de protocolos, métodos y mecanismos que fueron utilizados e integrados en el caso de uso con el objetivo de cumplir con los requisitos indicados.

5.3 Implementación

Este apartado describe la implementación que da respuesta a las funciones requeridas para un Sistema de Automatización de Subestaciones, centrándose en la distribución de la sincronización y la fiabilidad, escalabilidad y seguridad de la red.

A) Transferencia de tiempo y frecuencia deterministas de alta precisión y compatibilidad industrial de distribución de tiempo.

Como se indicó en el apartado 5.2, la principal tecnología utilizada en el centro de la red es White-Rabbit. White-Rabbit nació en el CERN (Consejo Europeo para la Investigación Nuclear), como tecnología de sincronización de Ethernet de código abierto. Es capaz de sincronizar dispositivos con una exactitud de menos de un nanosegundo y precisión de decenas de pico segundos.

Está basada en tres elementos fundamentales: una extensión de PTPv2 IEEE 1588 [165], la distribución de frecuencia usando ethernet síncrono (SyncE, Synchronous Ethernet) y una técnica de recuperación de señal precisa usando DDMTD (Dual Digital Mixer Time Difference) [166].

White-Rabbit-PTP se implementa en PPSi (PTP Ported to Silicon) que es un PTP portable desarrollado en el proyecto White Rabbit y bajo licencia GNU LGPL [167]. White-Rabbit-PTP funciona como una arquitectura jerárquica en modo maestro-esclavo, donde el maestro usa un mecanismo de sincronización en dos pasos y envía su sincronismo al esclavo [135]. La solución White-Rabbit, compuesta de Switches White-Rabbit y White-Rabbit-LENs, se implementa con productos de la empresa Seven Solutions S.L. [168].

Con respecto a la compatibilidad industrial, los dispositivos White-Rabbit permiten el uso de protocolos de bajo rendimiento como PTP e IRIG-B en la periferia de la red. Como los dispositivos White-Rabbit son capaces de distribuir PTP e IRIG-B a las RTUs se garantiza que dichos dispositivos son sincronizados con la misma referencia de tiempo que el maestro de sincronización. Por lo tanto, todos los eventos de todas las RTUs están etiquetados con una marca de tiempo con la misma referencia temporal. La sincronización se implementa no solo en el nivel de control, sino también en el nivel de adquisición, donde las entradas digitales de los dispositivos de la RTU de adquisición (concretamente los módulos de la familia Saitel de Schneider Electric SM_DI32 y AB_DI) registran eventos con una marca de tiempo basada en la sincronización referencia.

B) Tiempo confiable y transferencia de datos.

Con el fin de cumplir con los requisitos de fiabilidad sugeridos por el estándar IEC61850 para SmartGrid, se integró una implementación compatible con White-Rabbit del protocolo HSR [140] para los Switches White-Rabbit. HSR garantiza tolerancia a fallos, alta disponibilidad y resiste un fallo simple, tanto para el tiempo como para tramas de datos en la topología en anillo.

Como se puede observar en la Figura 39, el Maestro de Sincronización está conectado al anillo y envía la información temporal (White-Rabbit-PTP) por dos puertos conectados al anillo, de modo que el resto de los nodos reciben las tramas de tiempo duplicadas. Cada nodo del anillo solo procesa las tramas de tiempo recibidas por un puerto (puerto activo), y las tramas recibidas por el otro puerto se consideran de respaldo y son descartadas. Los nodos no HSR conectados a los Switches White-Rabbit HSR-WS solo reciben la copia principal de las tramas White-Rabbit-PTP (comportamiento de RedBox [140]).

En el caso de que ocurriese un fallo en alguna referencia de temporización primaria en el anillo, los Switches White-Rabbit-HSR afectados cambiarían de la referencia activa a la de respaldo. Este proceso denominado conmutación se realiza localmente en microsegundos. Este enfoque se basa en un trabajo desarrollado en el CERN para redes paralelas, pero sin ningún protocolo de redundancia [169].

A diferencia de otras soluciones similares a PTP, White-Rabbit usa Ethernet síncrono para distribuir la frecuencia. Esto representa un gran desafío tanto para las topologías de anillo como para el propio mecanismo de conmutación, ya que la utilización del Ethernet síncrono obliga a conmutar lo antes posible, ya que, de lo contrario, la sincronización se perdería. El tiempo máximo que un Switch White-Rabbit permanece sincronizado después de perder la referencia es de 100 ms [169]. Esto significa que el resto del anillo debe detectar la pérdida de referencia de tiempo primaria y en ese caso forzar una conmutación.

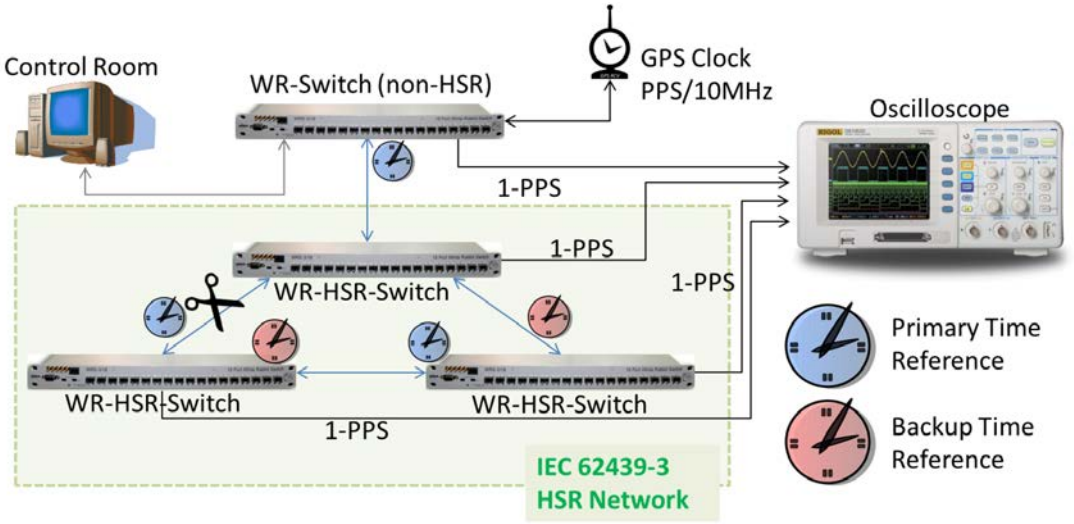

Figura 39: Red White-Rabbit HSR mostrando las referencias de tiempo primarias y secundarias.

Por esta razón, se desarrolló un mecanismo basado en hardware usando una matriz de puertas programables (FPGA, Field-Programmable Gate Array), para distribuir una alerta de conmutación usando símbolos de control 8b/10b sin formato, y codificación para la transmisión de bits en líneas de alta velocidad. Este mecanismo se administra mediante la Unidad de Conmutación Rápida (FSU: Fast Switchover Unit) y tarda aproximadamente un microsegundo por salto, garantizando así la precisión de sub-nanosegundo, incluso después de la conmutación. Cabe reseñar además que la sincronización de los nodos de la periferia tampoco se ve afectada.

En cuanto a la distribución de datos a través de la red, todas las tramas que circulan a través del anillo incluyen una etiqueta HSR. La etiqueta HSR se usa para identificar las tramas en redes HSR y realizar las operaciones propias del protocolo (supervisión, duplicación, caída y reenvío). Dicha etiqueta, como se puede observar en la siguiente figura, está compuesta por el Ethertype HSR, el identificador de path, el tamaño de la trama y el número de secuencia, como sugiere el estándar IEC 62439-3 [140].

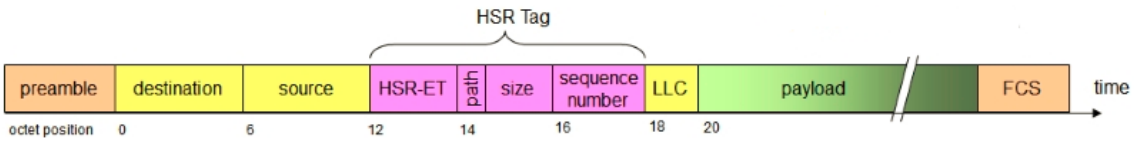

Figura 40: Trama HSR, en la que se destaca la etiqueta HSR. [Fuente: Estándar IEC 62439-3]

Cuando se envía una trama de datos desde un nodo de la periferia a otro nodo de la periferia conectado al anillo a través de un Switch White-Rabbit, el Switch White-Rabbit (que actúa como un RedBox) duplica la trama e inserta una etiqueta HSR en ambos con el mismo número de secuencia. Cada trama duplicada se envía en ambos sentidos del anillo para garantizar su recepción en el dispositivo de destino como se comentó en el apartado 5.1.

Cuando la primera trama de datos duplicados llega al Switch White-Rabbit que está conectado al nodo de destino, el Switch White-Rabbit le permite pasar hasta el nodo final. Cuando la segunda trama duplicada alcanza el switch, se identifica gracias a la etiqueta HSR y es descartada eliminándose de la red, asegurando que solo una trama llegue a su destino.

Los Switches White-Rabbit con capacidades HSR incluyen un bloque de lógica especial implementada a nivel hardware (IP core) denominada Unidad de Envío Rápido (FFU, Fast Forwarding Unit), que cuando el nodo de destino no está conectado por uno de sus puertos no HSR, reenvía tramas desde el puerto de recepción al otro puerto. Esto ayuda a reducir la latencia de la red, ya que las tramas no pasan por la lógica del núcleo de conmutación del Switch White-Rabbit y no se deben tener en cuenta en la toma de decisiones de enrutamiento, que, por otro lado, consumen mucho tiempo.

Sirva como referencia, el hecho de que los operadores de la red usan de forma masiva la fibra óptica a nivel de infraestructura de comunicación SmartGrid debido, por un lado, a la inmunidad frente a interferencias electromagnéticas y, por otro lado, a su cumplimiento con los requisitos de latencia, siendo la regla general de 5 microsegundos de latencia por kilómetro de longitud del cable [170].

C) Escalabilidad de tiempo.

La escalabilidad de una infraestructura de comunicación se vuelve crucial en redes heterogéneas. Concretamente en [171] se indica que “Para establecer una red inteligente se requiere una comunicación escalable máquina a máquina que permita controlar y coordinar millones de dispositivos de producción y consumo de energía”.

Para aumentar la escalabilidad de la red de sincronización, la implementación de White-Rabbit, para este caso de uso, como alternativa al enfoque de end-to-end original, utiliza un enfoque de Peer-to-Peer (P2P) para medir el retraso entre nodos. Por otro lado, los nodos que forman el anillo se comportan como Relojes Transparentes (TC, Transparent Clocks) en lugar de Relojes Frontera (BC, Boundary Clocks). Esto mejora la estabilidad y, por lo tanto, la escalabilidad de todo el sistema de sincronización [136]. Además, la interoperabilidad también se incrementa ya que este tipo de aplicaciones tiende a utilizar Relojes Transparentes junto con el enfoque P2P [172].

D) Seguridad (safety y security).

Para analizar los aspectos de seguridad (safety y security) del sistema, se utilizó una herramienta basada en Eclipse. Dicha herramienta aúna en un mismo entorno tres procesos distintos. Dos procesos permiten estimar el nivel de seguridad (safety) mediante la métrica SIL (comentada en el apartado 3.2) definida en el estándar IEC61508, y el tercero analiza la seguridad (security) basado en el estándar IEEE1686. A continuación se ilustran dichos procesos:

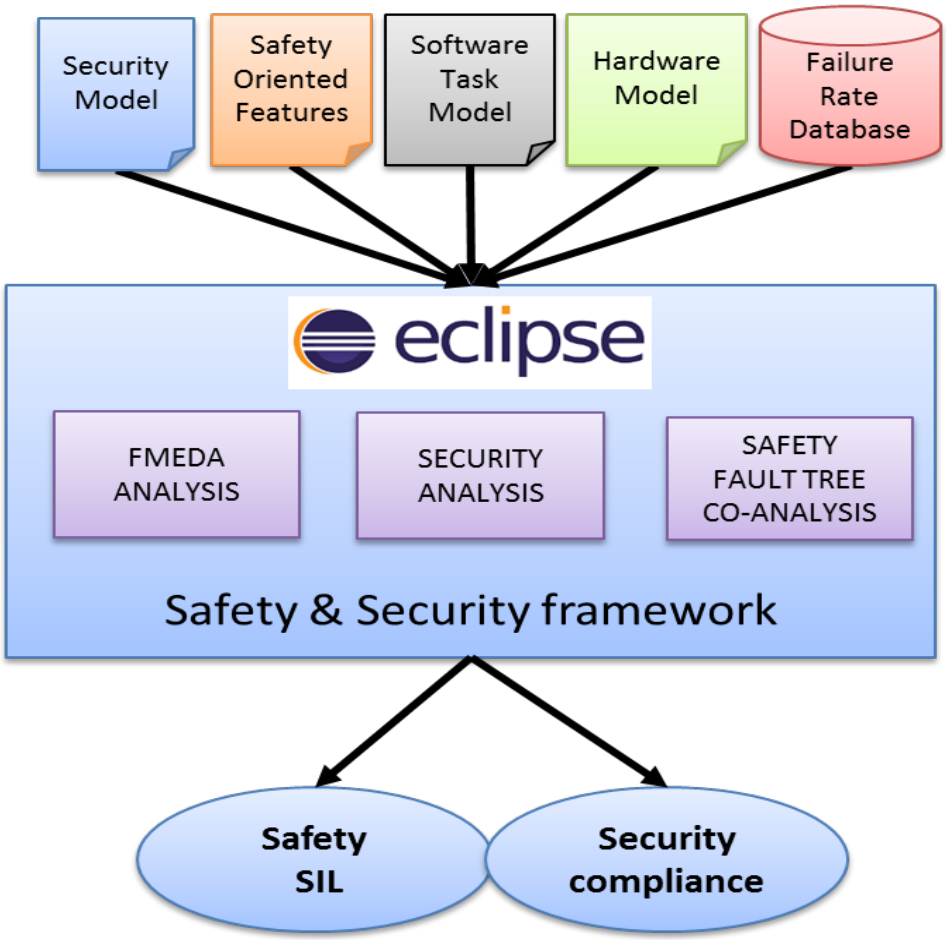

Figura 41: Componentes integrados en el sistema de Safety y Security en el entorno utilizado.

El primer proceso consiste en la realización de un análisis de modos de fallo, efectos y diagnósticos, lo cual permite estimar el SIL de los componentes hardware del sistema. Para ello, se ha utilizado un método que permite automatizar la captura de las características del sistema, usando los ficheros que los usuarios generan durante el desarrollo del sistema: el fichero BOM (Bill Of Materials) o el esquema EDIF (Electronic Design Interchange Format). Automáticamente, se genera el "Análisis de Diagnósticos, Efectos y Modos de Fallo" y el informe correspondiente con la información necesaria para la certificación de seguridad. Dicho análisis, como se puede ver en la Figura 42, incluye tablas con los modos de fallo de cada componente y parámetros adicionales, como el Porcentaje de Fallos de Seguridad (SFF, Safe

Failure Fraction) o Cobertura de Diagnóstico (DC, Diagnostic Coverage) que se requieren para calcular el nivel de SIL del hardware.

Además, para la captura de las tasas de errores (necesarias para los cálculos del nivel de SIL) de cada componente, se desarrolló e integró en la herramienta una base de datos de componentes. Se buscaron y añadieron a la base de datos información de tasas de fallos de componentes básicos. En el caso de que algún componente del sistema no estuviese en la base de datos, ésta es fácilmente ampliable, lo cual permite utilizarla para la evaluación de cualquier sistema.

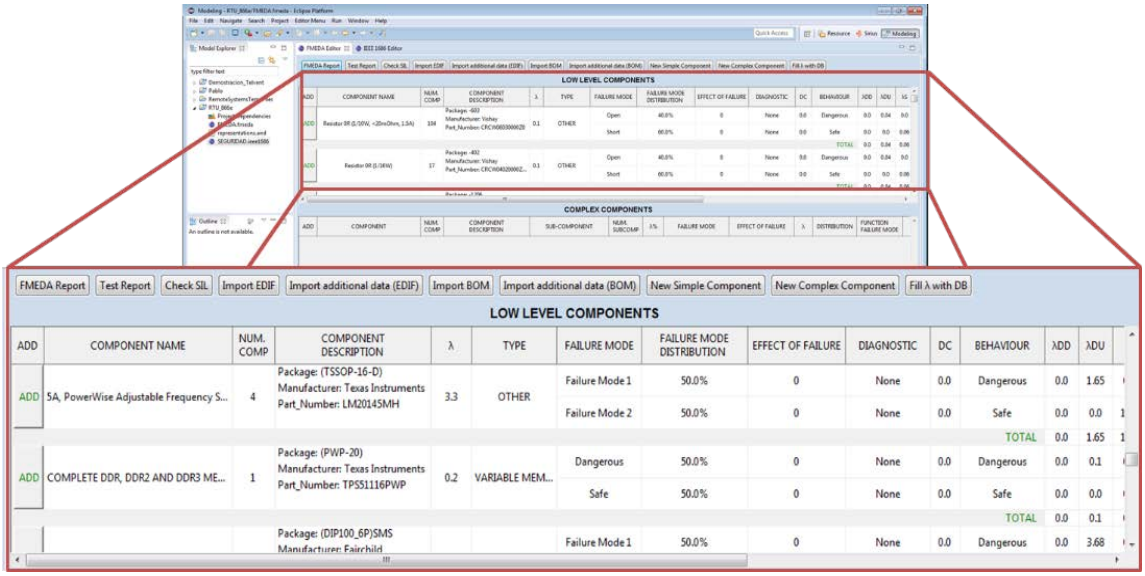

Figura 42: Análisis de Diagnósticos, Efectos y Modos de Fallo generado que incluye los modos de fallo de cada componente y parámetros adicionales, como el porcentaje de fallos de seguridad o la cobertura de diagnóstico que se requieren para calcular el nivel de SIL. [Fuente: Proyecto EMC2 Public deliverable “D6.15 – Validation Report” [129]]

El segundo proceso, co-análisis de fallos de seguridad (safety fault tree co-analysis), permite realizar un análisis de fallos en árbol teniendo en cuenta tanto los componentes hardware como el software, dando como resultado una estimación del nivel de SIL del sistema en su conjunto. La descripción de la tecnología de los componentes hardware se completa con modelos de los componentes software (tareas y / o funciones) y mapeo hardware / software (asignación de tareas / funciones a recursos hardware). La herramienta genera un análisis de fallos en árbol (FTA, Fault Tree Analysis) para estimar la tasa de riesgo tolerable (THR, Tolerable Hazard Rate) que está relacionada con el parámetro “Safe Failure Fraction” y en último término permite estimar el nivel de SIL.

Esto genera un esquema del árbol y una tabla con la información que ayuda a detectar las ramas más débiles del árbol, con el fin de mejorar los parámetros de seguridad. A continuación se ilustra dicho esquema.

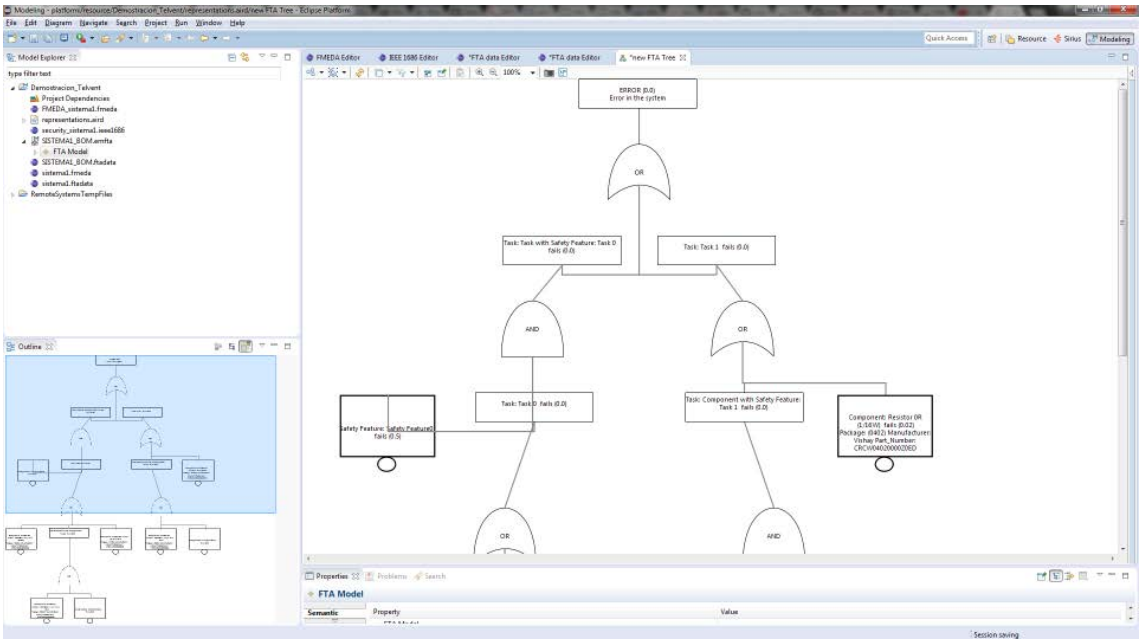

Figura 43: Diagrama de análisis de fallos en árbol, FTA. [Fuente: Proyecto EMC2 Public deliverable “D6.15 – Validation Report” [129]]

El tercer proceso está directamente relacionado con el análisis de seguridad (security). Dicha metodología está basada en el estándar de seguridad IEEE 1686, que establece las cláusulas que el sistema debe cumplir. Estas cláusulas están agrupadas en una "Tabla de Cumplimiento", lo que facilita la captura de información. Con dicha información la herramienta genera el correspondiente informe.

5.4 Resultados

En este apartado se presenta la evaluación del funcionamiento y los beneficios de los desarrollos descritos para el caso de uso de Subestación relacionados con los requisitos enunciados previamente en el apartado 5.2.

A) Transferencia de tiempo y frecuencia deterministas de alta precisión y compatibilidad industrial de distribución de tiempo.

La precisión del tiempo y de la frecuencia se han medido teniendo en cuenta los diferentes protocolos que coexisten dentro de la red y la forma en que están interconectados. En aras de plantear un sistema interoperable, para sincronizar las RTU del sistema de control de la periferia de la red, además de la tecnología White-Rabbit, se han evaluado PTPv2 e IRIG-B.

El dispositivo SM_CPU866e utiliza PTPv2 y el dispositivo HU_A usa IRIG-B. La siguiente tabla resume la interconexión del sistema de sincronización y las diferentes precisiones del caso de uso en función de la tecnología utilizada. Las mediciones se tomaron usando un contador de señal Tektronix FCA3000/3100 Timer/Counter/Analyzer [173], con el que se compararon la señal del pulso por segundo con las salidas de los White-Rabbit Switch, White-Rabbit-LEN,

SM_CPU866e y la RTU HU_A. Dicho dispositivo suma 20 picosegundos de incertidumbre a los resultados finales.

Dispositivo Maestro	**WR (offset medio)**	**PTPv2 (offset medio)**	**IRIG-B (offset medio)**	**Dispositivo esclavo**
WRS	21 ps	N/A	N/A	WRS
WRS	111 ps	N/A	N/A	WR-LEN
WRS	N/A	112,33 ns	N/A	SM_CPU866e
WR-LEN	N/A	N/A	10 ms	RTU HU_A

Tabla 9: Precisión por protocolo en el caso de uso.

En la Tabla 9 se puede observar los siguientes resultados:

- Dos Switches White-Rabbit calibrados que utilizan White-Rabbit se sincronizan con una precisión media de 21ps, como se muestra en la Figura 44.
- Un White-Rabbit-LEN conectado a un Switch White-Rabbit con White-Rabbit presenta una precisión de 111ps.
- Utilizando PTPv2 estándar con marcas de tiempo, un SM_CPU866e conectado a un Switch White-Rabbit muestra una media de 112,33 ns.
- La precisión de sincronización entre un White-Rabbit y una RTU HU_A usando IRIG-B es de 10 ms de media.

Es importante indicar que la tecnología de sincronización de White-Rabbit es prácticamente inmune al tráfico de datos, lo que lleva a una implementación de red más determinista. Este no es el caso de PTPv2, que se degrada significativamente cuando hay un importante tráfico de datos.

A continuación se muestra la salida de 10MHz desde dispositivos White-Rabbit sincronizados con una precisión por debajo de un nanosegundo, concretamente 21 picosegundos.

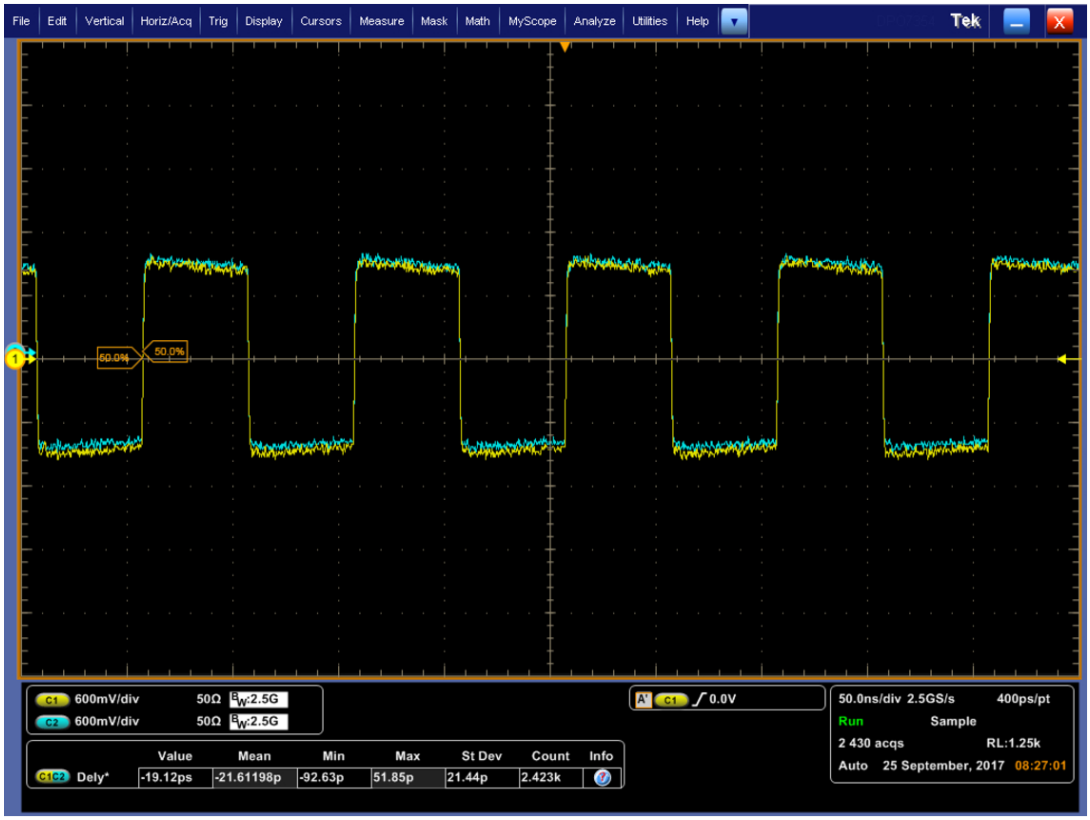

Figura 44: Salida de 10MHz desde dispositivos White Rabbit sincronizados con una precisión por debajo de un nanosegundo.

Finalmente señalar, que la adaptación de los dispositivos White-Rabbit para admitir protocolos de sincronización industriales, como PTP e IRIG-B, permite reducir la fuente de sincronización de todos los dispositivos a un único maestro de sincronización, en lugar de utilizar uno por protocolo, lo que a su vez aumenta el nivel de determinismo en la red.

B) Tiempo confiable y transferencia de datos.

La implementación del protocolo HSR proporciona al sistema de adquisición y control funciones de redundancia para la sincronización y tramos de datos, lo que aumenta la disponibilidad de los servicios de red debido a la duplicación de dichas tramas y, por lo tanto, permite el presentar un solo punto vulnerable a un fallo simple.

En cuanto a la distribución de la sincronización de forma redundante, el protocolo HSR garantiza disponer de dos referencias de tiempo simultáneamente. En caso de que se pierda la referencia de tiempo primaria, los nodos HSR pueden cambiar a la referencia de respaldo en microsegundos [174] manteniendo la precisión de los nanosegundos. Esto se debe a la adaptación del mecanismo de conmutación a topologías de anillo y al sistema de alerta de conmutación que utiliza símbolos de control sin procesar, que es capaz de enviar la alerta en un microsegundo por salto.

Para realizar una comparación precisa entre la latencia de datos del Switch White-Rabbit estándar y el Switch White-Rabbit HSR, se han realizado medidas de latencia a nivel de hardware (FPGA gateware) utilizando Xilinx Chipscope Tool [175] para contar el número de ciclos entre la llegada de la trama y su envío. Se han utilizado diferentes tamaños de tramas para realizar estas pruebas: 64, 128, 512 y 1024 bytes.

Por un lado, los Switches White-Rabbit estándar usan una Unidad de Tabla de Enrutamiento para decidir a qué puerto de trama de datos se deben enviar para llegar a su destino. Dichos datos se envían a un núcleo de lógica de conmutación IP que consume varios ciclos de FPGA. La siguiente tabla presenta los resultados para la latencia de los datos para el Switch White-Rabbit estándar.

Switching Core (Bytes)	64	128	512	1024
Ciclos	106	139	136	136
Tiempo (ns)	1701	2227	2180	2174

Tabla 10: Latencia en el WRS estándar.

Los resultados muestran que la latencia del WRS estándar está en el rango 1701 y 2174 nanosegundos dependiendo del tamaño de la trama.

Por otro lado, los Switches White-Rabbit HSR pueden reducir la latencia gracias a la Unidad de Envío Rápido que reduce el tiempo de residencia de una trama dentro de un Switch FPGA White-Rabbit. Este módulo reenvía tramas de datos de un puerto conectado al anillo al otro en el caso de que la dirección MAC (Media Access Control) de destino no pertenezca a él mismo.

Además de esto, las tramas que pasan por el anillo tienen una prioridad mayor que los que provienen de la lógica de conmutación de FPGA, de modo que comienzan a abandonar el Switch White-Rabbit al mismo tiempo que llegan a la Unidad de Envío Rápido. En la siguiente tabla se presentan los resultados de latencia para el Switch White-Rabbit HSR usando la Unidad de Envío Rápido. Independientemente del tamaño de la trama, reenviar una trama de un puerto a otro consume 63 ciclos de reloj, cuyo período es de 16 nanosegundos, resultando 1,01 nanosegundos la latencia total para Switches White-Rabbit HSR y, por lo tanto, reduciendo a aproximadamente la mitad de la latencia Switch White-Rabbit estándar.

HSR Fast Forwarding (bytes)	64	128	512	1024
Ciclos	63	63	63	63
Tiempo (ns)	1008	1008	1008	1008

Tabla 11: Latencia en el HSR- White-Rabbit con la Unidad de Envío Rápido.

C) Escalabilidad de tiempo.

La escalabilidad del sistema de temporización y sus efectos en la señal de sincronismo del pulso por segundo en términos de fluctuación de fase y retardo de propagación (jitter y skew) se evaluó utilizando catorce nodos White-Rabbit-LEN que forman una cadena margarita, donde el primer eslabón es el maestro de sincronización y el resto de los nodos son esclavos del nodo que le precede, sucediéndose unos a otros y actuando como maestro del nodo que le sucede.

Así pues, se ha utilizado el contador de señal Tektronix FCA3000/3100 Timer/Counter/Analyzer [173] para medir el retardo de propagación (skew) de la señal de pulso por segundo del maestro de sincronización con respecto a los esclavos primero, decimosegundo y decimotercero de la cadena de margaritas.

Los resultados obtenidos por el grupo de trabajo del proyecto EMC2 en "EMC2 Public deliverable D11.4 – Final demonstrator implementation and evaluation" [129] indican que la precisión de sub-nanosegundo en toda la cascada hasta el duodécimo nodo esclavo está garantizada. Desde el nodo decimotercero en adelante, los nodos están sincronizados, pero la precisión, en este caso es superior a un nanosegundo.

D) Seguridad (safety y security).

La herramienta de seguridad ha sido utilizada con los dispositivos más relevantes del caso de uso, es decir, Switch White-Rabbit, White-Rabbit-LEN, SM_CPU866e y SM_DO32T, obteniendo la estimación del nivel SIL y el nivel de cumplimiento con el estándar IEEE1686, previamente introducidos en el apartado 3.2.

El nivel de SIL se obtiene a partir de la tasa de fallos (λs) que provee cada fabricante para cada tipo de fallo y componente, la cual se representa en tasas de fallo de campo (FITS: Field Failure Rate).

En este caso, los tipos de fallo significativos son el fallo peligroso no detectado (λDU), el fallo seguro (λS) y el fallo sin efecto (λNE). El resto de fallos, es decir fallo peligroso detectado (λDD), fallo High (λH), fallo Low (λL) y fallo Annunciation (λA) para estos dispositivos son cero.

En la Tabla 12 se presentan los valores de los tipos de fallos para cada componente del caso de uso y el resultado que arroja la herramienta utilizada a partir de dichos valores. Así pues, la estimación de nivel de SIL para los cuatro dispositivos resulta ser "nivel 1".

En una primera aproximación, dicho nivel de SIL resulta ser bajo para todos los dispositivos, pero el conocimiento de la información detallada y estructurada es el punto de partida para mejorar el nivel de SIL obtenido.

Device		WR-LEN	WRS	SM_CPU866e	SM_DO32T
Safe Failure Fraction (SFF) :	%	83,64	81,33	72,91	76,44
Internal Hardware Fault Tolerance (HFT) :		0,00	0,00	0,00	0,00
Dangerous Detected (DD) Failure Rate(λDD) :	FITS	0,00	0,00	0,10	0,00
Dangerous Undetected (DU) Failure Rate(λDU) :	FITS	61,22	113,02	283,24	264,70
Safe (S) Failure Rate(λS) :	FITS	312,96	492,18	762,41	858,76
Fail High (H) Failure Rate(λH) :	FITS	0,00	0,00	0,00	0,00
Fail Low (L) Failure Rate(λL) :	FITS	0,00	0,00	0,00	0,00
No Effect (NE) Failure Rate(λNE) :	FITS	4,00	6,20	3,60	0,00
No Part (-) Failure Rate(λ-) :	FITS	0,00	0,00	0,00	0,00
System Type:		B	B	B	B
Safety Integrity Level (SIL):		SIL 1	SIL 1	SIL 1	SIL 1

Tabla 12: Resultados del SIL de los dispositivos representativos del caso de uso de Subestación.

Para poder realizar dicha mejora, en primer lugar, es necesario identificar los componentes críticos, que vienen a ser, básicamente, aquellos con la mayor tasa de fallos no detectados. En este caso habría tres posibles acciones para aumentar el nivel de SIL:

a) Cambiar el componente por otro equivalente con mejor tasa de fallos no detectados.
b) Incluir diagnosis para mejorar la cobertura de diagnóstico.
c) Incluir redundancia.

Con respecto al análisis de seguridad, en primer lugar, se incluye la información de seguridad del dispositivo SM_CPU866e. Las cláusulas del estándar IEEE1686 se introducen en la "tabla de cumplimiento" indicando en cada caso el nivel de cumplimiento entre cuatro posibles opciones según se define en el estándar:

a) Acknowledge: se usa como marcador cuando no se presenta ningún requisito en la cláusula.
b) Exception: no cumple con uno o más de los requisitos de la cláusula.
c) Comply: cumple completamente los requisitos establecidos de la cláusula.
d) Exceed: excede uno o más de los requisitos establecidos de la cláusula.

A continuación se ilustra dicho proceso:

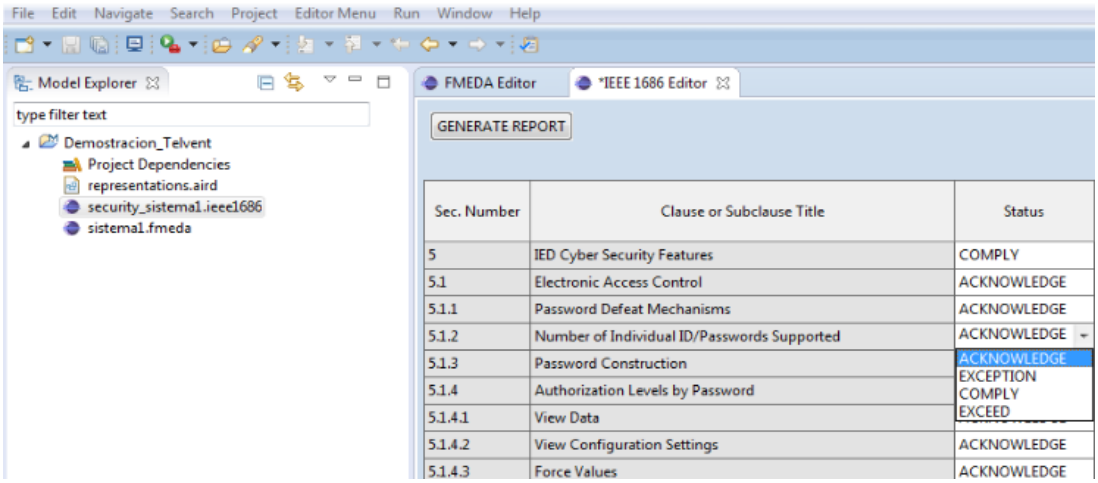

Figura 45: Herramienta de cumplimiento de seguridad. [Fuente: Proyecto EMC2 Public deliverable "D6.15 – Validation Report" [129]]

Después de completar dichas cláusulas, se genera un informe que muestra gráficamente la información sobre el nivel de cumplimiento del dispositivo con respecto a la norma, como se muestra en la siguiente figura. En el caso de uso de la subestación el 94% de las cláusulas no representan ningún requisito, mientras que un 2% cumple los requisitos, otro 2% los excede y solamente un 2% no cumple uno o varios de los requisitos. Por ello se puede concluir que se cumple con el 98% de las cláusulas.

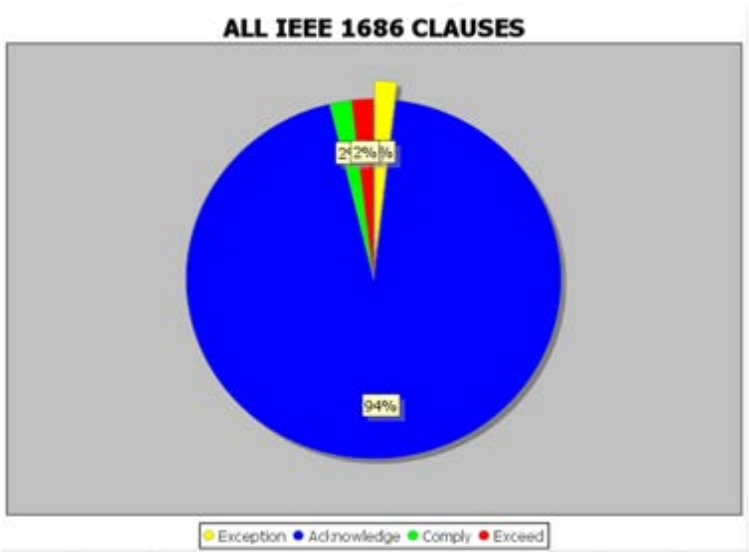

Figura 46: Resultados de cumplimiento de seguridad.

A continuación se ilustra el demostrador utilizado en el caso de uso de la subestación, desarrollado por el grupo de trabajo del proyecto EMC2 [129] que incorpora los dispositivos, componentes y tecnologías descritos anteriormente.

En primer lugar, se presenta la implementación del anillo HSR formando por un WRS actuando como Maestro de Sincronización y los otros 5 WRS para formar el anillo.

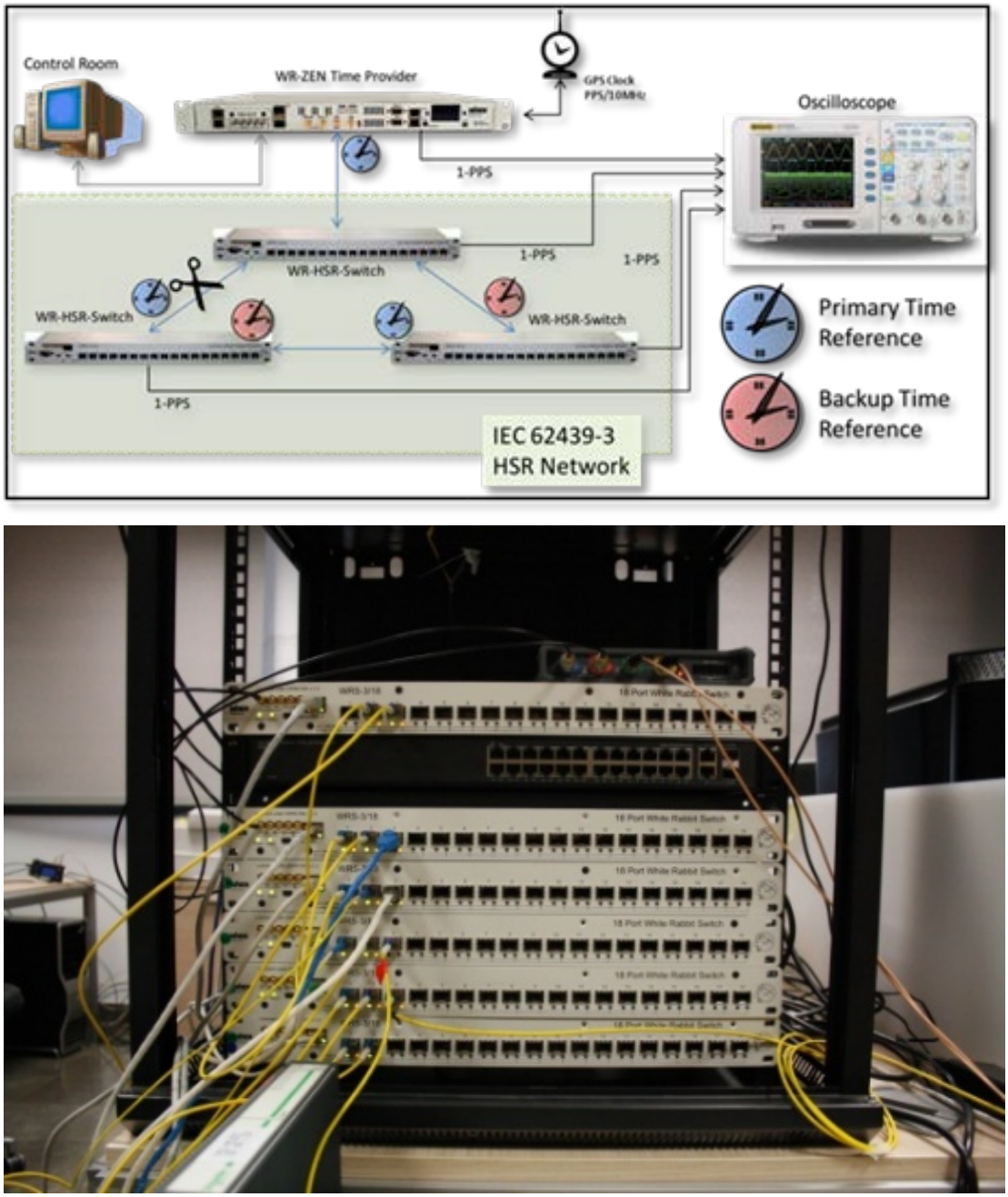

Figura 47: Demostrador: Diseño HSR (arriba), la implementación (abajo). [Fuente: Proyecto EMC2 Public deliverable “D11.4 – Final demonstrator implementation and evaluation” [129]]

A continuación se muestran los elementos que están sincronizados por los distintos medios, es decir, la RTU Front-end por PTPv2 IEEE1588, la RTU de adquisición por IRIG-B y el WR-LEN por White-Rabbit.

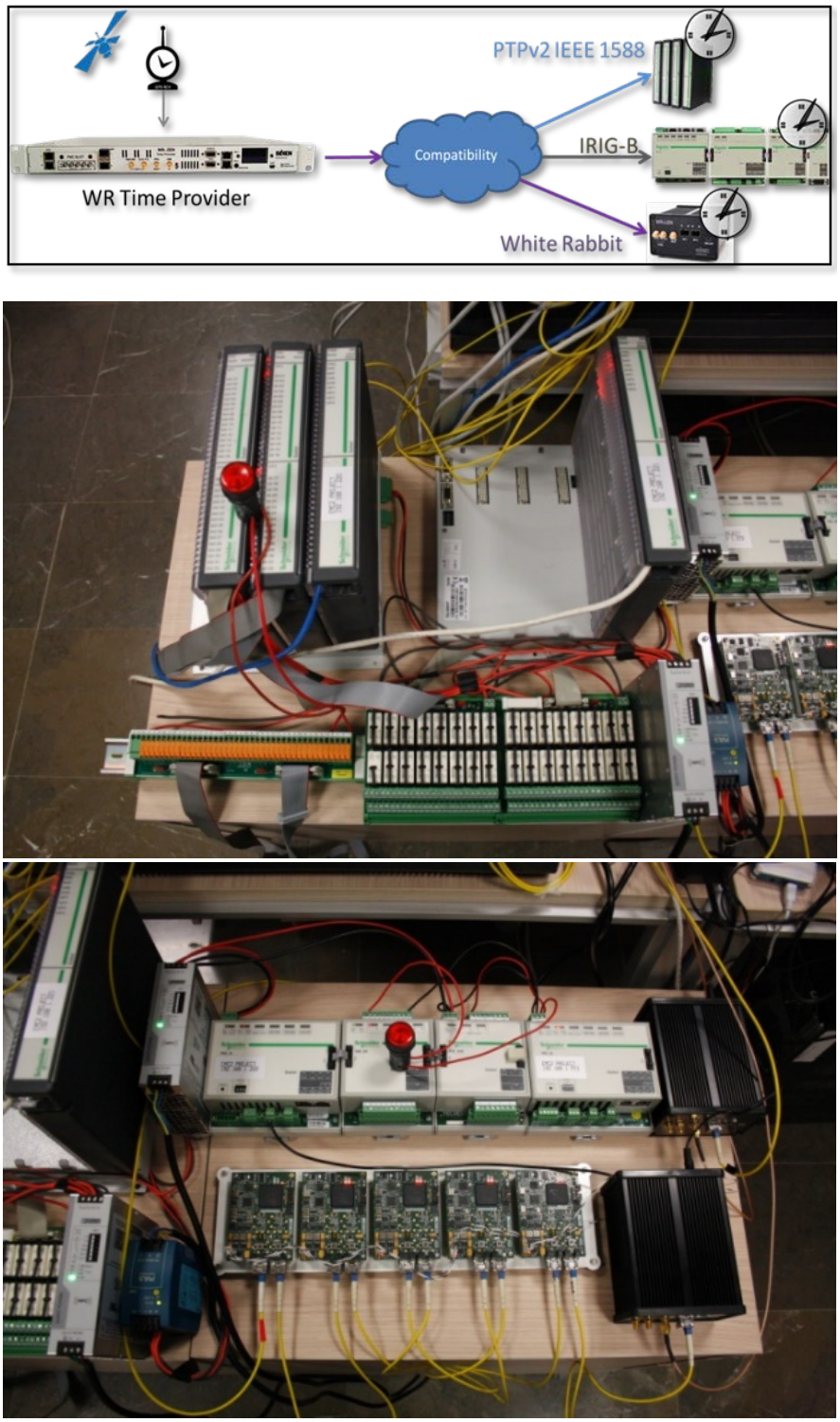

Figura 48: Demostrador: Diseño (arriba), implementación sincronización PTP (en medio), IRIG-B y la cadena de margaritas formada por 6 WR-LEN (abajo) [Fuente: Proyecto EMC2 Public deliverable “D11.4 – Final demonstrator implementation and evaluation” [129]]

Finalmente, en la Figura 49**¡Error! No se encuentra el origen de la referencia.** se presenta el demostrador completo, en donde sombreado en naranja se encuentra el sistema de sincronización redundante que soporta un fallo simple, sombreado en azul se encuentra el Sistemas de Automatización de Subestación a sincronizar, formado por las

RTUs, y finalmente sombreado en verde la parte dedicada a demostrar la escalabilidad con la cadena de margaritas de WR-LEN.

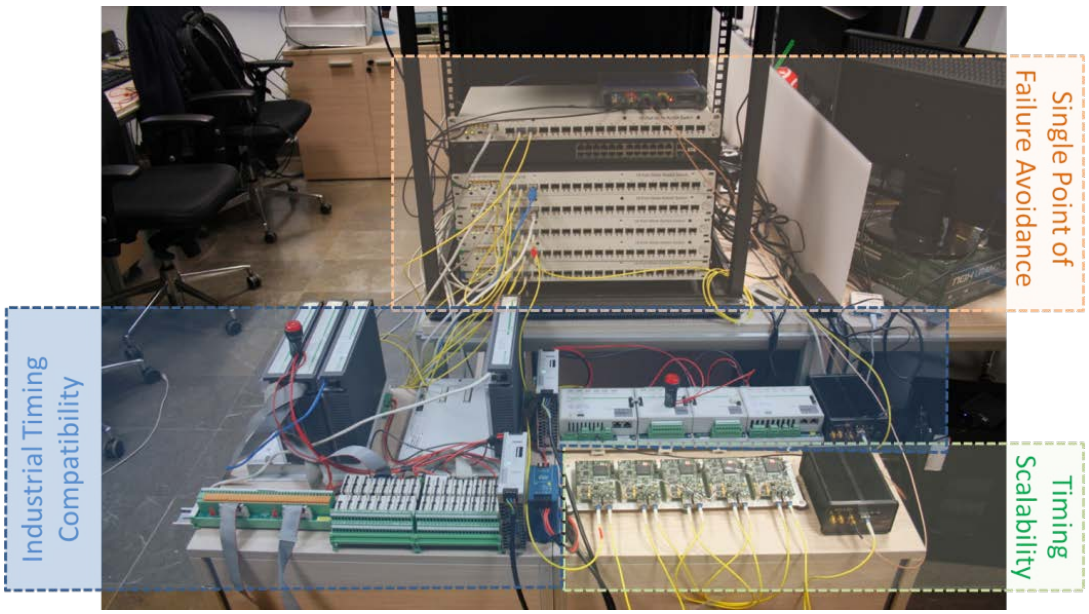

Figura 49: Demostrador donde se encuentra un WRS como Maestro de Sincronización, 5 WRS para formar un anillo HSR al que se conecta la RTU que actúa como Front-end, varios WR-LEN en cascada que proveen sincronización mediante IRIG-B a la RTU de adquisición, así como los relés y los pulsadores para simular entradas de sensores de campo. [Fuente: Proyecto EMC2 Public deliverable “D11.4 – Final demonstrator implementation and evaluation” [129]]

5.5 Conclusiones

En este capítulo se ha presentado la implementación del caso de uso del Sistema de Automatización de Subestación como una prueba de concepto para las nuevas aplicaciones SmartGrid donde la confiabilidad, la escalabilidad, los protocolos de sincronización heterogéneos y la baja latencia son características clave y hasta, en ciertas ocasiones, obligatorias para los sistemas de control. Los estudios realizados en este caso de uso representan un nuevo horizonte en términos de sincronización y confiabilidad en SmartGrid.

De esta forma, se han utilizado dispositivos industriales de mercado para implementar un Sistema de Automatización de Subestación en el que se ha integrado HSR con tecnología White-Rabbit siguiendo las sugerencias del estándar IEC62439-3. En este escenario se ha demostrado la bondad de la tecnología White-Rabbit con la que se consiguen precisiones de hasta 21ps entre Switches White-Rabbit.

Por otro lado, la utilización de dispositivos White-Rabbit para este tipo de sistemas de control con elementos distribuidos en la red, garantiza una precisión de sincronización de nanosegundos para hasta 13 nodos en topologías de anillo y cascada. Además, estos dispositivos pueden operar con diferentes protocolos de sincronización como PTPv2 o IRIG-B, lo que aumenta las opciones a nivel de compatibilidad del sistema.

En lo que respecta a los datos, el hardware White-Rabbit-HSR utilizado es capaz de reducir la latencia de reenvío de las tramas a más de la mitad de la estándar, es decir de 2,2 µs a 1 µs.

Al mismo tiempo, se ha realizado el desarrollo de un entorno de evaluación de seguridad (security y safety) basado en FMEDA hardware, análisis de árbol de fallos hardware/software y análisis de seguridad. Los resultados obtenidos de la evaluación de las RTU y los elementos de sincronización en este entorno demuestran que, aunque el punto de partida inicial era un nivel básico de seguridad, las mejoras propuestas a nivel de componentes, cobertura de diagnóstico y redundancia de componentes mejorarían los resultados de evaluación hasta el segundo nivel SIL.

Capítulo 6. Concepción de un Nuevo Sistema de Gestión y Mantenimiento de Subestaciones Eléctricas Basado en Internet Social de las Cosas

La innovación en el ámbito de las Tecnologías de la Información y Comunicaciones (TIC) y la evolución y el desarrollo del concepto de Internet de las Cosas han representado un gran impacto en el campo de las comunicaciones. Si bien, el sector industrial es el mayor beneficiario potencial de esta ventana de oportunidad, la industria se enfrenta al desafío de implementar los últimos avances tecnológicos para aumentar la competitividad de sus soluciones.

En este capítulo se presenta un sistema funcional para mejorar la gestión y mantenimiento de las Subestaciones eléctricas utilizando una aproximación completamente disruptiva. La solución se basa en el paradigma de Redes Sociales combinado con el mundo de Internet de las Cosas sobre la RTU, y presenta un enfoque novedoso en el mundo del control en tiempo real de SmartGrid, yendo más allá del concepto clásico de comunicación Máquina a Máquina (M2M) y Máquina a Humano (M2H) en la interacción entre RTUs-usuarios.

Por tanto, se describe la implementación de un sistema de control en tiempo real basado en Internet Social de las Cosas para Subestaciones eléctricas basado en las RTUs. Este capítulo está organizado de la siguiente forma: se proporciona una breve descripción sobre conceptos como el Internet Social de las Cosas y las Redes Sociales, así como el potencial uso de dichas redes como entorno para el desarrollo del Internet de las Cosas Industrial. Posteriormente, se presenta la RTU como representante de Internet de las Cosas en las Subestaciones eléctricas y a continuación se describe la implementación realizada, destacando los principales desafíos y limitaciones. Finalmente se presenta la discusión y las conclusiones de estos resultados.

6.1 Introducción

Como se ha comentado anteriormente en el apartado 3.5.1, Internet de las Cosas es ya una realidad y representa un nuevo potencial para el sector industrial. Desde la optimización de procesos hasta el desarrollo de nuevos modelos de negocios, la industria se encuentra con la necesidad de explotar las innovaciones tecnológicas que ofrece IoT para mejorar la competitividad de sus soluciones y aumentar sus ingresos.

En la actualidad, como también se ha comentado en el apartado 3.5.1, existen ya múltiples plataformas de IoT y protocolos en desarrollo y producción y, por tanto, los esfuerzos se centran, principalmente, en el desarrollo de aplicaciones inteligentes. Dichas aplicaciones en su mayor parte están destinadas a usuarios, y todavía son pocas las implementaciones reales que se pueden encontrar en el sector industrial [176]. Las principales razones por las que la industria es reacia a incorporar nuevas tecnologías son: los estrictos requisitos

de fiabilidad y tiempo real, la interoperabilidad limitada entre estándares, el desconocimiento del estado actual de la tecnología, y el alto costo y la larga vida útil de productos industriales [177], [178].

Estos requisitos específicos han dado lugar a la llamada IoT Industrial (IIoT, Industrial IoT) o visión industrial de Internet de las Cosas que cuenta con el apoyo del Industrial Internet Consortium (IIC) [179] fundado en 2014 por AT & T, Cisco, GE, IBM e Intel, y que incluye a miembros relevantes del sector como Schneider Electric, con la misión de coordinar las iniciativas de ecosistemas para conectar e integrar objetos con personas, procesos y datos, utilizando arquitecturas comunes, interoperabilidad y estándares.

El impacto futuro del IoT en la industria se analizó en el "World Economic Forum, Geneve, en 2015" [177] y reveló que se espera, a corto plazo, lograr la eficiencia operativa y la creación de nuevos productos, y a largo plazo, ecosistemas conectados, mercados y plataformas, y automatización y optimización de recursos. Esta visión es compatible con los sistemas industriales basados en agentes [180], [181], [182] en el paradigma de Agentes de las Cosas (AoT, Agents of the Things) [183].

Como se ha indicado anteriormente, existe un conocimiento limitado de la tecnología IoT desde la industria y, por lo tanto, existe la necesidad de encuadrar desarrollos recientes. En [183] se propone un modelo útil y funcional del IoT que define dos ámbitos diferentes: IoT Industrial y IoT Humano. Las principales diferencias entre ambos se enumeran en [178] y [184], que además ponen de manifiesto una limitación importante cuando hacen referencia a la interacción humana.

IoT industrial se refiere al control autónomo, donde el flujo de datos es asimétrico y principalmente hacia arriba, y donde las reglas se pueden cambiar, aunque los cambios impulsados por el ser humano se consideran como algo fuera de lo normal.

Dicha limitación se resuelve parcialmente en el IoT Humano, donde las acciones explícitas o arbitrarias de las personas pueden cambiar las reglas o desencadenar secuencias de control. La interacción con el ser humano también podría resolverse en el ecosistema de Internet Social de las Cosas, concepto introducido anteriormente en el apartado 3.5. Como se ha comentado en dicho apartado, SIoT surgió como un nuevo enfoque conceptual donde el paradigma de Red Social se aplica al mundo de IoT facilitando el proceso de comunicación, y trabajando hacia un nuevo modelo de mejora de la conexión entre dispositivos y entre usuarios por un lado y entre los propios dispositivos por otro lado, más allá de la clásica comunicación M2M o M2H.

La investigación sobre IoT y SIoT se ha realizado en el marco de los proyectos nacionales INFIERE (INvestigation of the Future Intelligent Elements for Renewable Energy) [185], SAGRA (Sistema Avanzado para Gestión de Redes Aisladas) [186] y 3S-CS (Standardization Security Synchronization Connected Substation) [187].

6.2 IoT y el paradigma de las Redes Sociales

Partiendo de lo introducido al respecto de las Redes Sociales en el apartado 3.5, es necesario profundizar en el potencial de las mismas. Las Redes Sociales han demostrado disponer de unas inmejorables características a nivel estructural y relacional centradas en lo que respecta al usuario, lo que sin duda les ha permitido disfrutar de un impresionante

impacto social y, en definitiva, ha creado una nueva forma de comunicación y entendimiento.

El principio, de que gran número de personas vinculadas en una red social puede proporcionar respuestas más precisas a problemas complejos que un solo individuo, ha sido explotado en diferentes ámbitos relacionados con Internet, y ha sido utilizado para la implementación de sistemas de Internet de las Cosas, que esperan integrar un gran número de tecnologías y conectarse a decenas de miles de millones de objetos a corto plazo y poder explotar dicho principio.

En este contexto de conectividad entre millones de objetos y los usuarios de servicios de Internet de las Cosas, se aplica el concepto de las Redes Sociales al IoT, y entre sus objetivos más ambiciosos se encuentra el que los propios objetos imiten el comportamiento humano y creen relaciones basadas en las normas establecidas por sus propietarios. Esto permitiría mejorar la comunicación entre los seres humanos y la inmensa cantidad de objetos conectados a la red, que sigue creciendo día tras día [188], [189], [190].

Así pues, la combinación de la Red Social y el IoT aportará a esta última las siguientes nuevas características y capacidades:

- Capacidad de definir un perfil.
- Capacidad de suscrición a perfiles y/o canales.
- Creación de comunidades y/o canales de acuerdo con perfiles.
- Establecimiento de diferentes relaciones en función del entorno.
- Mejora de comunicaciones para sistemas distribuidos.
- Escalabilidad.
- Control de acceso, elementos y políticas de seguridad.

Además, SIoT resuelve la mayor parte de los problemas cuando se establece una comunicación, concretamente:

- Descubrimiento: cuando se establece una comunicación, en los sistemas tradicionales es necesaria la intervención de un agente intermediario. Sin embargo, SIoT presenta mecanismos de autodescubrimiento de dispositivos.
- Direccionamiento: los dispositivos en una red privada suelen estar asignados a una dirección estática o en caso contrario a una dirección dinámica. En ambos casos, se entorpece el proceso de ruteado. En el SIoT, la identificación de los usuarios está asignada en la Red Social y de esta forma la plataforma gestiona fácilmente el proceso de ruteado.
- Bidireccionalidad en la comunicación: normalmente el problema de direccionar correctamente los dispositivos obstaculiza la comunicación en dos sentidos. El SIoT da solución a dicha problemática asegurando la comunicación.

Al mismo tiempo, SIoT permite la publicación de mensajes sin la necesidad de descubrir los dispositivos, simplemente utilizando círculos o comunidades de confianza, tras el previo filtro de seguridad y control de acceso definido en dichas comunidades.

Así, se establece un nivel de confianza que potencia el grado de interacción entre los objetos clasificados como “amigos”, es decir, es posible asociarlos mediante algún tipo de relación dentro de la red.

Los objetos pueden establecer relaciones sociales sobre la base del perfil del objeto, actividades e intereses (aplicaciones implementadas en el objeto y servicios que ofrece). Estas relaciones también se pueden clasificar de acuerdo con los eventos que desencadenan su establecimiento [191]:

- Una relación de “co-ubicación” puede establecerse entre los objetos que se utilizan siempre en el mismo lugar.
- Una relación de “co-trabajo” puede establecerse cuando algunos elementos colaboran para proporcionar una aplicación común de IoT.
- Una relación "parental” puede estar relacionada con los objetos pertenecientes al mismo lote de producción.
- Una relación "social" puede ser creada cuando los objetos entran en contacto, de forma esporádica o continua, debido a que sus propietarios tienen contacto unos con otros durante sus vidas.
- Una relación de “co-propiedad” puede establecerse entre los objetos heterogéneos que pertenecen a un mismo usuario.

Se podrían considerar otros tipos de relaciones y clasificaciones, pero lo importante es el potencial que este tipo de paradigma implica para el desarrollo, sobre la base de estos “objetos sociales”, de aplicaciones al servicio de las personas inalcanzables por soluciones IoT no sociales.

Igualmente, como otra capacidad añadida, se pueden reutilizar los modelos diseñados para estudiar las redes sociales para abordar los problemas asociados al IoT, relacionados principalmente con la gestión de extensas redes de objetos interconectados.

Por tanto, la potencialidad e impacto que esta nueva aproximación ofrece a las comunicaciones M2M y M2H ha resultado en varias iniciativas que combinan los dos ecosistemas y destacan el importante reto que la comunidad científica tiene por delante [192], [193]. Otros autores, sin embargo, han centrado su interés en la planificación de las comunicaciones Ethernet para el Internet Industrial y las implicaciones de las interacciones H2M [194], [195].

En este contexto a continuación se presenta la concepción de una metodología basada en SIoT para un Sistema de Control de Subestaciones Industrial.

6.3 La RTU como representante del IoT en la Subestación

Como ya se ha comentado en el apartado 2.3, la RTU es un sistema embebido que actúa como elemento fundamental del Sistema de Automatización de la Subestación eléctrica en el ámbito de SmartGrid. La RTU, como se indica en [149], es el sistema embebido predominante en la Subestación eléctrica y el que en último término comunica con el SCADA del Centro de Control. Por tanto, es el claro representante de las “cosas” en la aplicación del concepto de IoT al ámbito de la Subestación eléctrica.

Así pues, se toma como punto de partida la arquitectura del Sistema de Automatización de Subestación descrita en el “Capítulo 5”, que se muestra en la Tabla 8.

Además de lo mostrado en dicha tabla, hay que tener en cuenta a los actores humanos que interactúan con la Subestación eléctrica. Éstos presentan distintos perfiles y roles en función de la situación en la red, funcionalidad y las características específicas de la Subestación con la que deben interactuar, además de su propia función.

Así, entre los actores y roles para la gestión y el mantenimiento de Subestaciones eléctricas destacan los siguientes [196], [197], [198], [199], [200], [201]:

Actor	**Rol**
Gerente de operaciones de la red	• Encargado de las labores de dirección, seguimiento, planificación, análisis, y ejecución de operaciones en la red. • Responsable de garantizar un servicio eléctrico seguro y confiable. • Puede haber varios gerentes, según el alcance de la operación, uno para cada tipo de red.
Encargado del centro de control	• Dirige al personal de operación desde un centro de control responsable de un grupo de Subestaciones y líneas de transmisión y/o distribución. • Realiza o dirige operaciones en los equipos de las Subestaciones a través de sistemas automatizados. Por ejemplo, conexión y desconexión de baterías y condensadores. • Inicia acciones correctivas en base a problemas comunicados y detectados. • Gestionan los picos de demanda y mantienen la calidad del servicio. • Trabajador cualificado, certificado por organismos u organizaciones pertinentes según sea necesario.
Operario del centro de control (técnico SCADA)	• Gestiona el estado de todas las Subestaciones desde un centro de control. • Encargado de controlar la carga del sistema, corregir problemas en la red y satisfacer la demanda. • Se centra en la supervisión y adquisición de datos.
Jefe de mantenimiento, técnico superior	• Se encarga de proporcionar dirección, asesoramiento y control en tareas específicas o múltiples. • Supervisa y asigna los recursos en base a las actuaciones y tareas pendientes. • Recibe actuaciones del centro de control.
Técnico de mantenimiento	• Determina el estado de funcionamiento de las Subestaciones. • Repara equipos defectuosos. • Comprueba registros e inspecciona los instrumentos y equipos. • Realiza informes de mantenimiento regularmente.

Tabla 13: Principales actores y funciones en la Subestación Eléctrica

Otros actores que también pueden intervenir en una Subestación eléctrica pueden ser:

Actor	Rol
Ingeniero/ técnico especialista	• Realiza las funciones de operación del sistema de energía, tales como la programación de la generación, la planificación de recursos, el análisis y el diseño de la formación de los operadores del sistema. • Coordina junto con otros departamentos el diseño y construcción de instalaciones del sistema eléctrico. • Anticipa, y comunica condiciones, tendencias y acciones correctivas en las áreas operativas. • Resuelve desafíos y problemas técnicos.
Ingeniero/técnico de aplicación	• Se centran en aplicaciones en tiempo real tales como la estimación del estado, análisis de contingencia, la estabilidad del voltaje y la estabilidad transitoria.
Técnico de calidad	• Asegurar el cumplimiento de los estándares, normas, reglamentos y procedimientos en materia de salud ocupacional, medio ambiente y seguridad industrial. • Identificar y evaluar los riesgos profesionales derivados de los trabajos en presencia de tensión eléctrica.
Responsable de comunicaciones	• Dirige la gestión de la red de comunicaciones del sistema eléctrico.
Ingeniero/técnico de comunicaciones	• Se centra en la administración de servidores, cortafuegos, comunicaciones y equipos de control en el tiempo real.
Ingeniero/técnico de simulación	• Se centra en el testeo a través de aplicaciones de simulación. • Forma parte del centro de control.
Responsable de seguridad	• Encargado de vigilar una Subestación.
Personal de retén	• Personal de guardia, realiza actuaciones de emergencia sobre una Subestación. • En esta categoría estaría incluido el equipo contraincendios específico de la empresa.
Encargado de limpieza	• Realiza actuaciones de limpieza periódica en la Subestación.
Encargado de ampliación/adecuación	• Realiza actuaciones para reforma o ampliación de las instalaciones de una Subestación.
Encargado de desherbado	• Realiza actuaciones para limpieza de vegetación en la Subestación.
Encargado de desratización	• Realiza actuaciones para limpieza y prevención de roedores en la Subestación.

Actor	Rol
Encargado de mantenimiento manual	• Realiza actuaciones para el mantenimiento físico sobre ciertos componentes de la Subestación. Por ejemplo, revisión del aceite del transformador.

Tabla 14: Otros actores y funciones en la Subestación Eléctrica

Por tanto, nos encontramos ante un escenario en donde primero se aplica el concepto de IoT al Sistema de Automatización de Subestaciones, donde la RTU ejerce como el representante de las "cosas" del mundo del IoT, segundo se listan los principales roles y funciones de los humanos que interactúan con la Subestación, y finalmente se aplica al conjunto el concepto de SIoT, a través de las Redes Sociales como se desarrolla en el siguiente apartado. A continuación se ilustra lo comentado (ver Figura 50):

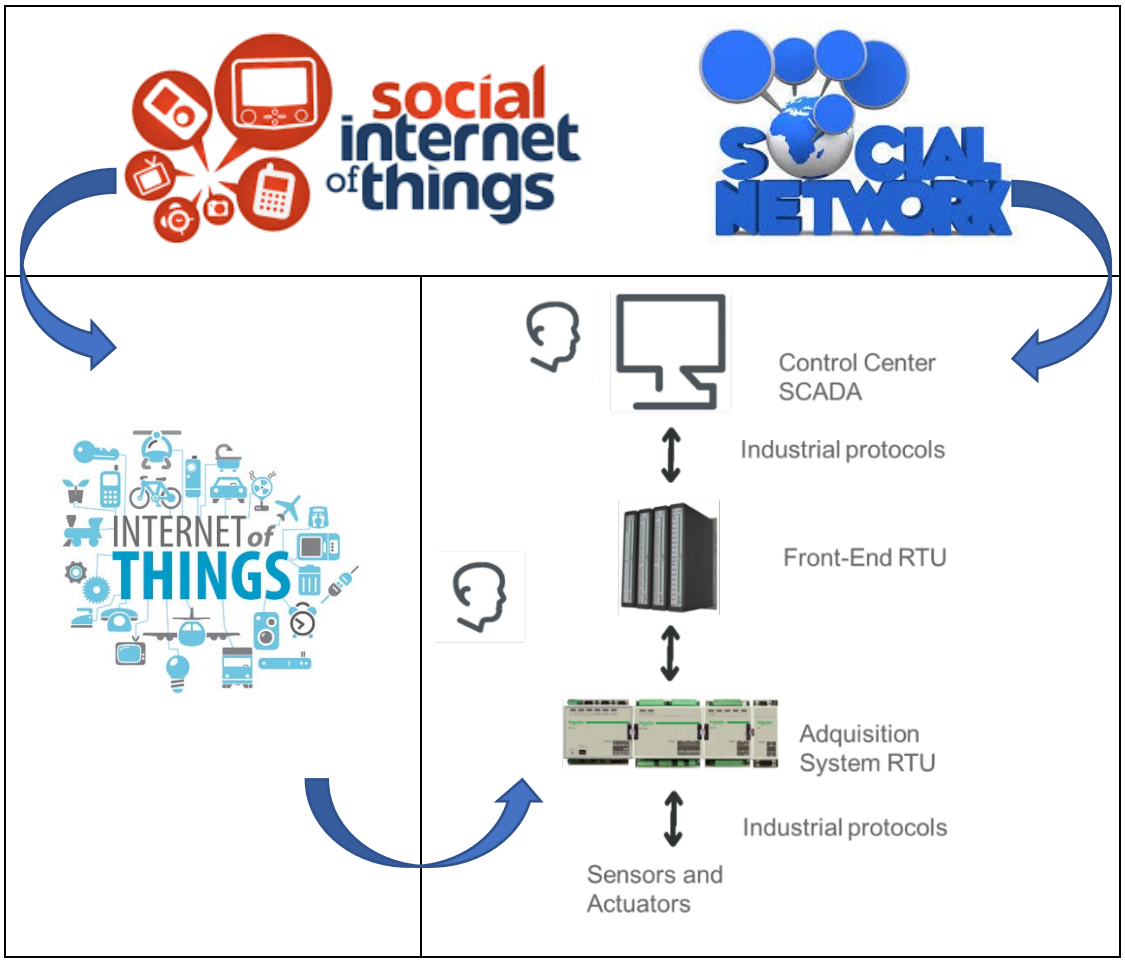

Figura 50: SIoT aplicado a la RTU de IoT y sus actores humanos.

6.4 Aproximación basada en SIoT

Ante el escenario presentado, la aproximación propuesta para probar el concepto de un nuevo modelo de interacción entre la RTU y el usuario de Subestación se basa en el uso de las Redes Sociales como habilitadores tecnológicos. Este entorno permite el establecimiento de jerarquías entre los dispositivos de acuerdo con los perfiles, y proporciona comunicación bidireccional en un lenguaje natural con los usuarios.

Para dicha prueba de concepto, la RTU podrá actuar como Front-end (concentrador de datos) y actuar a nivel de campo como unidad de adquisición en un nivel jerárquico inferior, como se puede observar en la Figura 51.

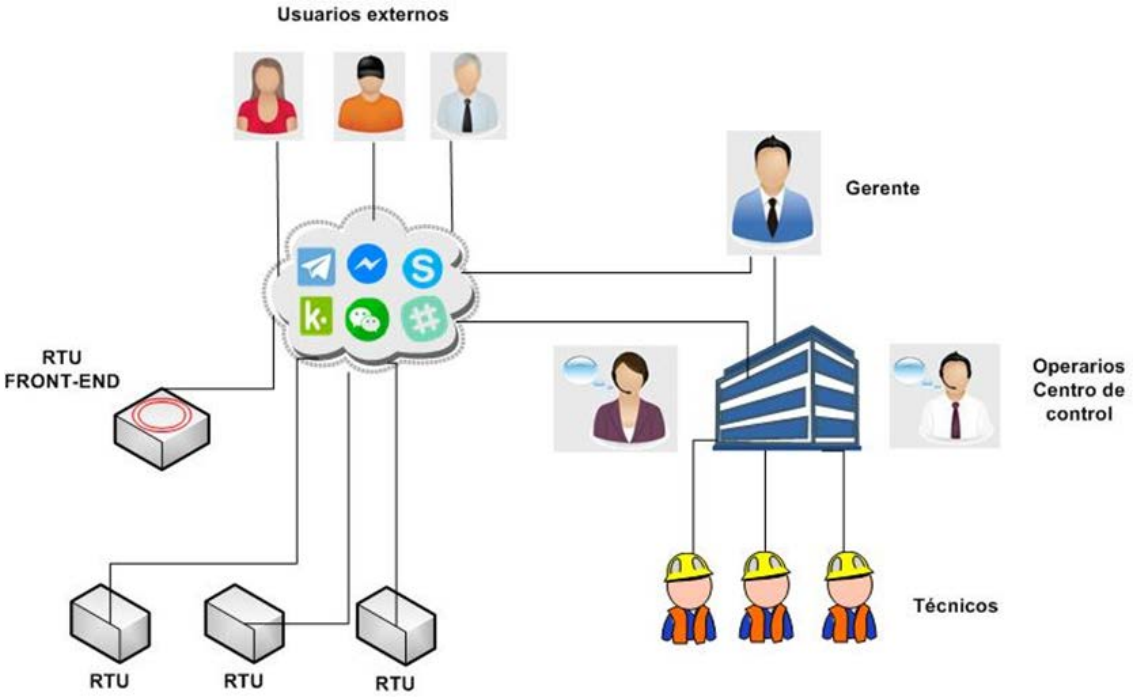

Figura 51: Ilustración de la prueba de concepto, en la que se representan los distintos grupos de humanos que se relacionan con las RTUs de la Subestación eléctrica, tanto de Front-end como de adquisición, a través de las Redes Sociales. [Fuente: Proyecto SAGRA [186]]

Desde el punto de vista del usuario, habrá usuarios profesionales (por ejemplo, responsables de la gestión, operación, mantenimiento y seguridad de la Subestación) y usuarios no profesionales, interesados en ciertos datos genéricos y rendimiento de las Subestaciones eléctricas. En este caso, el uso del paradigma SIoT ofrece la posibilidad de proporcionar a los usuarios no profesionales información general y no sensible.

A continuación se describen genéricamente los procesos necesarios para la implementación:

A) Conexión con la Red Social

En primer lugar, es necesario registrar las RTUs en la Red Social seleccionada, lo que se realiza a través de un proceso de autenticación propio de cada Red Social. Una

vez que la RTU se conecta, se asigna a cada una de ellas un identificador de usuario en la Red Social y a partir de ese momento las RTUs dispondrán de sus correspondientes perfiles. Se representa a continuación el proceso de conexión:

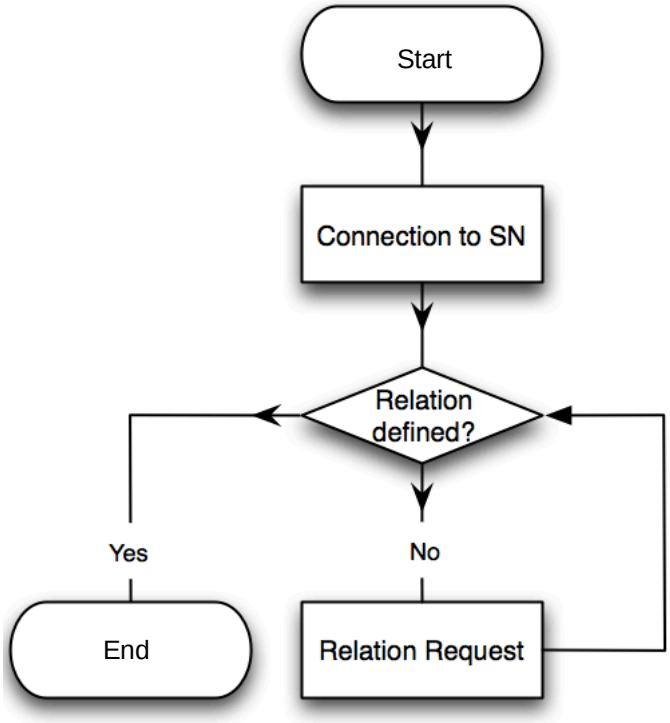

Figura 52: Diagrama de conexión con la Red Social.

B) Solicitud de relación

Posteriormente, es necesario establecer la comunicación entre RTUs y usuarios humanos, por lo que una petición de relación o seguimiento debe ser generada y enviada a la RTU o al usuario dependiendo del tipo de escenario y el tipo de gestión. Para tal fin se utilizan las herramientas y funciones de descubrimiento de las distintas Redes Sociales.

Para lograr una comunicación bidireccional entre los dispositivos (ya sea de las RTUs concentradores o unidades de adquisición) y los usuarios, se requiere realizar una solicitud de relación. Este proceso, que se ilustra seguidamente, consiste en verificar nuevas solicitudes y la fiabilidad de su origen, procediendo luego a aceptarlas o rechazarlas. Es importante resaltar que, en este paso, se requiere una simple verificación de la identificación de usuario para ser considerado como un dispositivo confiable.

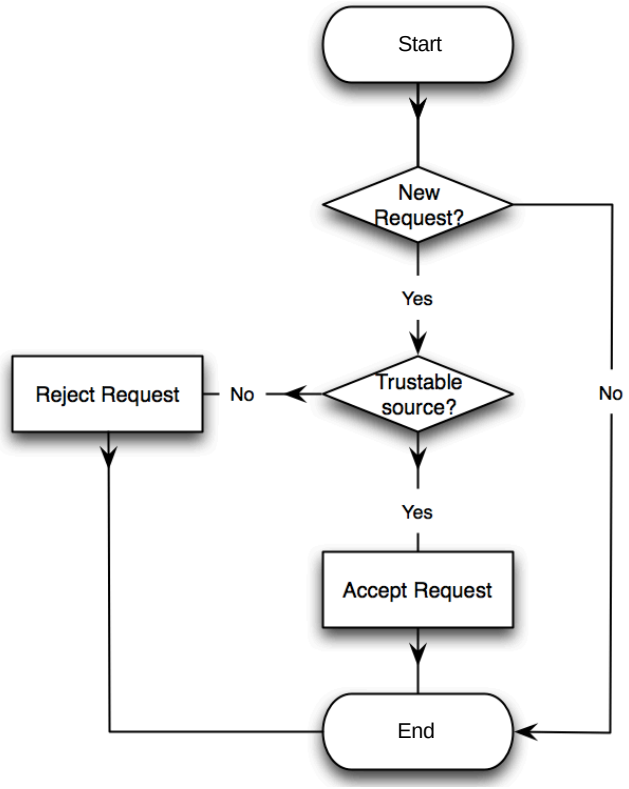

Figura 53: Diagrama de solicitud de relación.

C) Mensajes

Una vez establecida la relación entre los usuarios y los dispositivos, y entre los dispositivos, las RTU de adquisición podrán enviar datos a las RTU de Front-end como se ilustra a continuación:

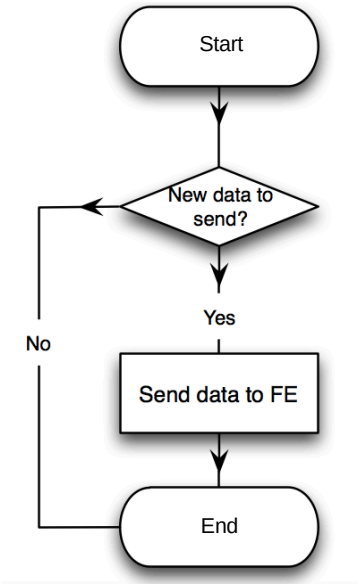

Figura 54: Diagrama de solicitud de mensajes al Front-end (FE).

A su vez, las RTUs realizarán el procesamiento de mensajes que consiste en responder a dichos mensajes o realizar acciones, si esos mensajes provienen de un usuario de confianza. Entre los mensajes de respuesta, podrían encontrarse, por ejemplo, la notificación del estado de la RTU, alarmas o eventos. En lo que respecta a las acciones, podrían ser por ejemplo comandos para accionar actuadores.

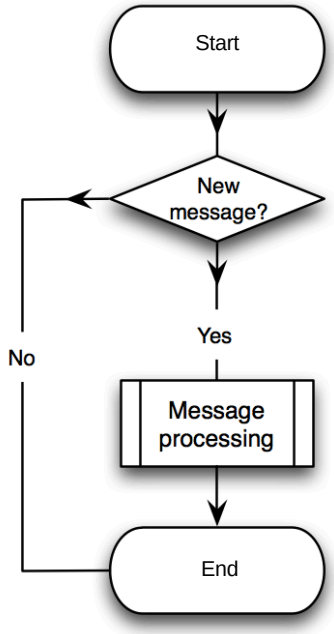

Figura 55: Diagrama de procesamiento de mensajes.

D) Lenguaje Natural

Además, las RTU están equipadas con un procesador de lenguaje natural, muy simple pero suficiente para demostrar el potencial, que permite la interpretación de mensajes de las Redes Sociales y la publicación automática de información en la misma, proporcionando una abstracción total para los usuarios.

6.5 Prueba de concepto con la Red Social Twitter

En esta sección se describe la implementación de la prueba de concepto en una Red Social como Twitter [202]. Twitter es una red social basada en microblogging. Este concepto consiste en la realización de blogs con entradas limitadas en tamaño. En concreto Twitter establecía el límite de caracteres en 140 pero en 2017 lo amplió a 280 caracteres. Las entradas que publican los usuarios en Twitter se llaman tweets (del inglés to tweet, piar). Estos mensajes pueden ser vitaminados con enlaces, multimedia, posición geográfica y otros contenidos. Dentro de Twitter los mensajes se organizan en líneas temporales, timelines.

A nivel personal un usuario emplea Twiter para mantenerse informado sobre las últimas novedades de los temas y personas que le interesan. Los usuarios también lanzan

información que ellos mismos producen. Además, pueden promocionar otros tweets marcándolos como favoritos o haciendo que sean vistos por los usuarios que los siguen. A nivel profesional Twitter es empleado como medio de promoción de productos y servicios. También es posible usarlo como fuente de información para el análisis de opinión sobre algún tema o para hacer análisis de mercado.

Los usuarios se relacionan en Twitter mediante la acción seguir, si un usuario sigue a otro, el primero verá en su timeline todos los tweets que el segundo escriba, así como los que este promocione haciendo retweet. El hecho de seguir es una suscripción en un sentido. El usuario seguido no tiene porqué seguir recíprocamente al usuario seguidor. Si un usuario cuenta con muchos seguidores significa que hay mucha gente interesada en la información que publica. Otra forma adicional de relación son las menciones, un usuario puede mencionar a otro en un tweet, si hace esto, el usuario citado recibirá una notificación.

Una forma de organizar tweets sin depender de los usuarios que los originan son las etiquetas o hashtags. Al escribir un tweet es posible marcarlo con una de estas etiquetas. Existen listan con las etiquetas más repetidas en el momento, lo cual puede dar una idea de los temas más candentes de la actualidad.

En cuanto a la privacidad, la filosofía de Twitter está orientada a que todo sea público para quien quiera verlo. No obstante, existe la posibilidad de hacer una cuenta privada. En ese caso la información que se lanza a través de esa cuenta sólo puede ser vista por las personas autorizadas. También existe la posibilidad de bloquear a usuarios concretos.

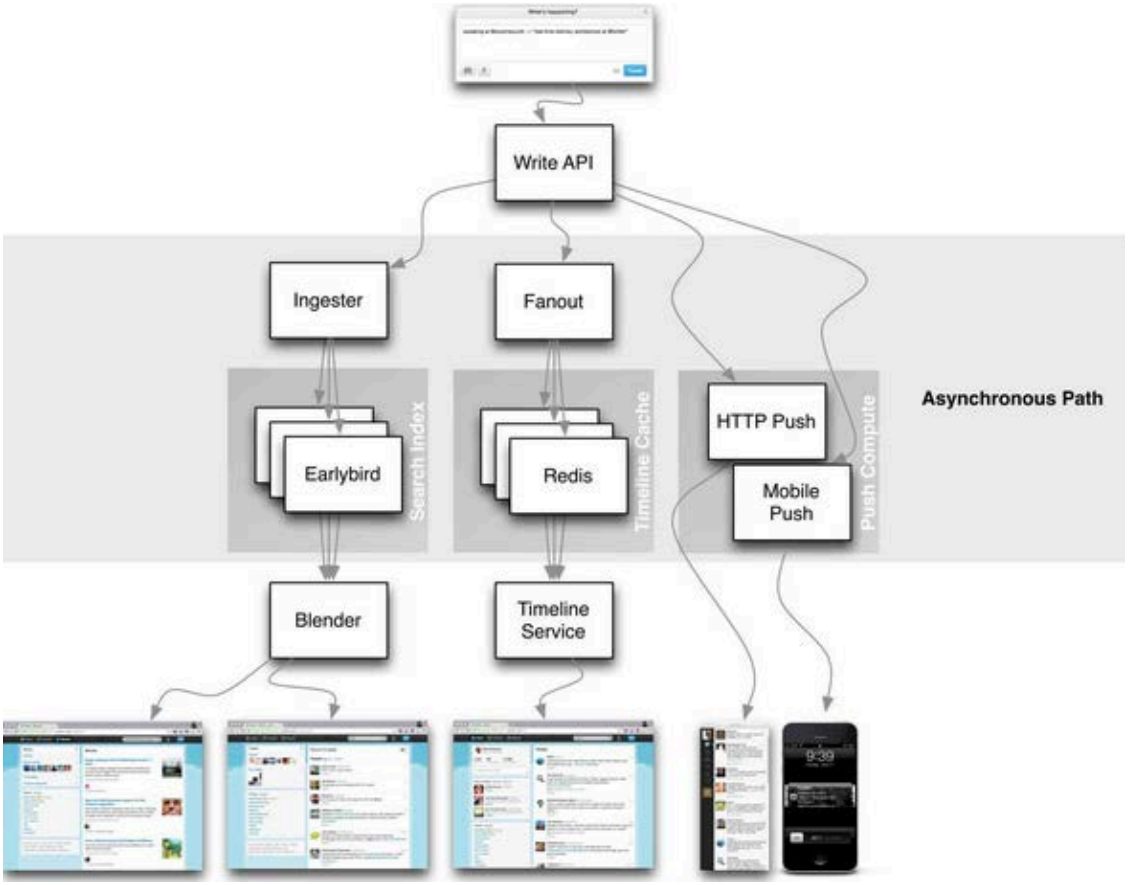

Figura 56: Arquitectura de Twitter. [Fuente: Highscalability [205]]

En Twitter se presume de ser totalmente open-source [203]. Desde su web se puede acceder a todos los módulos software que han realizado. Los timelines se almacenan en un clúster Redis [204]. Redis es un servidor de estructuras de datos muy avanzado y de alta carga. El flujo de entrada de tweets también es dirigido al Search Index. Este es el índice de búsquedas de Twitter. La información no se vuelca sin más, sino que hay un elemento a la entrada llamado Ingester que procesa la información para hacer que la indexación sea inteligente. La información es almacenada en Early Bird, que mantiene en RAM el índice completo. Conectado a este elemento hay otro llamado Blender, que recrea el timeline de las búsquedas. En la Figura 56 se presenta su arquitectura [205].

Así pues, la prueba de concepto diseñada explota las funcionalidades y características de Twitter, siendo dependiente totalmente de su implementación en campos tan críticos como la seguridad y privacidad. Sin embargo, lo más relevante es que hace uso de su interfaz, que es simple y amigable, su capacidad de escalado y su penetración a nivel mundial.

Una vez expuestas básicamente las características de Twitter, a continuación se describe la implementación realizada, en la que se dispone de tres cuentas en Twitter. La primera asociada a un usuario humano, la segunda asociada a una RTU Front-end y la tercera a una RTU de adquisición. La cuenta del usuario humano sigue a la RTU Front-end y esta a su vez sigue al humano y a la RTU de adquisición, y esta última sigue a la RTU Front-end. En la siguiente figura se ilustra la cadena de seguimiento entre los distintos elementos.

Figura 57: Representa las cuentas de Twitter y las relaciones de seguimiento que se indican con las flechas.

Las cuentas de usuario y Front-end se configuran como públicas y sus mensajes son visibles por todo aquel que haya sido aceptado para seguirlas. Por el contrario, la cuenta de la RTU de adquisición se configura como privada, solo se permite ser seguida por la RTU Front-end y los mensajes son siempre y únicamente privados, con objeto de mantener confidencial la información que se recibe de los sensores de la Subestación y solamente publicar a nivel de RTU Front-end la información que se considere que no es sensible.

Para disponer de dichas cuentas, en el caso de las RTUs, es necesario que el instalador de las RTUs obtenga las claves para el uso de la API de Twitter denominado “Access Token”. Este proceso se basa en el estándar abierto que permite flujos simples de autorización para sitios web o aplicaciones informáticas OAuth [206], en concreto PIN-Based OAuth.

El proceso de login para cada RTU se presenta seguidamente como se muestra en la Figura 58.

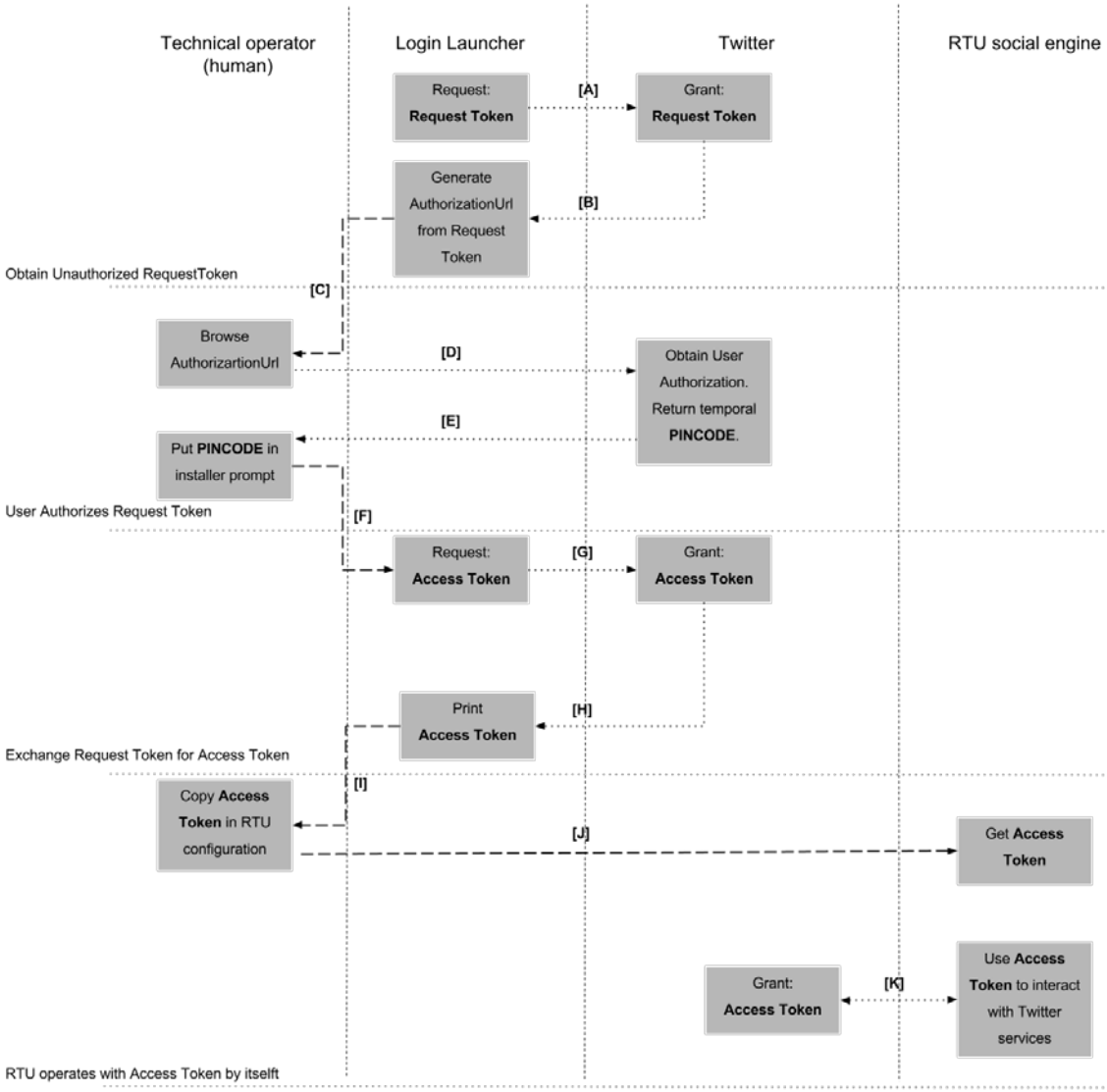

Figura 58: Login RTU en Twitter. [Fuente: Proyecto INFIERE [185]]

- Se ejecuta en un PC el proceso para login (Login Launcher).
- [A] El programa solicita a Twitter un “Request Token”. La petición incluye su “Consumer key”. “Consumer key” es una pareja de claves asimétricas (clave pública y clave privada) que identifican y autentican al proveedor de la aplicación. Cada aplicación que hace uso de la API de Twitter tiene un “Consumer key” que la identifica.
- El servicio Twitter responde [B] con una pareja de claves temporales “Request Token” y “Request Token Secret”. Esta pareja de claves es un “token” temporal para mantener una referencia a un intento de autorización de uso de la API en cuestión.
- El programa genera una URL de autenticación con el “Request Token” que corresponde.
- El usuario utiliza la URL indicada y le dirige a la página acceso de login de Twitter [C]. Se debe iniciar sesión con las credenciales de la cuenta de la RTU (o crear una nueva cuenta). En este momento del proceso, se pregunta si se permite que la aplicación “Twitter for RTU” haga cambios en su nombre, pudiendo aceptar o cancelar el proceso. En caso de aceptar, el navegador enviará la solicitud al servidor de Twitter [D].
- Si el login es correcto y el usuario ha aceptado, Twitter le asignará un código numérico (pincode) [E].
- En este punto, el usuario escribe el pincode asignado en el programa de login [F].
- El programa de login envía una petición [G] al servidor de Twitter en la que se le solicita un “Access Token” y como prueba de fidelidad le adjunta el pincode asignado anteriormente.
- Twitter genera una pareja “Access Token” y “Access Token Secret”. Esta pareja de claves es un token que identifica a una pareja de aplicación y usuario, y se usa para dar autenticidad a las peticiones y asegurar el intercambio de información con la plataforma. De esta forma se identifica de forma unívoca a esa instancia de aplicación para el usuario que ha hecho login y lo envía de vuelta [H].
- El programa imprime la pareja “Access Token” y “Access Token Secret” para que el operario las pueda copiar [I].
- Se configura esta pareja de tokens en la aplicación social de la RTU [J].
- La RTU puede interactuar con la API de Twitter por sí misma usando el “Access Token” [K].

Una vez hecho esto, se configura la cuenta de la RTU Front-end de manera que siga al usuario humano definido como “manager”. Antes de empezar su ciclo de eventos, la RTU debe esperar a que éste le siga de vuelta (lo que se conoce como “follow back” en la jerga Twitter). Cuando el humano siga a la RTU Front-end, ésta publicará su primer mensaje, en el que se presenta. Así, la RTU entra en el siguiente ciclo de operación.

Dicha operación se presenta en el diagrama de flujo que se muestra en la Figura 59.

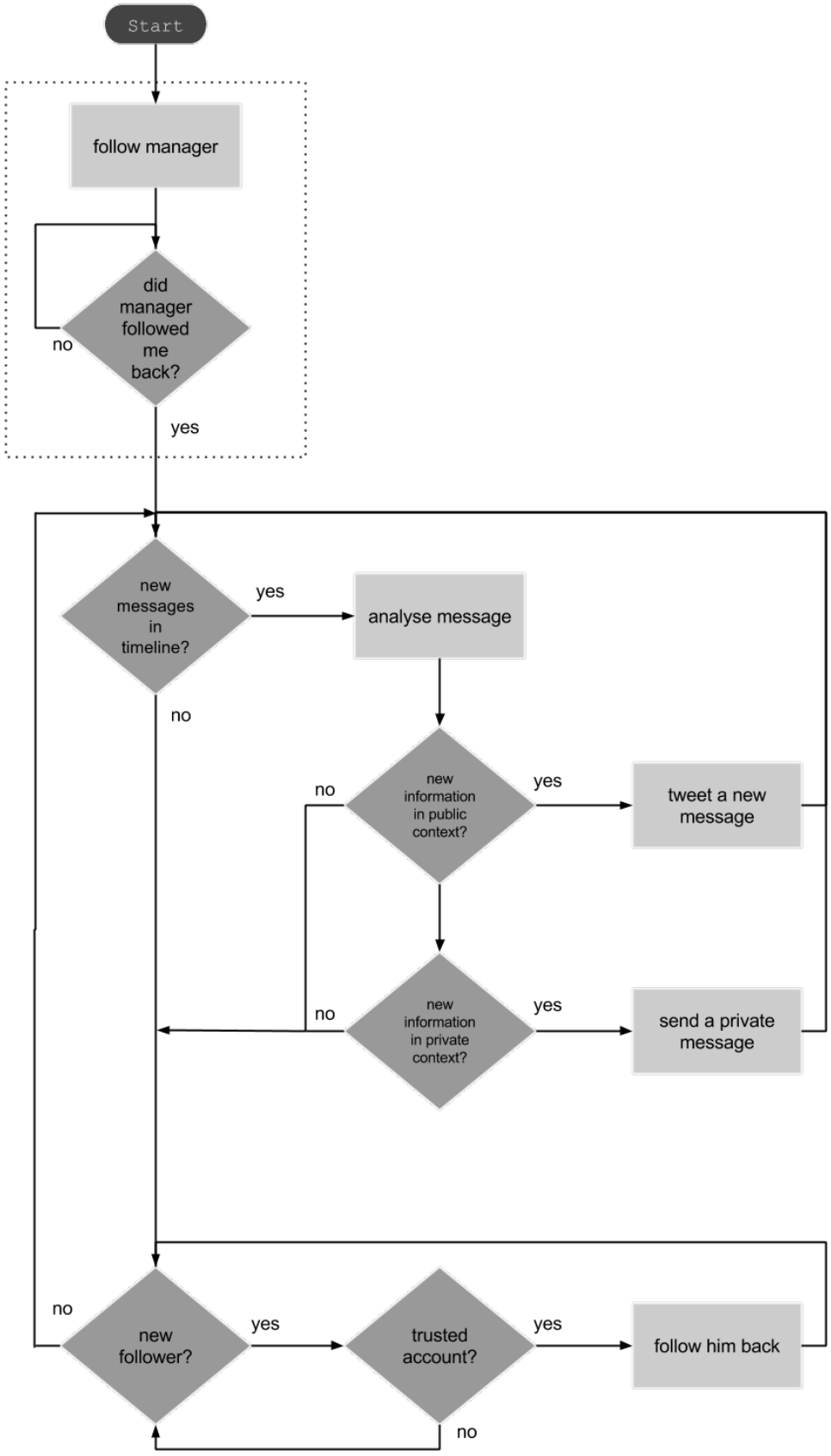

Figura 59: Diagrama del proceso de operación de la RTU FE en Twitter. [Fuente: Proyecto INFIERE [185]]

Se realizan las siguientes operaciones:

- Búsqueda de nuevos mensajes en sus timelines (timeline de menciones y timeline de mensajes directos).
- Cada nuevo mensaje es analizado y se comprueba si encaja en los patrones disponibles.
- Si el mensaje proporciona información de interés en un contexto público, se envía un nuevo tweet con dicha información en un lenguaje entendible por humanos a partir del diccionario en lenguaje natural disponible. El destinatario de este mensaje puede ser cualquier usuario común que siga a la cuenta del Front-end.
- Si el mensaje proporciona información de interés en un contexto privado, la aplicación envía un mensaje privado con dicha información en el que se referencia a todos los interesados, por ejemplo, el responsable de mantenimiento, de seguridad, gestión o incluso es posible mencionar a alguna otra RTU.
- Búsqueda de nuevos seguidores:
    - Para cada seguidor se realiza una comprobación de si es o no una cuenta de confianza.
    - Si el usuario es de confianza la RTU lo sigue en Twitter.

Por otro lado, la RTU de adquisición seguirá un proceso análogo. Una vez realizado el proceso de login, se configura la cuenta de la RTU de adquisición de manera que siga a la RTU Front-end. Antes de empezar su ciclo de eventos, la RTU debe esperar a que ésta le siga de vuelta. Cuando la RTU Front-end siga a la RTU de adquisición, ésta publicará su primer mensaje privado en el que se presenta. Así, la RTU entra en el siguiente ciclo de operación como se representa en la Figura 60.

En dicho ciclo se siguen los siguientes pasos:

- La aplicación interna conecta con la base de datos en tiempo real de la RTU, donde se registra la información del estado de sensores de la subestación.
- Cada nuevo dato es valorado y procesado por una lógica básica en la que se determina si el dato debe ser transmitido hacia un nivel superior, en este caso la RTU Front-end.
- En caso de que el dato deba ser enviado al Front-end, la operación se realiza usando para ello el sistema disponible de mensajes privados de Twitter. De esta forma la información de nivel de campo permanece restringida y es el Front-end el que, en función de las reglas que tiene programadas, remonta la información necesaria a cada grupo de humanos.
- En cuanto a la búsqueda de nuevos seguidores se procede de la misma forma que en el ciclo de operación mostrado anteriormente.

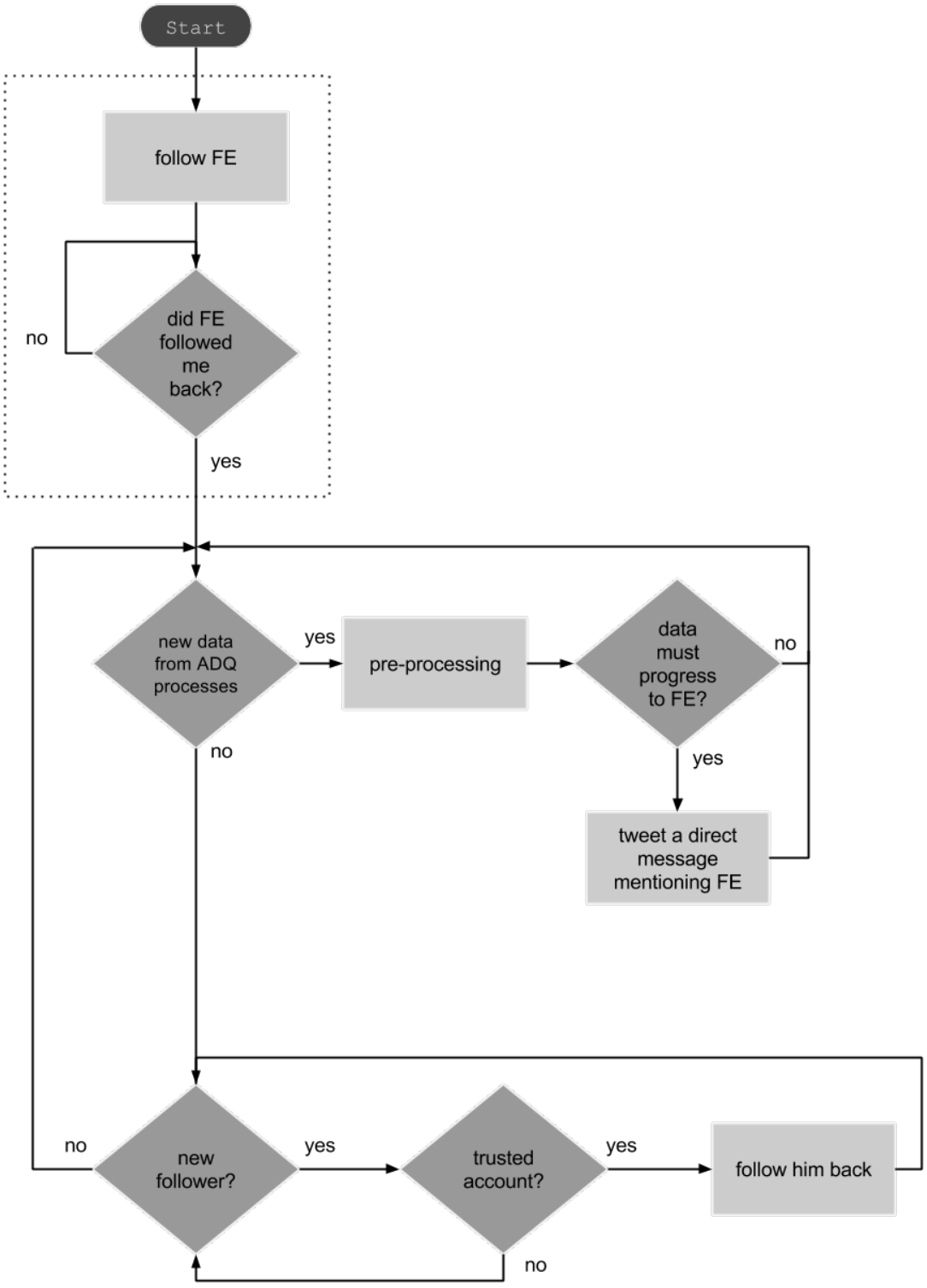

Figura 60: Diagrama del proceso de operación de la RTU de adquisición en Twitter. [Fuente: Proyecto INFIERE [185]]

A continuación se presentan las cuentas de Twitter de la RTU de adquisición y la RTU Front-end:

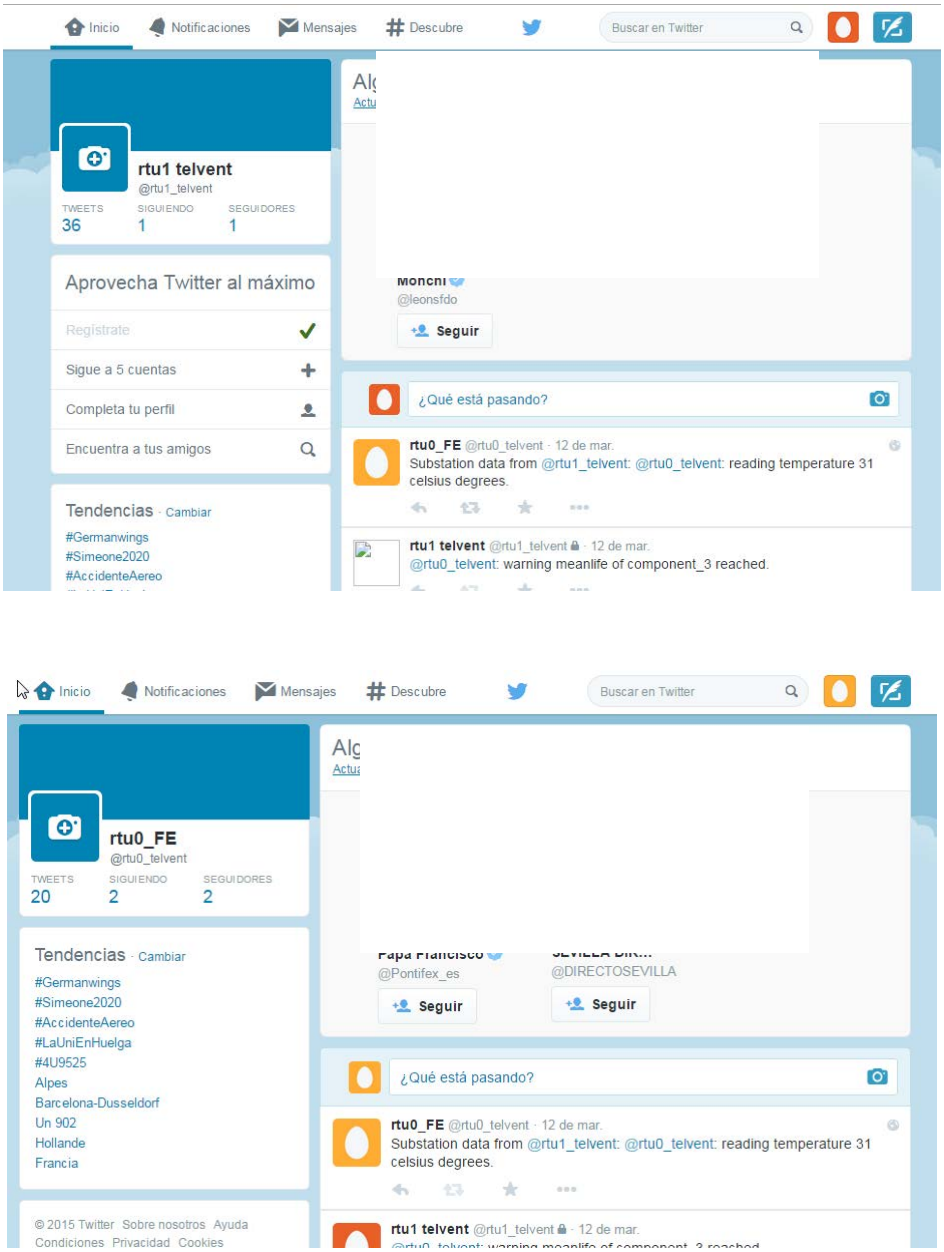

Figura 61: Cuenta de Twitter de la RTU de adquisición (arriba) y RTU Front-end (abajo).

Seguidamente se presentan ejemplos de los timelines de las cuentas de Twitter de la RTU Front-end y de la RTU de adquisición en la que se mantienen una conversación.

En la Figura 62 se muestra como la RTU de adquisición se presenta como “ADQ_RTU” con su número de serie y publica datos, en este caso de la temperatura. Dicha temperatura sube, lo que acaba originando una alarma por alta temperatura, “alert temperatura too high”. Además, publica un aviso sobre la vida media de un componente “warning meanlife of component_3 reached”.

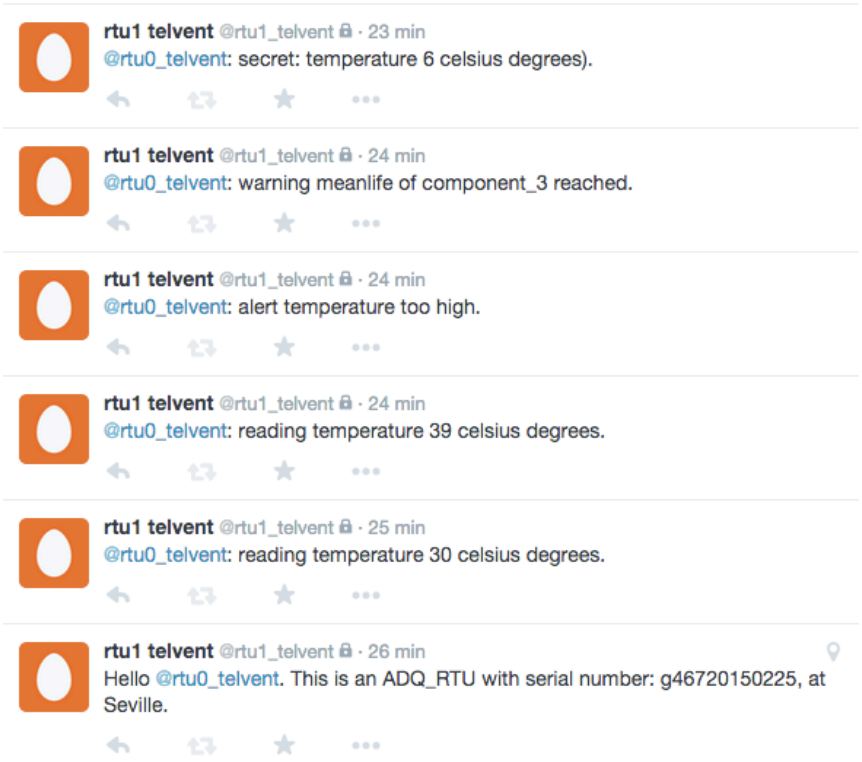

Figura 62: Ejemplo de timeline de la RTU de adquisición.

Por otro lado, en la Figura 63 se muestra como la RTU Fron-end reporta al usuario humano, en este caso “@dev_gie”, la alarma que ha generado la RTU de adquisición, tratándola como una situación peligrosa y además indica al usuario quién es y dónde está localizada, en este caso “frontend from substation_1 at Sevilla”.

En los timelines de la Figura 62 y de la Figura 63, se muestra cómo se mantiene una conversación básica y cómo se transmiten datos, alarmas y avisos. Esta información llegaría directamente al dispositivo móvil (smartphone, Tablet) o al ordenador del usuario humano que esté siguiendo al Front-end.

Además, en esta prueba de concepto se demuestra que también es posible la ejecución de comandos definidos por el usuario humano. Dichos comandos son enviados por el usuario humano a la RTU Front-end que los procesa y envía a la RTU de adquisición para que ésta los ejecute por medio de los actuadores.

Para que los comandos se traduzcan en cambios del estado de los actuadores, la RTU de adquisición debe estar previamente configurada para recibir comandos y las salidas (analógicas o digitales) de la RTU deben estar conectas físicamente a los actuadores

Figura 63: Ejemplo de timeline de la RTU Front-end.

A continuación se representa dicha conversación, en la que el usuario humano "@dev_gie" ordena que se bajen las cargas "drop loads", lo cual es comunicado por la RTU de Front-end a la RTU de adquisición que termina ejecutando la orden.

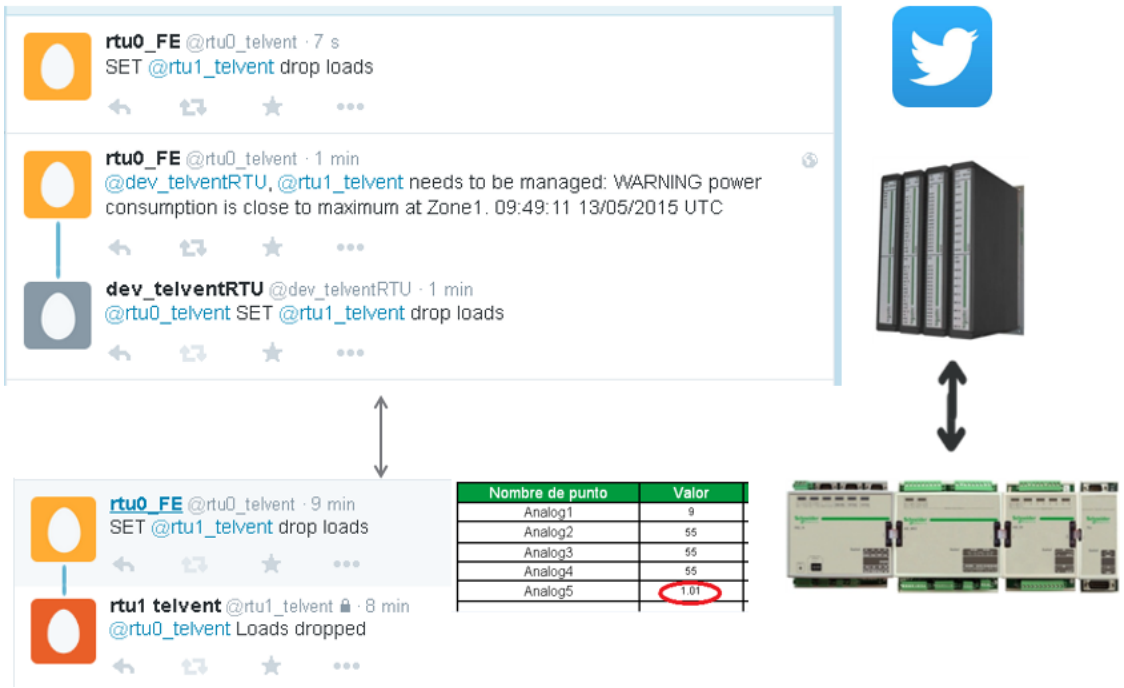

Figura 64: Ejemplo de timeline de ejecución de comandos.

Así pues, hemos visto como en un Sistema de Automatización de Subestación es posible utilizar una Red Social, en este caso Twitter, para el envío de información en los dos sentidos, desde la RTU de adquisición hasta el usuario humano y, al contrario.

Por tanto, se demuestra una alternativa usando las Redes Sociales a las comunicaciones clásicas a través de protocolos de comunicaciones industriales como los comentados en el apartado 2.3.2.1.

6.6 Conversaciones entre RTUs

Una vez demostrada la viabilidad de las comunicaciones a través de las Redes Sociales, el siguiente paso que se plantea es profundizar sobre el valor añadido que aporta comunicarse en lenguaje natural entre RTUs en Redes Sociales.

Dicho valor añadido surge como complemento a las comunicaciones industriales clásicas, ya que las RTUs continúan realizando sus misiones en la Subestación, comunicando con otras RTUs y el SCADA por protocolos industriales como IEC101, IEC104, DNP3 o Modbus.

Así pues, el trabajo de investigación se articula en torno a RTUs que siguen funcionando como se espera y que a su vez están dotadas de la capacidad de comunicarse en Redes Sociales y que interactúan entre ellas y con el usuario humano a través de las mismas.

A continuación se representa este tipo de RTUs en el que conviven lo que podemos denominar la parte “RTU clásica” y la parte “RTU SIoT”, y en el que existe un sistema de comunicación entre ambas partes.

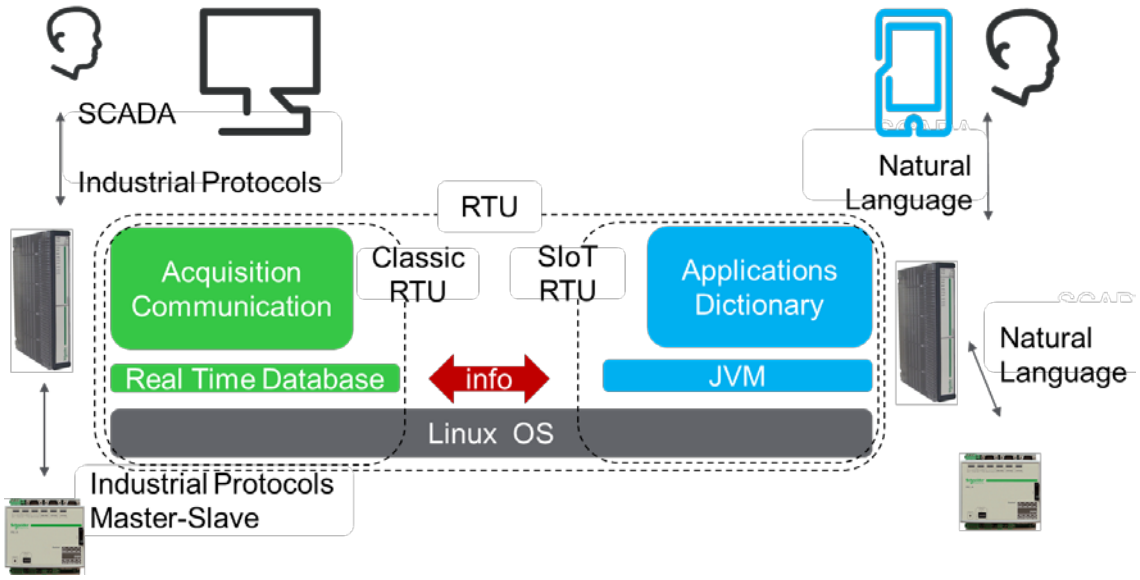

Figura 65: Representación de la parte clásica de la RTU (a la izquierda) que comunica por protocolos industriales maestro esclavo y la parte SIoT de la RTU (a la derecha) que comunica en lenguaje natural.

Como se puede observar en la Figura 65, la RTU clásica posee un sistema operativo Linux sobre el que básicamente se encuentra una base de datos en tiempo real, el software para la implementación de las comunicaciones por protocolos industriales y el software dedicado a la adquisición de entradas y salidas. Sobre el mismo sistema operativo y gracias a una máquina virtual Java (JVM, Java Virtual Machine), se implementa la nueva estructura para la RTU SIoT, que básicamente consta de un diccionario predefinido y las aplicaciones correspondientes de las Redes Sociales. Por último, se utiliza una aplicación para comunicar entre ambas partes.

Así pues, dotando a varias RTUs de la capacidad SIoT y utilizando Redes Sociales, las RTUs son capaces de dialogar con el usuario humano y entre ellas como se puede ver a continuación en donde se usa la aplicación de redes sociales Slack (https://slack.com/) [207]:

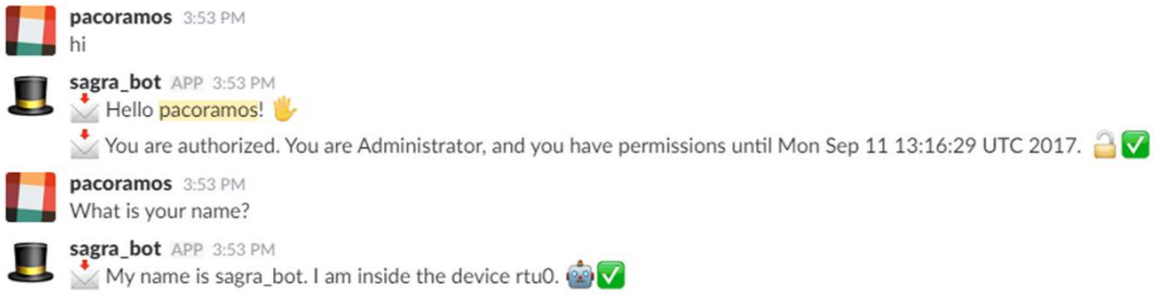

Figura 66: Usuario humano y RTU se presentan

A su vez, la RTU puede conocer otros dispositivos que están en el grupo de Slack con los cuales se pueden entablar conversaciones.

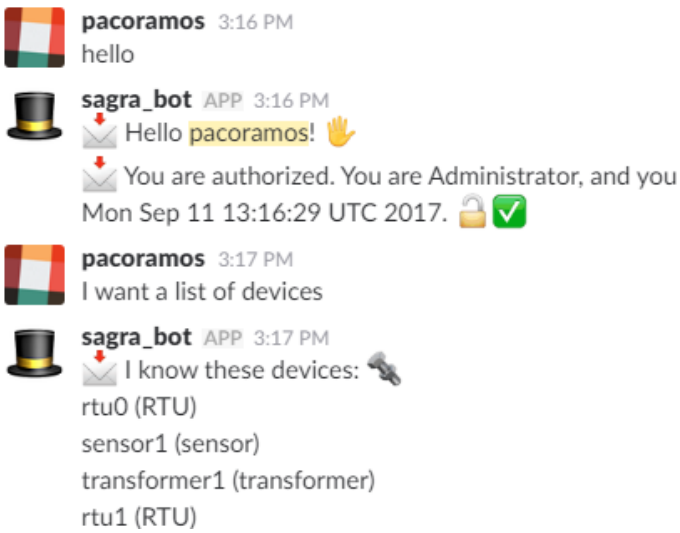

Figura 67: Usuario humano pregunta por los dispositivos que conoce la RTU en el grupo de Slack.

La posibilidad de dialogar en lenguaje natural entre RTUs en un mismo grupo de Slack en el que se encuentre el usuario humano permite al humano conocer el estado de los dispositivos de Subestación, y lo que es mejor aún le permite detectar incidencias sin necesidad de utilizar un sistema experto, simplemente siguiendo conversaciones entre RTUs.

Así pues, el potencial valor añadido de la comunicación en lenguaje natural entre RTUs se demuestra con distintos casos de uso en diferentes ámbitos de aplicación como, por ejemplo, mantenimiento, seguridad, depuración de fallos e incluso operación. Seguidamente se ilustran dos casos de uso, uno en el ámbito del mantenimiento y otro en el de la seguridad.

6.6.1 Caso de Uso de Mantenimiento

En el ámbito del mantenimiento, se plantean conversaciones en las que las RTUs son capaces ayudar al humano a detectar un problema en el grupo.

Se considera un escenario en el que es necesario realizar una actualización masiva de la versión del software de las RTUs de una Subestación, y en el que ambas versiones sean incompatibles. Ante el olvido de alguna actualización, las RTUs de la Red Social de la Subestación serían capaces de poner de manifiesto el problema para que el humano que forma parte del grupo de la Red Social de la Subestación pueda ser consciente del problema y realizar las acciones necesarias. A continuación se ilustra el escenario y la conversación.

Escenario:

- Una subestación que consta de RTUs que tienen un canal especifico de mantenimiento en la Red Social de la Subestación en el que se encuentra el operario de mantenimiento.
- Un protocolo que contiene un fallo crítico que debe ser actualizado.
- Las versiones del protocolo son incompatibles pudiendo provocar un fallo grave si convivieran en la misma subestación.

Usuarios que conversan en la Red Social de la Subestación:

- OM: Operario de mantenimiento.
- RTU1, RTU2, RTU3 a RTU99.

Conversación:

> 09h01 OM: Buenos días, os voy a actualizar el software del protocolo IEC104 que tiene un fallo crítico, os voy a poner la versión iec104v5.0.0
>
> 09h02 RTU1: De acuerdo, yo tengo la versión iec104v4.3.1
>
> 09h02 RTU2: OK por mí, yo también tengo la versión iec104v4.3.1

…….

09h02 RTU99: Me alegro de que me actualices, yo tengo la versión iec104v4.3.1

…….instalación en curso….

12h01 OM: Ya he terminado, por fin

12h01 OM: Por favor, comprobad que estáis actualizadas

12h03 RTU1: Hola a todas, estoy contenta con la nueva actualización iec104v5.0.0

12h03 RTU2: Genial, a mí me han actualizado a la versión iec104v5.0.0

12h03 RTU3: a mí también

…..

12h04 RTU13: yo tengo la versión iec104v4.3.1

12h05 OM: @RTU13, perdona, ha fallado tu actualización, la repito ahora

12h10 OM: ya está lista @RTU13, por favor confirma

12h11 RTU13: confirmado iec104v5.0.0

12h02 OM: Si no pasa nada extraordinario volveré según el plan establecido el próximo 19 de octubre

12h03 OM: Gracias, hasta pronto

12h03 RTU1: Gracias @OM, te esperamos para el 19.10.2018

12h04 RTU2: ¡Hasta pronto! Anotado el 19.10.2018

Este tipo de conversación resuelve una situación cuya detección, en la mayoría de las ocasiones, no sería posible hasta que un fallo la evidenciara. Típicamente cuando la RTU13 tuviera que comunicar en IEC104 con otra RTU con otra versión incompatible se produciría un fallo, y habría que realizar la correspondiente investigación para encontrar que no se había actualizado bien la RTU13, lo cual puede ser muy costoso en tiempo y dinero.

Se puede repetir la misma dinámica o muy similar en otras situaciones parecidas como, por ejemplo, realizar una calibración, los checklist de mantenimiento, la revisión de tensiones de alimentación, o incluso para verificar que la sincronización que se trató en el capítulo anterior es correcta.

En el caso de la sincronización de la fecha y la hora en los dispositivos de Subestación, una RTU podría resetearse y compartir con sus compañeras la fecha y la hora, mientras que las otras RTUs indicarían una fecha o una hora distinta a la publicada por la primera. De esta forma, la discusión pondría de manifiesto que existen distintas fechas y horas, y por tanto que existe un problema de sincronización.

6.6.2 Caso de Uso de Seguridad

En el ámbito de la seguridad se plantean conversaciones en las que RTUs ponen de manifiesto un ataque en el grupo de Redes Sociales. Es necesario comentar que, en este ámbito, existen sistemas de gestión de eventos e información de seguridad (SIEM Security Information and Event Management) que recolectan datos de la infraestructura a proteger, los analizan y correlacionan generando las correspondientes alertas de seguridad [208]. La gran potencia de los SIEM se encuentra en que son capaces de tener en cuenta eventos que, por su naturaleza, no representa en principio una amenaza de seguridad o que, analizados aisladamente, no presentan indicios de ser maliciosos.

El escenario se presenta de tal forma que la seguridad de la Subestación está siendo comprometida por un grupo de piratas informáticos, que lanzan dosificadamente ataques a una Subestación eléctrica. Para dichos ataques los piratas utilizarían vectores de ataque que solo se manifiestan a través de eventos que, analizados aisladamente, carecen de relativa importancia. Así pues, la detección de este tipo de ataques solo sería posible si se encuentran correlaciones entre varios de los eventos después de ser analizados por un experto o un SIEM, los cuales podrían reaccionar generando una alarma de seguridad después de haber encontrado dichas correlaciones entre eventos.

Escenario:

- Una subestación que consta de RTUs que tienen un canal especifico de seguridad en la Red Social de la Subestación en el que se encuentra el Jefe de Seguridad.
- Un grupo de piratas informáticos lanzando ataques a la subestación.

Usuarios que conversan en la Red Social de la Subestación:

- JS: Jefe de Seguridad (humano)
- RTU1, RTU2, RTU3 a RTU99.

Conversación:

09h02 RTU1: Hola a todas, alguien ha intentado usar el password por defecto dos veces, pero no ha conseguido entrar

09h02 RTU1: @JS pidió que se cambiaran todos los password en la última auditoría

09h03 RTU2: Intentaron acceder sin éxito un intento fallido y lo dejaron

……..

09h05 RTU13: Hola, han accedido a mi servidor web con el password por defecto

09h05 RTU13: @JS tengo el password por defecto todavía

……

09h07 RTU45: Detecto bastante tráfico

……

09h10 RTU21: he recibido comunicaciones por protocolo IEC104 con campos que no tengo configurados y no he podido procesarlo

…….

09h20 RTU13: @JS me están cambiando los privilegios

09h21 JS: Atentas todas, parece que estamos siendo atacados el centro de control os saca de servicio inmediatamente, gracias por la información

Aunque pudiera parecer sencillo, la detección de un ataque de estas características puede resultar muy complejo. Este tipo de conversación alerta sobre una situación crítica, cuya detección temprana puede evitar enormes problemas.

Además, personal que no necesita estar altamente cualificado en seguridad puede detectar un ataque. Esto contrasta con la complejidad y el importante coste económico de los SIEM, así como la necesidad de personal experto en seguridad que estos sistemas requieren.

Por otro lado, con estos ejemplos también se demuestra que la información se puede segmentar fácilmente por grupos o canales en las Redes Sociales. En los ejemplos bien se podrían tratar de dos grupos de discusión distintos en la misma Subestación, en este caso la información era un grupo de seguridad y otro de mantenimiento, pero podría haber, por ejemplo, otro para conversaciones de actualizaciones, de eficiencia energética o de sincronización, entre otros muchos posibles.

En definitiva, las conversaciones entre RTUs en lenguaje natural, siendo un complemento a la infraestructura de control existente, añaden valor de las siguientes formas:

1) Ofrecen las Redes Sociales y por tanto los Smarphones y Tablets como nueva interfaz de interacción con el Sistema de Automatización de Subestación frente a los SCADA.
2) Ponen al alcance de usuarios menos cualificados la información de lo que está sucediendo en los dispositivos de Subestación, al no necesitar conocer, por ejemplo, los protocolos industriales ni el manejo del SCADA.
3) El acceso a la información deja de ser solo local en la Subestación o centralizado en el SCADA para pasar a estar en los Smartphones del personal.
4) La información se puede segmentar fácilmente por canales o grupos de interés en función de cada necesidad concreta.

Por último, comentar que el resultado de la labor investigadora presentada en este capítulo ha dado lugar a la patente que se ha citado en el apartado 1.5.

6.7 Conclusiones

Se ha presentado un nuevo enfoque para la comunicación con las Subestaciones a través de las RTUs aplicando el paradigma de SIoT, que ofrece un nivel adicional de abstracción entre dispositivos y usuarios permitiendo la comunicación de los humanos con los dispositivos en lenguaje natural. Además, se abre la puerta a ofrecer información al público en general, lo que se ha denominado actores no profesionales.

La prueba de concepto presentada demuestra el potencial y las ventajas de la aplicación de SIoT al sector industrial, como es el caso del Sistema de Automatización de Subestación. El acceso a la información instantáneamente y de forma segmentada por parte del personal adecuado directamente en sus Smarphones es, sin lugar a duda, un importante valor añadido y complemento a los actuales sistemas.

Además, el que la información se presente en lenguaje natural supone la posibilidad de utilizar personal de menor cualificación, lo que representa otra ventaja para las empresas que operan en el sector eléctrico, al no tener que cualificar personal en “complicados” protocolos de comunicaciones industriales y sistemas SCADA entre otros.

Por último indicar, como se expondrá en el siguiente capítulo, que el siguiente paso natural en la investigación a este respecto es la utilización de inteligencia artificial para que los dispositivos puedan, por un lado, desarrollar conversaciones más naturales y por otro lado, reaccionar al entorno y sacar conclusiones de lo que se esté comentando en las conversaciones.

Capítulo 7. Conclusiones y Líneas Futuras

En la presente tesis se ha investigado sobre las RTUs como exponente fundamental de los sistemas embebidos en SmartGrid. Se han presentado contribuciones en distintos ámbitos que van desde los Sistemas de Protección y el estándar IEC61850, hasta los Sistemas de Sincronismo, pasando por los Sistemas de Gestión y Mantenimiento. En todos ellos, como se ha podido comprobar a lo largo de la investigación, la RTU juega un papel clave para el futuro de SmartGrid.

Se ha presentado un nuevo sistema de protección adaptativo que se ha probado y validado en subestaciones reales en Brescia (Italia). En dicho sistema se han demostrado las mejoras significativas, en términos de los índices SAIDI y SAIFI, que aporta la reconfiguración dinámica de los dispositivos de protección utilizados para implementar soluciones avanzadas de localización de faltas, aislamiento y restauración de servicio, para ello se ha hecho un uso novedoso del estándar IEC61850. Además, la mejora de dichos índices no solo hace que crezcan los beneficios de las eléctricas, sino que influye muy positivamente en las economías de empresas y países.

A su vez, se ha investigado sobre sistemas de automatización con alta disponibilidad y seguridad. Se han demostrado las bondades de la tecnología White-Rabbit para aumentar significativamente la precisión de la sincronización con arquitecturas redundantes y escalables. Además, se ha evaluado el nivel de seguridad, en sus dos acepciones (safety y security), de los dispositivos de subestaciones, aspecto de importancia fundamental para poder mejorar SmartGrid en el futuro.

Por último, se ha concebido una nueva forma de comunicación con las RTUs de Subestación usando Redes Sociales y lenguaje natural. La prueba de concepto presentada demuestra el potencial y las ventajas de la aplicación del Internet Social de las Cosas al Sistema de Automatización de Subestación. Gracias al Internet Social de las Cosas, el personal responsable puede acceder a información segmentada, instantáneamente y directamente en su Smarphone. Además, el que la información se presente en lenguaje natural supone la posibilidad de utilizar personal de menor cualificación, en dominios como el mantenimiento, pero también en dominios tan complejos como el de la ciberseguridad, lo que para las eléctricas se traducirá en un mercado laboral más amplio y una reducción del coste de las operaciones.

En lo que respecta al desarrollo futuro, se plantean varias posibles líneas de investigación derivadas de la presente tesis.

Los futuros sistemas embebidos de protección y los estándares de comunicación deben prever la integración de mecanismos para la reconfiguración remota y automática de los parámetros operacionales, permitiendo el correcto funcionamiento del sistema de automatización de la distribución sin interrupciones. De esta forma se presenta la oportunidad de investigar sobre mecanismos inteligentes de reconfiguración que tenga en cuenta el futuro nuevo escenario de alta penetración de renovables y microredes en el sistema eléctrico.

Al mismo tiempo, los progresos efectuados en la precisión de la sincronización en la Subestación abren la puerta a nuevas investigaciones para la mejora del sistema eléctrico. La posible aplicación e implantación de PMUs a nivel del sistema de distribución eléctrico, requerirán importantes avances en sincronización y redundancia para garantizar la confiabilidad del sistema.

Igualmente, ante la necesidad de mejorar la seguridad (safety y security), se plantea investigar en ambos aspectos simultáneamente desde las fases más tempranas del diseño de las RTUs en el dominio de la Subestación, en lo que sería safety y security co-design.

Además, teniendo en cuenta los importantes progresos que se están realizando en el ámbito de la Inteligencia Artificial se plantea su utilización en las RTUs. Así pues, gracias la Inteligencia Artificial, las RTUs, por un lado, podrían enriquecer su vocabulario y aprender a dialogar de forma más natural y, por otro lado, podría sacar sus propias conclusiones de lo que se esté comentando en las conversaciones, para lo cual será necesario investigar sobre técnicas de machine learning, modelos de toma de iniciativa y sobre estrategias para descifrar el entorno y los diálogos. Para ello, la utilización de técnicas de Inteligencia Artificial basadas en redes neuronales sería una alternativa a explorar.

Finalmente, dado que las RTUs son parte fundamental del sistema que vertebra la red eléctrica y que están ampliamente distribuidas por el mismo, otra de las líneas sobre la que avanzar sería la aplicación de la Inteligencia Artificial al concepto de control distribuido y toma de decisiones a nivel local, como contraposición a la toma de decisiones centralizada.

Capítulo 8. Referencias

[1] «Banco Mundial,» [En línea]. Available: https://blogs.worldbank.org/opendata/es/la-poblacion-mundial-en-el-futuro-en-cuatro-graficos.

[2] «Agencia Internacional de la Energía,» [En línea]. Available: https://www.iea.org/weo2017/.

[3] «Acción por el clima, Comisión Europea,» [En línea]. Available: https://ec.europa.eu/clima/citizens/eu_es .

[4] «Federal Energy Regulatory Commission. Assessment of Demand Response and Advanced Metering,» [En línea]. Available: http://www.ferc.gov/legal/staff-reports/12-08-demand-response.pdf .

[5] «European Technology Platform on Smartgrids,» [En línea]. Available: https://www.etip-snet.eu/ .

[6] «Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Redes inteligentes: de la innovación a la implantación,» 12.4.2011. [En línea]. Available: http://ec.europa.eu/transparency/regdoc/rep/1/2011/ES/1-2011-202-ES-F1-1.Pdf.

[7] «The Digital Transformation of Distribution Utilities 06/27/2017 By Jean-Yves Bodin Schneider Electric,» [En línea]. Available: http://www.elp.com/Electric-Light-Power-Newsletter/articles/2017/06/the-digital-transformation-of-distribution-utilities.html.

[8] «Powering an “always on” world,» [En línea]. Available: www.schneider-electric.com/smart-utility-ebook .

[9] «NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. Office of the National Coordinator for Smart Grid Interoperability,» U.S. Department of Commerce. National Institute of Standards and Technology.

[10] «The Future of Electricity New Technologies Transforming the Grid Edge,» Marzo 2017. [En línea]. Available: http://www3.weforum.org/docs/WEF_Future_of_Electricity_2017.pdf.

[11] «Estudio de Prospectiva: Tendencias y aplicaciones de los Sistemas Empotrados” del Observatorio de Prospectiva Tecnológica Industrial,» [En línea]. Available: http://www.opti.org/publicaciones/pdf/texto131.pdf.

[12] «Strategic Research Agenda (SRA). Artemis,» [En línea]. Available: https://artemis-ia.eu/publication/download/publication/541.

[13] «Tecnalia, certificación de smart meters,» [En línea]. Available: https://www.tecnalia.com/es/energia-medioambiente/noticias/tecnalia-lidera-la-certificacion-de-smart-meters.htm .

[14] «Prime Alliance,» [En línea]. Available: http://www.prime-alliance.org/.

[15] «G3 PLC alliance,» [En línea]. Available: http://www.g3-plc.com.

[16] «Meters and More,» [En línea]. Available: http://www.metersandmore.com/.

[17] Gordon R. Clarke, Deon Reynders, Edwin Wright, « Practical modern SCADA protocols: DNP3, 60870.5 and related systems Newnes,» ISBN 0-7506-5799-5 pages 19-21, 2004.

[18] «Manual de Usuario RTU Saitel, Schneider Electric,» [En línea]. Available: https://www.schneider-electric.com/en/product-range-download/61747-saitel#tabs-top.

[19] «Harmonization of CIM with IEC Standards: Draft Report for CIM and other IEC Working Groups.,» EPRI, Palo Alto, 2006.

[20] «International Electrotechnical Commission IEC 60870-5-101:2003 Telecontrol equipment and systems - Part 5-101: Transmission protocols - Companion standard for basic telecontrol tasks,» [En línea]. Available: http://www.iec.ch/.

[21] «International Electrotechnical Commission IEC 60870-5-04:2006+AMD1:2016 CSV Consolidated version Telecontrol equipment and systems - Part 5-104: Transmission protocols - Network access for IEC 60870-5-101 using standard transport profiles,» [En línea]. Available: http://www.iec.ch/.

[22] «International Electrotechnical Commission IEC 60870-5-103:1997 Telecontrol equipment and systems - Part 5-103: Transmission protocols - Companion standard for the informative interface of protection equipment,» [En línea]. Available: http://www.iec.ch/.

[23] «Distributed Network Protocol,» [En línea]. Available: https://www.dnp.org .

[24] «Modbus, Widely used serial fieldbus for all applications,» Schneider Electric, [En línea]. Available: https://www.schneider-electric.us/en/product-range-presentation/574-modbus/.

[25] «The Modbus Organization,» [En línea]. Available: http://www.modbus.org/.

[26] «International Electrotechnical Commission IEC 61131-3:2013 Programmable controllers - Part 3: Programming languages,» [En línea]. Available: http://www.iec.ch/ .

[27] «PLCopen,» [En línea]. Available: http://www.plcopen.org/.

[28] A. Dedè, d. Della Giustina, G. Massa, L. Cremaschini, «Toward a new standard for secondary substations: the viewpoint of a distribution utility,» IEEE Transactions on Power Delivery (2016) 1-10.

[29] «International Electrotechnical Commission IEC 61850:2017 SER Series Communication networks and systems for power utility automation,» [En línea]. Available: http://www.iec.ch/ .

[30] «Norma IEC 61850 Interoperabilidad para Protección Avanzada y Aplicaciones de Control Schneider Electric,» [En línea]. Available: https://www.schneider-electric.es/es/product-range-presentation/60793-norma-iec-61850/.

[31] «IEC61850 standard , part 8-1, Communication networks and systems insubstations, “Specific Communication Service Mapping (SCSM)-Mapping to MMS and to ISO/IEC 8802-3”, First edittion, 2004-05».

[32] Frei, Christian & Kostic, Tatjana, «Más allá de la primera impresión: IEC 61850, más que una mera norma de comunicación,» Revista ABB, ISSN 1013-3135, Nº 4, 2006, pags. 30-33, 2006.

[33] «International Electrotechnical Commission IEC 61850-6:2009 Communication networks and systems for power utility automation - Part 6: Configuration description language for communication in electrical substations related to IEDs,» [En línea]. Available: http://www.iec.ch/.

[34] S. Mohagheghi, J. Stoupis, Member and Z. Wang, «Communication Protocols and Networks for Power Systems- Current Status and Future Trends,» Conference: Conference: Power & Energy Society General Meeting, 2009. PES '09. IEEE, [En línea]. Available: https://www.researchgate.net.

[35] P. Parikh, I. Voloh, M. Mahony, «Fault Location, Isolation, and Service Restoration (FLISR) Technique using IEC 61850 GOOSE,» in Proc. Power and Energy Society General Meeting, (2013) 1-6.

[36] «IEC 61850-8-2, Communication networks and systems for power utility automation - Part 8-2: Specific Communication Service Mapping (SCSM) – Mapping to Extensible Messaging Presence Protocol (XMPP)».

[37] «IEC 61850-8-1, Communication networks and systems for power utility automation - Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO/IEC9506-1 and ISO/IEC 9506-2) - Ed.2».

[38] «IEC 61850-8-1 Communication networks and systems for power utility automation – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3,» 2011.

[39] «Introducción a los Sistemas de Control y Automatización y a la Problemática de Seguridad Asociada,» Instituto Nacional de Tecnologías de la comunicación S.A. 2014.

[40] «Smartgrid Core IEC Standards,» International Electrotechnical Commission, [En línea]. Available: http://www.iec.ch/smartgrid/standards/.

[41] «Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, IEC Std. 61508, 2010,» [En línea]. Available: http://www.iec.ch/functionalsafety/explained/ .

[42] «IEC 61508 Overview Report,» Exida, [En línea]. Available: http://www.win.tue.nl/~mvdbrand/courses/sse/1213/iec61508_overview.pdf.

[43] «IEC TR 62351-10:2012 Power systems management and associated information exchange - Data and communications security - Part 10: Security architecture guidelines».

[44] «IEC 62351:2018 SER Power systems management and associated information exchange - Data and communications security - ALL PARTS,» International Electrotechnical Commission, [En línea]. Available: https://webstore.iec.ch/publication/6912.

[45] «Standard for Intelligent Electronic Devices Cyber Security Capabilities, IEEE Std. 1686-2013, 2013,» [En línea]. Available: https://standards.ieee.org/findstds/standard/1686-2013.html .

[46] «Security for Internet Protocol,» [En línea]. Available: https://tools.ietf.org/html/rfc2401.

[47] «Creating Smart DISTRIBUTION through AUTOMATION,» Pacworld – Protection, Automation and Control World, [En línea]. Available: https://www.pacw.org/.

[48] «Brochure ADMS FLISR,» Schneider Electric, [En línea]. Available: https://infrastructurecommunity.schneider-electric.com/docs/DOC-4484.

[49] «White Paper– Data Communication in Substation Automation System (SAS) WP 1004HE,» Hirschmann , 2012 . [En línea]. Available: www.hirschmann.com.

[50] Hubert Kirrmann, Solutil, Switzerland and William Dickerson, Arbiter Systems, «Precision Time Protocol profile for power utility automation Application,» Inc, Canada, [En línea]. Available: https://www.pacw.org/.

[51] Luigi Atzori, Antonio Iera, Giacomo Morabito, «SIoT: Giving a Social Structure to the Internet of Things,» IEEE Communications Letters (Volume: 15, Issue: 11), November 2011.

[52] Kleinberg, J., «The small-world phenomenon: an algorithmic perspective,» in Proc. ACM Symposium on Theory and Computing, 2000.

[53] P. Scully, «Insights from ongoing research on IoT Platforms.,» [En línea]. Available: https://iot-analytics.com/5-things-know-about-iot-platform/.

[54] «PNNL VOLTTRON Specification,» [En línea]. Available: http://bgintegration.pnnl.gov/pdf/.

[55] «Duke Energy open source solution for smart grid,» [En línea]. Available: https://www.chartwellinc.com/duke-energy-creating-open-source-solution-for-the-smart-grid/.

[56] «New IEC 61850 Protocol - Mapping based on XMPP,» [En línea]. Available: https://www.pacw.org/.

[57] «RTI Connext DDS customers,» [En línea]. Available: https://www.rti.com/industries/energy.

[58] «IEC61850 companion specification for electrical substation automation systems,» [En línea]. Available: https://opcfoundation.org/markets-collaboration/iec61850/.

[59] «OPC UA Success Stories,» [En línea]. Available: https://jp.opcfoundation.org/wp-content/uploads/sites/2/2016/03/4_OPCDay2015_OPC-UA-SuccessStories.pdf.

[60] Yu Tian ,Zhenjiang Pang ,Weibin Wang ,Lizong Liu ,Dawei Wang, «Substation sensing monitoring system based on power,» Technology, Networking, Electronic and Automation Control Conference (ITNEC), 2017 IEEE 2nd Information, Diciembre 2017.

[61] «Azure electric customers,» [En línea]. Available: https://customers.microsoft.com/en-us/search?sq=&ff=story_industry%26>Power %26 Utilities%26%26story_product_categories%26>Cloud Platform&p=1&so=story_publish_date desc.

[62] «Fiware Succes Stories,» [En línea]. Available: https://www.fiware.org/success_stories/.

[63] Danah M. Boyd, Nicole B. Ellison, «Social Network Sites: Definition, History, and Scholarship,» Journal of Computer-Mediated Communication, Volume 13, Issue 1, 1 October 2007, Pages 210–230, https://doi.org/10.1111/j.1083-6101.2007.00393.x.

[64] I. Ponce, «Monográfico: Redes sociales,» Ministerio de Educación, Cultura y Deporte. Consultado el 28 de octubre de 2017, [En línea]. Available: http://recursostic.educacion.es/observatorio/web/ca/internet/web-20/1043-redes-sociales.

[65] «The 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining,» [En línea]. Available: http://asonam.cpsc.ucalgary.ca/2016/.

[66] «Mapa del uso de las redes sociales de internet en el 2017,» [En línea]. Available: https://norfipc.com/redes-sociales/mapa-uso-redes-sociales-internet.php.

[67] «Facebook's Secret Chat SDK Lets Developers Build Messenger Bots,» [En línea]. Available: http://techcrunch.com/2016/01/05/facebook-messenger-bots/.

[68] «Bots, the next frontier,» [En línea]. Available: http://www.economist.com/news/business-and-finance/21696477-market-apps-maturing-now-one-text-based-services-or-chatbots-looks-poised.

[69] «Forget Apps, Now The Bots Take Over,» [En línea]. Available: http://techcrunch.com/2015/09/29/forget-apps-now-the-bots-take-over/.

[70] «Most popular global mobile messenger apps as of January 2018, based on number of monthly active users (in millions),» [En línea]. Available: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/.

[71] «The Most Popular Messaging App in Every Country,» 2016. [En línea]. Available: https://www.similarweb.com/blog/worldwide-messaging-apps.

[72] Mg. Augusto Cortez Vásquez, Mg. Hugo Vega Huerta, Lic. Jaime Pariona Quispe, «Procesamiento de lenguaje natural,» Unv. Nacional Mayor de San Marcos y Unv. Ricardo Palma, [En línea]. Available: http://sisbib.unmsm.edu.pe/.

[73] «Procesamiento del Lenguaje Natural,» [En línea]. Available: http://www.vicomtech.org/t4/e11/procesamiento-del-lenguaje-natural.

[74] M. Hernández y J. Gómez, «Aplicaciones de Procesamiento de Lenguaje,» Revista Politécnica. Vol. 32, No. 1 . ISSN 1390-0129, pp. 87-96, 2013.

[75] «Natural Language for Developers,» [En línea]. Available: https://wit.ai.

[76] «Watson,» [En línea]. Available: http://www.ibm.com/watson/what-is-watson.html.

[77] «Azure. Language Understanding,» [En línea]. Available: https://azure.microsoft.com/es-es/services/cognitive-services/language-understanding-intelligent-service/.

[78] «General natural language facilities for node,» [En línea]. Available: https://github.com/NaturalNode/natural.

[79] «Natural Language Toolkit,» [En línea]. Available: http://www.nltk.org.

[80] «Apache OpenNLP,» [En línea]. Available: https://opennlp.apache.org.

[81] «The Stanford Natural Language Processing Group,» [En línea]. Available: http://nlp.stanford.edu/software.

[82] «LingPipe,» [En línea]. Available: http://alias-i.com/lingpipe.

[83] «IDE4L (Ideal Grid for All), financiado por la Comisión Europea en el programa FP7, Grant agreement: 608860,» [En línea]. Available: http://ide4l.eu/.

[84] G. K. Venayagamoorthy, «Smart grid and electric transportation,» , 12th International IEEE Conference on Intelligent Transportation Systems, pp. 1-2, October, 2009, St. Louis, MO, USA.

[85] N. Kanwar, N. Gupta, K. R. Niazi, A. Swarnkar, «An integrated approach for distributed resource allocation and network reconfiguration considering load diversity among customers,» Sustainable Energy, Grids and Networks 7 (2016) 37–46.

[86] G. Massa, G. Gross, V. Galdi, A. Piccolo, «Dispersed voltage control in microgrids,» IEEE Transactions on Power Systems 31 (5) (2016) 3950-3960.

[87] H. Zhan, C. Wang, Y. Wang, X. Yang, X. Zhang, C. Wu, Y. Chen, «Relay protection coordination integrated with optimal placement and sizing of distributed generation in distribution networks,» IEEE Transactions on Smart Grid 7 (1) (2016) 55-65.

[88] Gauci A, « Smart Grid Fault Location, Isolation, and Service Restoration (FLISR) Solutions to Manage Operational and Capital Expenditures,» [En línea]. Available: http://www.schneider-electric.ca/documents/solutions/FLISR.pdf.

[89] Ponemon Institute, «Cost of Data Center Outages,» 2016. [En línea]. Available: https://www.vertivco.com/globalassets/documents/reports/2016-cost-of-data-center-outages-11-11_51190_1.pdf.

[90] V. C. Nikolaidis, E. Papanikolaou, A. S. Safigianni, «A communication-assisted overcurrent protection scheme for radial distribution systems with distributed generation,» IEEE Transactions on Smart Grid, 7 (1) (2016) 114-123.

[91] Y. Chollot, J. Wild, T. Berry, A Jourdan, J. Houss, «Decentralized Self Healing Solution Tested in the Framework of GreenLys Smart Grid Project,» in Proc. IEEE PowerTech Conference (2013) 1-7.

[92] P. Balakrishna, K. Rajagopal, K. S. Swarup, «Application benefits of Distribution Automation and AMI systems convergence methodology for distribution power restoration analysis,» Sustainable Energy, Grids and Networks 2 (2015) 15–22.

[93] R. Uluski, B. Wojszczyk, H. Tram, «Distribution Automation - Smart Feeders in a Smart Grid World,» Utility University Course (UU304), DistribuTECH, 2009.

[94] T. Bensley, C. Grommesh y P. Stemborg, «Implementing new configurable self-healing smart grid technology with an existing distribution management system (DMS),» Cooper Power Systems (2011) 1-8.

[95] J. Romero Aguero, «Applying Self-Healing Schemes to Modern Power Distribution Systems,» in Proc. IEEE Power and Energy Society General Meeting (2012) 1-4.

[96] A. Ukil , B. Deck and V. H. Shah, «Smart distribution protection using current-onlydirectional overcurrent relay,» Proc. IEEE PES Conf. Innov. Smart Grid Technol. (ISGT '10).

[97] G. Zhang, Z.A Xu, « A new real-time negative and positive sequence components detecting method based on space vector,» IEEE Powe Enginneting Society Winter Meeting, Jan-Feb 2001, IEEE, 1: 275-280.

[98] J.A Jiang, J.Z Yang, Y.H Lin, C.W Liu, J.C Ma, «An adaptive PMU based fault detection/location technique for transmission lines.,» Theory and algorithms, IEEE Transactions on Power Delivery, April 2000, IEEE, 15 (2): 486-493.

[99] C. González de Miguel, T. De Rybel, J. Driesen, « Implementation of a digital directional Fault Passage Indicator,» 39th Annual Conference of the IEEE Industrial Electronics Society, IECON 2013, 10-13 Nov 2013, Vienna, Austria: 2075-2080.

[100] Lehtonen M, «Novel Techniques for Fault Location in Distribution Networks,» Power Quality and Supply Reliability Conference (PQ 2008); 2008 August 27-29; Parnu; IEEE; 199-204.

[101] Peretto L, Sasdelli R, Scala E, Tinarelli R, «A distributed Measurement System for Locating Transient-Voltage Sources,» Proceeding of the 23rd IEEE Instrumentation and Measurement Technology Conference (IMCT 2006); April 2006; Sorrento, Italy; IEEE; 200.

[102] Borghetti A, Bossetti M, Silvestro M Di, Nucci C.A, Paolone M, « Continuous-Wavelet Transform for Fault Location in Distribution Power Networks: Definition of Mother Wavelets Inferred from Fault Originated Transients,» IEEE Transactions on Power Systems.

[103] Prakash S, Gupta S.C, «Fuzzy Logic Based Trained Fault Locating Mechanism in Power Distribution Network,» International Journal of Emerging Technology and Advanced Engineering; July 2012; 2(7): 129-135.

[104] Dehghani F, Nezami H, «A New Fault Location Technique on Radial Distribution Systems Using Artificial Neural Network,» 22nd International Conference on Electricity Distribution (CIRED 2013); 2013 June 10-13; Stockholm; Paper 0375.

[105] Uluski, R.W., «Using distribution automation for a self-healing grid,» IEEE (2012) 1-5.

[106] D. Della Giustina, A. Dedè, G. Invernizzi, D. Pozo Valle, F. Franzoni,, «Smart Grid Automation Based on IEC 61850: An Experimental Characterization,» IEEE Transactions on Instrumentation and Measurement 64 (8) (2015) 2055-2063.

[107] D. Pala, C. Tornelli and G. Proserpio, «An adaptive, agent-based protection scheme for radial distribution networks based on IEC 61850 and IEC 61499,» in Proc. CIRED Workshop on Integration of Renewables into the Distribution Grid (2012) 1-4.

[108] «Energizing the digital grid, review 4, ABB, 2014,» [En línea]. Available: https://library.e.abb.com/.

[109] P. Jafary, S. Repo, and H. Koivisto, «Security solutions for smart grid feeder automation data communication,» In International Conference on Industrial Technology (ICIT 2016), IEEE, 2016, pp. 551-557.

[110] N. Kashyap, C. W. Yang, S. Sierla and P. G. Flikkema, «Automated Fault Location and Isolation in Distribution Grids With Distributed Control and Unreliable

Communication,» IEEE Transactions on Industrial Electronics, 62 (4) (2015) 2612-2619.

[111] D. Della Giustina, S. Rinaldi, « Hybrid Communication Network for the Smart Grid: Validation of a Field Test Experience,» IEEE Transactions on Power Delivery 30 (6) (2015) 2492-2500.

[112] F. Muzi, «Logic selectivity for an automatic reclosing and reconfiguration of electrical distribution systems,» In WSEAS International Conference on Information Technology and Computer Networks, 2012, pp. 10-12.

[113] T. Berry and L. Guise, «IEC61850 for distribution feeder automation,» IET International Conference on Resilience of Transmission and Distribution Networks (RTDN) 2015. IET, 2015.

[114] C. Kalalas, L. Gkatzikis, C. Fischione, P. Ljungberg and J. Alonso-Zarate, «Enabling IEC 61850 communication services over public LTE infrastructure,» 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, 2016, pp. 1-6.

[115] L. Huchel, H. H. Zeineldin, «Planning the coordination of directional overcurrent relays for distribution systems considering DG,» IEEE Transactions on Smart Grid, 7 (3) 1642-1649.

[116] «Directiva 96/92/CE del Parlamento Europeo y del Consejo de 19 de diciembre de 1996 sobre normas comunes para el mercado interior de la electricidad,» [En línea]. Available: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex:31996L0092.

[117] «IEC TR 62689-100:2016. Current and voltage sensors or detectors, to be used for fault passage indication purposes - Part 100: Requirements and proposals for the IEC 61850 series data model extensions to support fault passage indicators applications».

[118] Dede, A.; Della Giustina, D.; Franzoni, F.; Pegoiani, A., «IEC 61850-based logic selectivity scheme for the MV distribution network,» Applied Measurements for Power Systems Proceedings (AMPS) 2014 IEEE International Workshop on, vol., no., pp.1,5, 2.

[119] S. Lu, S. Repo, D. Della Giustina, «Standard-based Secondary Substation AutomationUnit–the ICT Perspective,» in Proc. 5th IEEE PES Innovative Smart Grid Technologies (ISGT Europe) (2014) 1-6.

[120] «Layer 2 Tunneling Protocol version 3.,» [En línea]. Available: https://tools.ietf.org/html/rfc3931.

[121] «CISCO 892 router,» [En línea]. Available: https://www.cisco.com/c/en/us/support/routers/892-integrated-services-router-isr/model.html.

[122] «CISCO 819 4G/LTE Modem and Router,» [En línea]. Available: https://www.cisco.com/c/en/us/products/collateral/routers/819-integrated-services-router-isr/data_sheet_c78-678459.html.

[123] «L2 Bridging Across an L3 Network Configuration Example,» [En línea]. Available: https://www.cisco.com/c/en/us/support/docs/ip/layer-two-tunnel-protocol-l2tp/116266-configure-l2-00.html.

[124] «INTEGRIS (INTelligent Electrical Grid Sensor communications) Funded by FP7-ICT-ENERGY-2009-1, Project ID: 247938,» [En línea]. Available: https://cordis.europa.eu/project/rcn/93726_es.html.

[125] ENSTO, «SAIDI and SAIFI indices guiding towards more reliable distribution network,» Nov 2016. [En línea]. Available: https://www.ensto.com/company/newsroom/articles/saidi-and-saifi-indices-guiding-towards-more-reliable-distribution-network/.

[126] «Common T&D Reliability Indices,» Institute of Electrical and Electronics Engineers, [En línea]. Available: http://www.ewh.ieee.org/.

[127] Carl Johan WALLNERSTRÖM, Elin GRAHN, Tommy JOHANSSON, «Analyses of The Current Swedish Revenue Cap Regulation, Paper 1021,» CIRED 24th International Conference on Electricity Distribution, June 2017.

[128] Jean Arlet, «Electricity Tariffs, Power Outages and Firm Performance: A Comparative Analysis,» Global Indicators Group, Development Economics. The World Bank, March 2017. [En línea]. Available: http://pubdocs.worldbank.org/en/444681490076354657/Electricity-Tariffs-Power-Outages-and-Firm-Performance.pdf.

[129] «EMC2 (Embedded Multi-Core systems for Mixed Criticality applications in dynamic and changeable real-time environments) project,» ARTEMIS and National European Authorities of 19 European countries, and in part by the Spanish Ministry of Industry, Energy, and Tourism, the project (Grant 621429 and national reference number ART-010000-2014-1), [En línea]. Available: www.artemis-emc2.eu.

[130] A. J. D. Rathnayaka, V. M. Potdar y S. J. Kurupp, «An innovative approach to manageprosumers in Smart Grid,» Proc. World CongressSustainable Technol., pp.141 -146 2011.

[131] Farhangi, H. et al. , «The path of the smart grid.,» IEEE power and energy magazine, 8(1)., 2010.

[132] Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., and Hancke, G. P., «Smart grid technologies: Communication technologies and standards,» IEEE transactions on Industrial informatics, 7(4), 529-539., 2011.

[133] Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., and Hancke, G. P. , «A survey on smart grid potential applications and communication requirement,» IEEE transactions on Industrial informatics, 9(1), 28-42., 2013.

[134] H Zeynal, M Eidiani, D. Yazdanpanah, «Intelligent Substation Automation Systems for robust operation of smart grids,» Innovative Smart Grid Technologies-Asia (ISGT Asia), pp. 786-790, 2014.

[135] Moreira P., Serrano J, Wlostowski T., Loschmidt P. and Gaderer G., «White-Rabbit: Sub-nanosecond timing distribution over ethernet. ISBN 978-1- 4244-4391-8. International Symposium on Precision Clock Synchronization for Measurement, Control and Communication,» ISPCS 2009.

[136] J.L. Gutierrez-Rivas et al, «Sub-nanosecond synchronization accuracy for time-sensitive applications on industrial networks,» European Frequency and Time Forum - EFTF, 2016.

[137] J. Díaz Javier, J.L. Gutiérrez, R. Rodríguez, B. Rat Benoi, «Industrial White-Rabbit Solutions,» Poster at “The 2015 Joint Conference of the IEEE Int'l Frequency Control Symposium & European Frequency & Time Forum, IFCS-EFTF, Denver, Colorado USA April 12-16, 2015, pp, 238–239.

[138] «IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems High Accuracy changelog, M. Lipinski, CERN,» [En línea]. Available: http://www.ohwr.org/projects/wr-std/wiki.

[139] «White Rabbit HSR Project,» [En línea]. Available: http://www.ohwr.org/projects/wr-hsr/.

[140] «International Electrotechnical Commission. IEC 62439-3 “Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)”,» [En línea]. Available: https://webstore.iec.ch/publication/24447 .

[141] M. I. Ridwan, N. S. Miswan, M. S. M. Shokri, M. N. Noran, R. M. Lajim, H. N. Awang, «Interoperability in Smart Grid using IEC 61850 standard: A power utility prospect,» Innovative Smart Grid Technologies - Asia (ISGT Asia) 2014 IEEE, pp. 261-2.

[142] S.Kumar, N. Das, S. Islam, «High Performance Communication Redundancy in a Digital Substation based on IEC 62439-3 with a Station Bus Configuration,» Power Engineering Conference (AUPEC), 2015 Australasian Universities, 27-30 Sept. 2015.

[143] «Communication Networks and Systems for Power Utility Automation, IInternational Electrotechnical Commission Std. 61850, 2013,» [En línea]. Available: http://www.iec.ch/.

[144] «PRP y HSR: Protocolos redundantes, INCIBE,» [En línea]. Available: https://www.certsi.es/blog/prp-y-hsr-protocolos-redundantes .

[145] J. A. Araujo, J. Lázaro, A. Astarloa, A. Zuloaga, J. I. Garate, «PRP and HSR for high availability networks in power utility automation: A method for redundant frames discarding,» IEEE Trans. Smart Grid, vol. 6, no. 5, pp. 2325-2332, Sep. 2015.

[146] «FMEDA,» Exida, [En línea]. Available: http://www.exida.com/Resources/Term/fmeda.

[147] M. Adamiak, A. Kulshrestha, «Design and Implementation of a UCA based Substation Control System,» [En línea]. Available: http://store.gedigitalenergy.com/faq/documents/b30/ger-3994.pdf .

[148] M. J. S. Mingarro, «Subestaciones eléctricas de alta tensión, Structuralia,» Red Eléctrica de España SAU19 de octubre de 2011.

[149] «IEEE Standard for SCADA and Automation Systems. IEEE Std C37.1-2007,» [En línea]. Available: https://standards.ieee.org/findstds/standard/C37.1-2007.html.

[150] «Saitel Remote Terminal Units,» [En línea]. Available: http://www.schneider-electric.com/en/product-subcategory/1990-Remote%20Terminal%20Units?filter=business-6-Medium Voltage Distribution and Grid Automation&parent-category-id=1900 .

[151] «International Electrotechnical Commission, International Standards and Conformity Assessment for all electrical, electronic and related technologies,» [En línea]. Available: https://webstore.iec.ch/preview/info_iec60870-5-104%7Bed2.0%7Den_d.pdf.

[152] «Inter-Range Instrumentation Group,» [En línea]. Available: http://irig.org/.

[153] «Time Synchronization in the Electric Power System,» NASPI (North American Synchrophasor Initiative), March 2017. [En línea]. Available: https://www.naspi.org/sites/default/files/reference_documents.

[154] David G. Hart, David Uy, Vasudev Gharpure, Damir Novosel, Daniel Karlsson, Mehmet Kaba, «Unidades PMU Supervisión de las redes eléctricas: un nuevo enfoque,» ABB, [En línea]. Available: https://library.e.abb.com/public/aacd3636143ee842c1256ddd00346ea2/58-61%20M800%20-%20SPA.pdf.

[155] «State Estimation and Voltage Security Monitoring Using Synchronized Phasor Measurement, Reynaldo Francisco Nuqui, Virginia Polytechnic Institute and State University 2.7.2001,» [En línea]. Available: citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.2.7959&rep=rep1&type=pdf.

[156] J. Northcote-Green, R.Wilson, «Control and Automation of Electrical Power Distribution Systems, p41».

[157] «International Electrotechnical Commission IEC 61850-5:2013 “Communication networks and systems for power utility automation - Part 5: Communication requirements for functions and device models” table 3, p72,» [En línea]. Available: https://webstore.iec.ch/publication/6012 .

[158] «C37.118-2005 Synchrophasors implemented in PMU devices,» [En línea]. Available: http://www.theiet.org/resources/books/pow-en/Phasor.cfm.

[159] R. Razzaghi, A. Derviˇskadi´c, and M. Paolone, «A White Rabbit Synchronized PMU».

[160] A. Derviˇskadi´c and M. Paolone, «A highly accurate calibration system for PMUs operating in distribution networks,» Swiss Federal Institute of Technology Lausanne (EPFL), Distributed Electrical Systems Laboratory (DESL), 2017, [En línea]. Available: http://57279746.swh.strato-hosting.eu/wp-content/uploads/2017/05/9-End_2017_04_20_GridSens_Derviskadic.pdf.

[161] M. Paolone, «Time synchronisation needs in phasor Measurement Units for the real-time monitoring of power grids,” Swiss Federal Institute of Technology Lausanne (EPFL), Distributed Electrical Systems Laboratory (DESL), 2015,» [En línea]. Available: https://indico.cern.ch/event/.

[162] «White Rabbit Switch,» [En línea]. Available: http://sevensols.com/index.php/products/wr-switch .

[163] «White Rabbit LEN,» [En línea]. Available: http://sevensols.com/index.php/products/wr-len.

[164] «Deliverable D11.1 System level requirements,» EMC2 project, December 2014.

[165] «IEEE Instrumentation and Measurement Society. IEEE 1588 Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.,» [En línea]. Available: https://standards.ieee.org/develop/project/1588.html.

[166] P. Moriera, P. Alvarez, J. Serrano, «Digital dual mixer time difference for sub-nanosecond time synchronization in ethernet,» Proc. IEEE Int. Frequency Control Symp. (FCS), pp. 449-453, 2010.

[167] Pietro Fezzardi, Maciej Lipiński, Alessandro Rubini, Aurelio Colosimo, «PPSi - A free software PTP implementation,,» Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS), IEEE International Symposium, 2014.

[168] «Seven Solutions S.L.,» [En línea]. Available: http://sevensols.com.

[169] M. Lipinski, «Redundant network topologies for dependable time transfer,» 9th White Rabbit Workshop in Amsterdam, Netherlands, 14-16 March 2016.

[170] V. K. Sood, D. Fischer, J. M. Eklund and T. Brown, «Developing a Communication Infrastructure for the Smart Grid,» IEEE on Electrical Power & Energy Conference (EPEC), Montreal, 22-23 October 2009, pp.1-7. doi:10. 1109/EPEC.2009.5420809.

[171] Sebastian Meiling, Till Steinbach, Thomas C. Schmidt, and Matthias Wählisch, «A Scalable Communication Infrastructure for Smart Grid Applications using Multicast over Public Networks».

[172] J. Han and D.-K. Jeon, «A practical implementation of IEEE 1588- 2008 transparent clock for distributed measurement and control systems,» IEEE Trans. Instrum. Meas., vol. 59, no. 2, pp. 433–439, Feb. 2010.

[173] «Tektronix FCA3000/3100 Timer/Counter/Analyzer,» [En línea]. Available: http://www.tek.com/ datasheet/fca3000-and-fca3100-series.

[174] Lipinski, Maciej Marek, «Vol. 40-Methods to Increase Reliability and Ensure Determinism in a White Rabbit Network. Diss. Warsaw U. of Tech».

[175] «Xilinx Chipscope FPGA Debugging Tool,» [En línea]. Available: www.xilinx.com/itp/xilinx10/isehelp/.

[176] C. Perera, C. H. Liu, S. Jayawardena, and M. Chen, «A Survey on Internet of Things From Industrial Market Perspective,» IEEE Access, vol. 2, 2014, pp. 1660–1679.

[177] «Industrial Internet of Things: Unleashing the Potential of Connected Products and Services, World Economic Forum, Geneve, SW, 2015,» [En línea]. Available: http://www.weforum.org.

[178] «Connecting with the Industrial Internet of Things (IIoT), Moor Insights & Strategy, Texas, USA 2013.,» [En línea]. Available: http://www.moorinsightsstrategy.com/ .

[179] «Industrial Internet Consortium,» [En línea]. Available: http://www.industrialinternetconsortium.org.

[180] D.P. Buse, Q.H. Wu, «Mobile agents for remote control of distributed systems,» IEEE Transactions on Industrial Electronics vol.51, no.6, 2004, pp.1142-1149.

[181] Kumar Nunna, S. Doolla, «Multiagent-Based Distributed-Energy-Resource Management for Intelligent Microgrids,» IEEE Transactions on Industrial Electronics, vol.60, no.4, 2013, pp.1678-1687.

[182] M. Eriksson, M. Armendariz, O.O. Vasilenko, A. Saleem, L. Nordstrom, «Multiagent-Based Distribution Automation Solution for Self-Healing Grids,» IEEE Transactions on Industrial Electronics, vol.62, no.4, 2015, pp.2620-2628.

[183] A. M. Mzahm, M. S. Ahmad, A.Y.C. Tang, «Enhancing the Internet of Things (IoT) via the Concept of Agent of Things (AoT),» Journal of Network and Innovative Computing, vol. 2, 2014, pp. 101-110.

[184] «Behaviorally Segmenting the Internet of Things (IoT), Moor Insights & Strategy, Texas, USA 2013,» [En línea]. Available: http://www.moorinsightsstrategy.com/.

[185] «INFIERE (INvestigation of the Future Intelligent Elements for Renewable Energy). Financiado por INVEST IN SPAIN/ICEX y los Fondos de Desarrollo Regionales Europeos. Ref: 1/2014-007,» [En línea]. Available: https://www.schneider-electric.com/en/work/products/medium-voltage-switchgear-and-energy-automation/r-and-d-projects/infiere.jsp.

[186] «SAGRA (Sistema Avanzado para Gestión de Redes Aisladas).Co Financiado por CDTI y la Junta de Andalucía. Programa Innterconecta. Ref: ITC-20151067.,» [En línea]. Available: https://www.schneider-electric.com/en/work/products/medium-voltage-switchgear-and-energy-automation/r-and-d-projects/sagra.jsp.

[187] «3S-CS (Standardization Security Synchronization Connected Substation).Co Financiado por CDTI y la Junta de Andalucía. Programa Innterconecta. Ref: ITC-20161012.,» [En línea]. Available: https://www.schneider-electric.com/en/work/products/medium-voltage-switchgear-and-energy-automation/r-and-d-projects/3s-cs.jsp.

[188] «When Things get smart, the Internet of Things gets Social,» [En línea]. Available: http://www.social-iot.org/.

[189] Roberto Girau, Michele Nitti, Luigi Atzori, «Implementation of an Experimental Platform for the Social Internet of Things,» Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on.

[190] Victoria Beltran ; Antonio M. Ortiz ; Dina Hussein ; Noel Crespi, «A semantic service creation platform for Social IoT,» Internet of Things (WF-IoT), 2014 IEEE World Forum on.

[191] Luigi Atzori, Antonio Iera and Giacomo Morabito, «Social Internet of Things: Turning Smart Objects into Social Objects to Boost the IoT,» November 11, 2014. [En línea]. Available: http://iot.ieee.org/newsletter/november-2014/social-internet-of-things-turning-smart-objects-into-social-objects-to-boost-the-iot.html.

[192] L. Atzori, A. Iera, G. Morabito and M. Nitti, «The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization,» Elsevier Computer Networks, vol. 56, 2012, pp. 3594–3608.

[193] A. Ortiz, D. Hussein, S. Park, S. N. Han and N. Crespi, «The Cluster Between Internet of Things and Social Networks: Review and Research Challenges,» IEEE Internet of Things Journal, vol. 1, no.1, June 2014, pp. 206–215.

[194] R. Serna, S. Craciunas, G. Stoger, «Analysis of Deterministic Ethernet scheduling for the Industrial Internet of Things,» 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, pp.320-324, 1-3 Dec. 2014.

[195] D. Gorecky, M. Schmitt, M. Loskyll, D. Zuhlke, «Human-machine-interaction in the industry 4.0 era,» 12th IEEE International Conference on Industrial Informatics (INDINpp.289,294, 27-30 July 2014.

[196] «Job Titles and Job Descriptions of Transmission Function Employees,» FERC Standards of Conduct Compliance, 2011. [En línea]. Available: https://www.sce.com/.

[197] Geraldo Rocha, David Dolezilek, Fernando Ayello, and Carlos Oliveira, «Distribution Substation Monitoring System,» Proceedings of the 2nd Annual Protection, Automation and Control World Conference, Junio 2011.

[198] «Manual de mantenimiento para subestaciones eléctricas.,» 2015. [En línea]. Available: http://dispac.com.co/wp-content/uploads/2015/05/ANEXO-18-A-MANUAL-DE-MANTENIMIENTO-PARA-SUBESTACIONES.pdf.

[199] «Transmission Function Employees,» BChydro, [En línea]. Available: https://www.bchydro.com/content/dam/BCHydro/customer-portal/documents/corporate/accountability-reports/openness-accountability/final-transmission-function-employees-job-descriptions-and-job-titles.pdf.

[200] «Procedimiento de Evaluación y Acreditación de las Competencias Profesionales Operación y Mantenimiento de Subestaciones Eléctricas Ministerio de Educación,» [En línea]. Available: https://www.educacion.es/.

[201] «Smart Grid Distribution Control Center and Operations,» [En línea]. Available: http://community.energycentral.com/community/t-d/smart-grid-distribution-control-center-and-operations.

[202] «Twitter social network from Twitter Inc,» [En línea]. Available: https://twitter.com.

[203] «Twitter,» [En línea]. Available: https://engineering.twitter.com/opensource .

[204] «Redis cluster,» [En línea]. Available: http://redis.io/topics/cluster-spec .

[205] «The Architecture Twitter Uses To Deal With 150M Active Users, 300K QPS, A 22 MB/S Firehose, And Send Tweets In Under 5 Seconds,» [En línea]. Available: http://highscalability.com/blog/2013/7/8/the-architecture-twitter-uses-to-deal-with-150m-active-users.html.

[206] «OAuth Twitter,» [En línea]. Available: https://dev.twitter.com/oauth/pin-based.

[207] «Slack,» [En línea]. Available: https://slack.com/intl/es-es.

[208] «Lookwise Enterprise Manager SIEM,» S21sec, [En línea]. Available: https://www.s21sec.com/es/lem-for-siem/.

[209] Danah M. Boyd, Nicole B. Ellison, «Social Network Sites: Definition, History, and Scholarship,» Journal of Computer-Mediated Communication, Volume 13, Issue 1, 1 October 2007, Pages 210–230, https://doi.org/10.1111/j.1083-6101.2007.00393.x.