Smart Grids Colombia VISIÓN 2030

**Parte IV**

# Anexo 5. Recomendaciones de Ciberseguridad e Interoperabilidad

Abril de 2016

## Equipo de Trabajo


**Editores:**
Grupo Técnico Proyecto BID integrado por Representantes de:

**Banco Interamericano de Desarrollo (Cooperación Técnica)**
José Ramón Gómez Guerrero
Jorge Luis Rodríguez Sanabria
Juan Eduardo Afanador Restrepo

**Ministerio de Minas y Energía**
Marie Paz Rodríguez Mier
Oficina de Asuntos Ambientales y Sociales

Carlos Arturo Rodriguez Castrillón
Profesional Especializado
Oficina Dirección de Energía

**Ministerio de Tecnologías de la Información y las Comunicaciones**
Liliana Jaimes Carrillo
Despacho Viceministerio TI

**Unidad de Planeación Minero-Energética**
Camilo Táutiva Mancera
Asesor de Energía

**Iniciativa Colombia Inteligente**
Alberto Olarte Aguirre
Secretario Técnico C N O – Presidente Colombia Inteligente

Renato Humberto Céspedes Gandarillas
Coordinador Técnico

**Firmas Consultoras**
**CIRCE**
Andrés Llombart Estopiñán
María Paz Comech Moreno
Adrián Alonso Hérranz
Samuel Borroy
Vicente Gorka Goicoechea Bañuelos
Carlos Pueyo Rufas

**Universidad de Alcalá de Henares**
Carlos Girón Casares
Francisco Javier Rodríguez Sánchez

**Universidad Tecnológica de Pereira**
Alejandro Garcés Ruiz
Juan José Mora Flórez

**CREARA CONSULTORES, S.L.**
María Jesús Báez Morandi
José Ignacio Briano Zerbino

**Afi – Analistas Financieros Internacionales**
Pablo I. Hernández González
Diego Vizcaíno Delgado



Bogotá D.C., Abril de 2016

NOTA ACLARATORIA - *DISCLAIMER*

1. Los planteamientos y propuestas presentados en este documento son los resultados del análisis y elaboración del Estudio desarrollado por el Equipo de Trabajo en el marco de la Cooperación Técnica ATN-KK-14254-CO (CO-T1337) con el aporte de fondos provenientes del Fondo Coreano para Tecnología e Innovación a través del Banco Interamericano de Desarrollo –BID–. Estos planteamientos y propuestas no representan ni comprometen la posición y planteamientos de las entidades oficiales del Gobierno Colombiano participantes.

2. Los análisis realizados en el desarrollo de la Cooperación Técnica consideraron la información disponible hasta el mes de diciembre del año 2015, fecha en la cual finalizó de manera oficial el trabajo realizado durante esta cooperación.

# Tabla de contenido



# Índice de figuras



# Índice de Tablas

# ANEXO 5

## 1. Recomendaciones de Ciberseguridad e Interoperabilidad

### 1.1 Ciberseguridad

***Introducción***

La seguridad cibernética es un concepto que se ha vuelto cada vez más predominante en el desarrollo de la tecnología de redes inteligentes[1], dado el aumento de la información generada en las distintas aplicaciones de las RI y el riesgo de un uso indeseado de esa información. Por tanto la seguridad cibernética es una prioridad crítica del desarrollo de redes inteligentes.

Sin embargo, los requisitos de seguridad cibernética para la RI están en un cierto estado de indefinición. La seguridad cibernética incluye medidas para garantizar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación electrónicos necesarios para la gestión y protección de la energía de la red inteligente, de las tecnologías de la información y de la infraestructura de telecomunicaciones.

Esta infraestructura incluye los sistemas de información y comunicaciones y la información contenida en estos sistemas y servicios. Los sistemas de información y comunicaciones están compuestos por el hardware y el software para procesar, almacenar y comunicar información, o cualquier combinación de todos estos elementos.

La seguridad cibernética se define como la protección frente a las amenazas que tienen su origen en ordenadores o terminales informáticos, así como la protección de otros bienes físicos ante su modificación o daños causados por mal uso accidental o malintencionado de las instalaciones de control soportadas en sistemas informáticos. Los protocolos de seguridad de las redes inteligentes deberían contener elementos de disuasión, prevención, detección, respuesta y mitigación ante ataques cibernéticos; una red inteligente madura será capaz de frustrar ataques múltiples y coordinados durante cierto periodo de tiempo. La seguridad mejorada reducirá el impacto de sucesos anormales en la estabilidad y la integridad de la red, garantizando la seguridad de la sociedad y la economía.

Los esfuerzos en seguridad cibernética deben ser dirigidos al diseño de la seguridad de la red a nivel de arquitectura, identificando, mediante el análisis de diversos casos de uso, los distintos riesgos de seguridad, su evaluación y posibilidades de mitigación. La idea subyacente es que la seguridad debe ser incorporada en la fase de diseño y no añadida a posteriori. Esta estrategia incluye:

- Revisión de la funcionalidad del sistema y los flujos datos, con especial atención a sus similitudes y diferencias con los casos de uso ya identificados y documentados (por ejemplo en la Hoja de Ruta del NIST (NIST, 2010).
- La identificación de las amenazas relevantes y de las consecuencias/impactos si la confidencialidad, la integridad, la disponibilidad o la trazabilidad de los flujos de datos del sistema se vieran comprometidos.

[1] Los términos Redes Inteligentes y Smart Grid, sus respectivas siglas RI - SG y Hoja de Ruta y Mapa de Ruta son utilizados indistintamente en estos documentos.

La seguridad requiere el uso combinado de diferentes soluciones y no se reduce a la encriptación y protección por contraseña. Los aspectos a considerar en la seguridad cibernética incluyen:

- Evaluación de la seguridad y fortalecimiento de los sistemas existentes.
- Evaluación de la vulnerabilidad.
- La recuperación de desastres.
- Respuesta a los incidentes de detección de intrusión.
- El registro de eventos, agregación y correlación.

Otro aspecto crítico a tener en cuenta en el desarrollo de la seguridad es darse cuenta de la inevitabilidad de la ocurrencia de situaciones donde la seguridad falle. Esto debe conducir a la elaboración de planes de contingencia y recuperación.

La Tabla 1 detalla las amenazas que enfrentan el sistema de red eléctrica tradicional y su metamorfosis en la nueva RI.

**Tabla 1. Amenazas de seguridad en la red eléctrica tradicional y la *RI***

| | Amenazas en la red eléctrica tradicional | Amenazas en las RI |
|---|---|---|
| **Impacto** | Daño físico directo a la red eléctrica | Daño indirecto al equipamiento a través de intrusiones en el software |
| **Ubicación del atacante** | Local | Local o remoto |
| **Tipo de atacante** | Individuos | Individuos, competidores, organizaciones, etc. |
| **Puntos de ataque** | Uno | Múltiples puntos simultáneamente |
| **Extensión del daño** | Daño inmediato visible de manera evidente | El ataque puede no detectarse o permanecer larvado y activarse posteriormente. |
| **Ocurrencia** | Episodios simples | Ataques continuados con daños crecientes |
| **Restauración del servicio** | De manera inmediata tras ataque | Los ataques pueden ser mantenidos en el tiempo e impedir la restauración |

*Fuente: CIRCE*

Los objetivos críticos del desarrollo de la seguridad cibernética para la red inteligente son: 1) asegurar la confidencialidad, la integridad y la disponibilidad de los dispositivos y sistemas de información y de los canales de comunicación; y 2) asegurar el registro, monitoreo, gestión de alarmas y su correcta notificación. La protección de datos requiere la confidencialidad de los datos transmitidos y almacenados de todos los agentes del sistema energético, usando para ello métodos de autenticación apoyados en el uso de criptografía, es decir, autenticación cifrada. Una combinación de actuaciones preventivas, detecciones rápidas y medidas correctivas permiten abordar los riesgos de seguridad cibernética.

Las amenazas cibernéticas conocidas pueden ser monitorizadas con varias herramientas. Por ejemplo, los sistemas de detección de intrusiones apoyados en hosts que supervisan los cambios no autorizados en los servidores y sistemas desplegados; los sistemas de detección de intrusión de red que detectan los ataques basados en la red; y los controles específicos de plataforma como la detección de virus y detección de malware. Estos controles proporcionan datos vitales para el personal de diseño y pruebas sobre los ataques reales y amenazas que enfrenta el sistema. Los controles de seguridad deben proporcionar evidencia forense para reconstruir ataques y, potencialmente, identificar y perseguir a los atacantes.

Además, los registros de seguridad también pueden ayudar en la selección de acciones correctivas y preventivas.

Las acciones correctivas pretenden restaurar las operaciones normales en el caso de un ataque cibernético. Tales acciones pueden ser de tipo manual, por ejemplo, un procedimiento estandarizado para cambiar a un sistema de respaldo, o automáticos, por ejemplo, sistemas redundantes que conmutan automáticamente en caso de fallo y que mantienen en todo momento la funcionalidad del sistema.

El desarrollo seguro de sistemas trata de abordar el riesgo a lo largo del ciclo de vida y durante todo el proceso de ingeniería. Algunos ataques, por ejemplo, los de denegación de servicio, sólo pueden mitigarse con una combinación de ingeniería de seguridad y de acciones preventivas. Otros ataques pueden ser parcialmente mitigados con acciones de protección temporales, por ejemplo, filtro de red o controles de acceso basados en roles, hasta que pueda resolverse definitivamente.

## ***Riesgos de Seguridad Cibernética***

Los riesgos de seguridad cibernética aparecen en cada fase del ciclo de vida de un proyecto e incluyen riesgos para los procesos administrativos, operativos y técnicos. Estos riesgos pueden afectar a equipos y sistemas de gestión de red y de integración, comunicación, control y operaciones, y a la disponibilidad del sistema. Los principales componentes que pueden ser vulnerables a los riesgos de seguridad incluyen aplicaciones informáticas, red de comunicaciones y puntos finales (por ejemplo, contadores inteligentes, displays en casa, y termostatos). Hay riesgos importantes para la integridad de los datos y comandos de control si el intercambio de información se realiza a través de equipamiento fácil de interceptar como por ejemplo, los contadores inteligentes que utilizan redes inalámbricas que pueden ser interceptadas e incluso alteradas si no están aseguradas apropiadamente.

## ***Amenazas para los sistemas físicos.***

Las amenazas informáticas de las RIs, tienen el potencial de romper la seguridad nacional, la estabilidad económica e incluso la seguridad física. Las centrales eléctricas y los sistemas SCADA (control de supervisión y adquisición de datos) siempre han sido blanco de los piratas informáticos. El paso de sistemas de control cerrados a redes IP abre un nuevo abanico de vulnerabilidades. Por ejemplo, la integridad de datos y la autenticación pueden verse comprometidos a través de ataques de red tales como *spoofing (Man in the middle)*, suplantación, o de denegación de servicio (DoS). Del mismo modo, la seguridad de datos puede verse comprometida por ataques de sabotaje o internos tales como virus y caballos de Troya. Este último se convierte en una amenaza significativa teniendo en cuenta la apertura potencial de los sistemas y sus interconexiones con diferentes redes, tales como NAN e Internet.

Una vez que se encuentra un punto de entrada, se hace más fácil para el atacante activar un ataque en cadena a la red inteligente. Por ejemplo, comprometer el canal de precios o lectura de medidas de contadores, en tiempo real, puede resultar en el robo de energía o el control remoto malicioso de electrodomésticos. Por lo tanto, se requiere una seguridad rigurosa del hardware / software para garantizar la validez de las diferentes partes de la comunicación tales como concentradores de cabecera y los contadores inteligentes. Si un atacante se apodera del concentrador de cabecera, entonces podría ser capaz de enviar un comando de interrupción de suministro a los contadores inteligentes con respuesta a la demanda. La interrupción puede hacerse permanente si se ordena a todos los contadores que cambien sus claves criptográficas a algún nuevo valor que sólo se conoce al atacante. El impacto podría ser enorme: millones de hogares se quedarían sin energía hasta que los contadores fuesen sustituidos o se repusiesen las claves auténticas. Como consecuencia de ello, la seguridad podría verse en peligro a nivel local, y las empresas podrían perder millones. La ciberseguridad en las RI necesita a) prevenir este tipo de ataques y b) tener un mecanismo de recuperación / capacidad de supervivencia en caso de ataques (con éxito).

La seguridad de las comunicaciones implica el diseño de un cripto-sistema de gestión de claves. Esto podría, por ejemplo, basarse en los sistemas existentes, tales como la Infraestructura de Clave Pública (PKI) y encriptación basada en identidad (IBE). IBE, en particular, puede ser atractivo para las redes inteligentes, ya que puede ser desplegado sin necesidad de configuración previa, dado que la identidad (ID) de un dispositivo se utiliza para generar claves únicas. Esto permite un fácil despliegue de los dispositivos de baja potencia, tales como sensores, ya que pueden empezar a enviar mensajes seguros sin necesidad de ponerse en contacto con un servidor de claves. En general, una mezcla de los regímenes de seguridad jerárquicos, descentralizados, delegados o híbridos puede ser factible. Preferiblemente, un esquema de seguridad candidato, debe incluir protocolos de inicialización seguros, es decir, debe ser sencillo y eficaz el modo de inicializar nuevos dispositivos. Además, las operaciones críticas de seguridad, tales como actualizaciones de claves, deben emplear preferentemente las técnicas de gestión de claves de grupo, como las técnicas de defensa en profundidad utilizadas en los sistemas de control nucleares o militares, para mitigar el impacto de los equipos concentradores de cabecera con seguridad comprometida (o de personas de confianza).

Para obtener más información sobre los diferentes ataques de ciberseguridad a la red inteligente y su impacto se pueden seguir las directrices del NIST (NIST, 2010).

### ***Aspecto relativos a la privacidad***

La recopilación frecuente de datos de los contadores inteligentes y su análisis, pueden ayudar a mejorar la eficiencia energética. Sin embargo, de este modo se pone en entredicho la privacidad del usuario. Es decir, la información contenida en dichos datos puede ser utilizada para fines distintos de la eficiencia energética, lo que da lugar a un problema de privacidad. En particular, la recopilación de datos frecuente de contadores inteligentes revela una gran cantidad de información sobre el uso de electrodomésticos y otro tipo de equipos residenciales.

En general, la protección de datos se refiere a la seguridad de los datos que están relacionados o que permiten inferir información relativa a la vida de los individuos. El uso de los mecanismos de control de acceso, por ejemplo servicios de autenticación, autorización y confidencialidad seguras, no permite abordar el problema de privacidad de los datos de redes inteligentes de manera integral. Esto es debido a que estos datos deben ser difundidos a muchos actores diferentes dentro de la red. Las consecuencias de los problemas de privacidad en las RI son difíciles de entender, ya que no se conocen a) toda la gama de posibilidades de extracción de información, y b) el concepto de la privacidad en las redes inteligentes no está todavía bien definido. Una buena razón de por qué el problema de la privacidad de los datos no se debe subestimar puede encontrarse en un documento sobre la inclusión digital y sus ramificaciones (Stallman, 2010).

Actualmente, este problema de privacidad destaca en las tecnologías NALM (Monitorización de Cargas no Intrusiva) que utilizan las mediciones de energía para extraer información detallada en relación con el uso de los electrodomésticos. Desde el trabajo original (Hart, 1992) se ha producido una gran cantidad de investigación en la construcción y mantenimiento de bibliotecas de electrodomésticos y algoritmos de detección (Lam, 2007). Los resultados recientes sugieren que incluso con perfiles de consumo doméstico agregados, se puede identificar con gran precisión (Prudenzi, 2002) el uso de aparatos domésticos. Los autores de (Taysi, 2010) han descrito un sistema de monitorización de energía que genera informes de consumo de energía a nivel de dispositivo, basado principalmente en las firmas acústicas de electrodomésticos. Sus experimentos demuestran que el sistema es capaz de informar del consumo de energía de los aparatos domésticos individuales dentro de un margen de error del 10%.

En general, la granularidad de eventos que un algoritmo puede ser capaz de detectar con éxito depende de la frecuencia de las lecturas del contador inteligente. El rango de frecuencia puede variar, dependiendo

de la empresa, pero podría llegar a ser tan alta como cada pocos minutos (1-5). La información detallada sobre el uso de energía podría poner al descubierto los patrones de uso de energía diarios de una casa y permitir la deducción de qué tipo de dispositivo o aparato estaba en uso en un momento dado. Además, se pueden utilizar las técnicas de minería de datos para revelar las tendencias del comportamiento personal en los datos de medición, incluso si se supone que las frecuencias de muestreo de datos son relativamente bajas (por ejemplo, cada 30 minutos).

De lo anterior queda claro que el problema de privacidad es importante y se necesitan soluciones. Hay dos clases de sistemas de protección de la privacidad: a) basados en la regulación normativa y b) basada en la tecnología. Las actividades de normalización actuales se centran en el desarrollo de normas y políticas para ayudar a proteger la privacidad de redes inteligentes. En Estados Unidos el NIST ha reconocido que el principal beneficio proporcionado por la red inteligente, es decir, la capacidad de obtener datos detallados de los contadores de los clientes y otros dispositivos eléctricos, es también su talón de Aquiles desde el punto de vista de la privacidad. Además, la Asociación Nacional Americana de Comisionados Reguladores de Servicios Públicos (NARUC) ha elaborado una resolución declarando que: "la información del cliente se puede utilizar para diferenciar los servicios de las empresas, de una manera que cree valor añadido para el cliente". Por otro lado, "debe alcanzarse un equilibrio entre el papel favorable a la competencia que la información del cliente puede jugar en mercados nuevos y en desarrollo y las implicaciones de privacidad de utilizar esa información".

En Europa, la Comisión Europea ha creado un grupo de trabajo sobre redes inteligentes con el objetivo de desarrollar una visión común de la UE respecto a las redes inteligentes e identificar los temas clave que necesitan ser resueltos. En respuesta, se han puesto en marcha tres grupos de expertos (EG), uno de los cuales, EG2, tiene como objetivo identificar los escenarios y recomendaciones regulatorias apropiadas para el manejo de datos, la seguridad y la protección del consumidor. Una de las recomendaciones del EG2 es utilizar servicios anónimos para proteger la privacidad. Por ejemplo, los datos de los contadores inteligentes se pueden separar en datos de baja frecuencia (por ejemplo, los datos utilizados para la facturación) y datos técnicos anónimos de alta frecuencia (por ejemplo, datos utilizados para la gestión de la demanda). En este caso, el principal desafío reside en anonimizar los datos de alta frecuencia, que son necesarios para las funcionalidades de la red eficientes, mientras se asegura que la fiabilidad, la eficacia y la seguridad de estas funcionalidades no se vean comprometidas.

Otras soluciones tecnológicas que se han propuesto son:

- Anonimato. En (Kalogridis, 2010), se propone un protocolo seguro para anonimizar la identificación de los datos de medición enviados por un medidor inteligente.
- La agregación. En (Bohli, 2010) los autores introducen dos soluciones diferentes para el modelo de protección de datos de red inteligente. Una solución utiliza un tercero de confianza como proxy de agregación de datos. La otra solución añade a los datos un valor aleatorio a partir de una distribución de probabilidad particular.
- Homomorfismo. El uso de la encriptación homomórfica puede ayudar a la privacidad de datos de los contadores inteligentes como se explica en (Jacobs, 2010). En este trabajo se desarrolla un método para un número de contadores que tienen un componente de confianza y disfrutan de un cierto nivel de autonomía. Un sistema confiable ofrece garantías sobre las mediciones para operadores de la red y los consumidores.
- La ofuscación. En (Kim, 2011) se introduce una técnica cooperativa de estimación de estado que protege la privacidad de las actividades diarias de los usuarios. El esquema propuesto puede ocultar los datos de privacidad sin comprometer el rendimiento de la estimación del estado.

- Negociación. En (Sankar, 2011) los autores introducen el concepto de privacidad competitiva entre la empresa que tiene que compartir los datos para garantizar la confiabilidad de la red y el usuario que retiene los datos por razones de rentabilidad y de privacidad.
- Gestión de la energía. En (Kalogridis G. , 2010) los autores introducen un algoritmo de gestión de baterías que cambia el consumo de energía en el hogar de tal forma que ayuda a proteger la privacidad.

Aunque hay mucha más investigación por hacer en esta área, parece que la privacidad de redes inteligentes es un tema delicado que puede ser abordado desde diferentes ángulos. La solución de protección futura es probable que sea una combinación o evolución de las soluciones introducidas anteriormente, dependiendo del coste del sistema y la necesidad de privacidad en las diferentes sociedades.

## ***Requerimientos de seguridad***

Deben tenerse en cuenta una serie de requerimientos para satisfacer las necesidades de seguridad. Como en la mayoría de las situaciones de diseño, deben adoptarse ciertos compromisos entre aspectos que no pueden satisfacerse simultáneamente o que, directamente, están uno en contraposición de otro. En los siguientes aspectos debe adoptarse un compromiso entre seguridad y prestaciones:

- Rendimiento (por ejemplo, tiempo de respuesta).
- Funcionalidad (por ejemplo, la complejidad de las interacciones de los usuarios).
- Capacidad de actualización (por ejemplo, la facilidad de sustitución de componentes).
- Adaptabilidad (por ejemplo, la facilidad de reconfiguración para su uso en otras aplicaciones).
- La eficacia (por ejemplo, información relevante y pertinente para el proceso de negocio, que además debe ser entregada a su debido tiempo y de forma correcta, consistente y utilizable).
- Eficiencia (por ejemplo, el suministro de información a través de los recursos más productivos y económicos).
- Confidencialidad (por ejemplo, la protección de la información sensible de la divulgación no autorizada).
- Integridad (por ejemplo, la exactitud, integridad y validez de la información de acuerdo con los valores empresariales y las expectativas).
- Disponibilidad (por ejemplo, la información debe estar disponible cuando sea requerida por los procesos de la empresa).
- Cumplimiento (por ejemplo, el cumplimiento de las leyes, regulaciones y acuerdos contractuales).

Es importante tener en cuenta otras limitaciones en el diseño de la seguridad:

- Computacionales (por ejemplo, la potencia de cálculo disponible en los dispositivos remotos).
- Trabajo en red (por ejemplo, el ancho de banda, rendimiento o latencia).
- Almacenamiento (por ejemplo, la capacidad requerida para almacenar el firmware y los registros de eventos).
- Energía disponible en los dispositivos remotos.
- El personal (por ejemplo, el impacto en el tiempo promedio dedicado a mantenimiento).

- Financiera (por ejemplo, el costo de los dispositivos).
- Temporal.
- Tecnología.
- Disponibilidad.
- Madurez.
- Integración / interoperabilidad (por ejemplo, red eléctrica tradicional).
- Ciclo de vida.
- Infraestructura (por ejemplo, la tecnología y las instalaciones, es decir, hardware, sistemas operativos, sistemas de gestión de bases de datos, redes y multimedia).
- Las personas (por ejemplo, el personal necesario para planificar, organizar, adquirir, implementar, dar soporte, monitorizar y evaluar los sistemas y servicios de información. El personal pueden ser internos, subcontratado o contratado según sea necesario).

## ***Aspectos de seguridad cibernética relativos a AMI***

AMI supone la convergencia de la red de energía, la infraestructura de comunicaciones, y la infraestructura de soporte de la información. Este sistema de sistemas está constituido por una colección de aplicaciones, hardware, operadores e información y tiene aplicaciones en la facturación, servicio y apoyo al cliente, y en la distribución eléctrica. Estas aplicaciones tienen ciertas consideraciones relativas a la seguridad que se resumen en la Tabla 2.

**Tabla 2. Implicaciones de ciberseguridad en AMI**

| Aplicación | Implicaciones de ciber seguridad |
|---|---|
| **Facturación** | • *Confidencialidad de* los datos de usuario, de órdenes de control y de la ubicación de los datos<br>• *Integridad* de medidas, órdenes de control y mensajes de indicación de fraude.<br>• *Disponibilidad* remota de las medidas y del servicio de conexión/desconexión |
| **Cliente** | • *Confidencialidad de* las órdenes de acceso al equipamiento del usuario, indicaciones y mensajes de precios. Privacidad de los datos y pagos de los usuarios.<br>• *Integridad* de las medidas leídas del contador, de los mensajes de control y de información con los datos de prepago, uso de energía y perfiles de consumo.<br>• *Disponibilidad* remota de las medidas, del servicio de conexión/desconexión, de los datos de pago del usuario y el balance energético. |
| **Sistema de distribución** | • *Confidencialidad* en el acceso remoto al equipamiento de usuario.<br>• *Integridad* de los mensajes de control e información y de los datos almacenados en el sistema.<br>• *Disponibilidad* de los equipos del usuario y de los datos recopilados. |

*Fuente: CIRCE*

El desarrollo de los aspectos de seguridad para implementar una solución robusta AMI puede describirse en seis dominios. Los servicios que se muestran en la Tabla 3 son descripciones de cada uno de los seis dominios de seguridad propuestos. Cada implementación de AMI variará en función de las tecnologías específicas seleccionadas, las políticas de la empresa eléctrica y el entorno de despliegue.

**Tabla 3. Dominios de seguridad en la *RI***

| Dominio de seguridad | Descripción |
|---|---|
| **Servicios controlados por la empresa** | Todos los servicios de monitorización, medida y control del equipamiento de campo, gestionados directamente por la empresa. |
| **Servicios delegados por el usuario** | Todos los servicios de monitorización, medida y control del equipamiento de campo, bajo control del cliente y que podrá delegar en un tercero. |
| **Servicios de comunicaciones** | Aplicaciones que gestionan la agregación, comunicación y encaminamiento de los datos y comandos relativos al equipamiento de campo. |
| **Servicios gestionados** | Servicios atendidos de gestión del equipamiento de automatización y comunicaciones |
| **Servicios automatizados** | Servicios desatendidos de agregación y transmisión de datos. |
| **Servicios de negocio** | Aplicaciones básicas del negocio, incluyendo gestión y evaluación. |

*Fuente: CIRCE*

Fundamentalmente los desafíos de seguridad AMI se refieren a la protección de los datos de los contadores inteligentes contra el acceso no autorizado y el repudio. Este es un requisito importante sin el cual los datos AMR no son de confianza, ni para las empresas, ni para los clientes. Se requieren soluciones a diferentes niveles: deben usarse protocolos seguros de comunicación extremo a extremo, los componentes de hardware (por ejemplo, contadores inteligentes) tienen que soportar los ataques físicos, la red debe detectar los elementos *hackeados*, y el software de medición inteligente debe estar libre de errores.

Los requisitos de seguridad de las comunicaciones en AMI pueden abordarse mediante la combinación de protocolos criptográficos existentes y soluciones de hardware a prueba de manipulaciones, probando exhaustivamente equipos y software contra todo tipo de ataques, y mediante la adopción de una arquitectura abierta para pruebas y actualización segura.

También, es igualmente importante desarrollar mecanismos de protección de los datos de medición inteligente contra los ataques internos. El uso de interfaces abiertas de red inteligente, creará una puerta de entrada para terceros actores (*stakeholders*) que podrán acceder y procesar datos AMR. Debe asegurarse que a este tipo de información privilegiada sólo tendrán acceso los agentes autorizados y solos para su uso de una manera aceptable.

Las políticas de seguridad y la legislación no son una panacea para la privacidad. La historia enseña que las técnicas legítimas para la minería y la explotación de los datos evolucionan rápidamente cuando hay un incentivo financiero claro. Por lo tanto, el problema del acceso y el uso de los datos de los contadores inteligentes deben ser analizado en diferentes aspectos de seguridad:

- Los datos medidos deberían pertenecer, en principio, a los usuarios. Por ejemplo, podría utilizarse un sistema de gestión de derechos digitales para permitir a las empresas proveedoras el uso de

los datos de una manera aceptable. Cualquier uso de los datos personales (aceptables o inaceptables) no debe poder ser repudiado.

- Los usuarios deben poder utilizar algoritmos de gestión de la energía de una manera que oculte su perfil de uso.
- Debe haber mecanismos que detecten (en retrospectiva) el mal uso de los datos de los contadores inteligentes. Estos mecanismos deben contar con el apoyo regulatorio para establecer sanciones proporcionadas contra las partes que hagan un uso no autorizado de la información.

El reto común sigue siendo alcanzar un compromiso entre seguridad y rendimiento, es decir, utilizar la seguridad adecuada para reducir al mínimo su uso de energía y los sobrecostes. En el futuro, las comunicaciones que soporten la RI podrán, potencialmente, integrarse con sistemas de comunicaciones heterogéneos, aplicaciones de Internet, etc. Por ejemplo, un cliente itinerante podría utilizar energía en zonas remotas y vincular este uso a su perfil de medición inteligente. Esta integración se puede utilizar para la facturación o para otros servicios personalizados. En este ejemplo, sería necesario establecer protocolos de comunicación seguros entre las diferentes partes, tales como el contador inteligente de casa, un teléfono móvil, una aplicación inteligente para la energía en itinerancia y el cliente. El cliente, además, podría permitir a terceros tener acceso a la información de su contador inteligente personal a cambio de servicios como acceso gratuito a ciertas instalaciones, o bien el cliente puede desear permanecer en el anonimato. Se pueden predecir nuevos retos que surgen de la integración de los sistemas de comunicación para la RI con otros sistemas de comunicación: sistemas de entretenimiento doméstico, sistemas de comunicación médicos y sistemas de comunicación para seguimiento del tráfico (por ejemplo, a través de GPS), sólo por citar unos pocos.

En los escenarios anteriores se pone de manifiesto que la integración de servicios e interfaces da lugar a toda una nueva gama de vulnerabilidades de seguridad y privacidad, y de requisitos. En estos entornos complejos de computación, comunicaciones y de gestión de la energía, es importante entender cómo se conectan en cascada los riesgos de seguridad, es decir, cómo un fallo de seguridad de un sistema conduce a un fallo de un sistema de aguas abajo. El análisis de riesgos debe ser capaz de detectar tanto las anomalías proactivas y reactivas del sistema y adoptar medidas apropiadas tales como la creación de registros de datos y alertas. Además, la extrapolación y la combinación de la información de varios dominios, como los datos de consumo de energía, información de ubicación, información de estilo de vida, y otra información personal, aumenta el potencial tanto para nuevas aplicaciones y servicios, como las amenazas de seguridad y de daños. De hecho, la futura integración de sistemas y servicios requiere, más que nunca, de mecanismos de protección transparentes y seguros.

### ***Mitigación de los riesgos de seguridad cibernética***

El proceso de mitigación de los errores o de las fuentes de inseguridad, incluye lo siguiente:

- Identificar y clasificar la información que necesita ser protegida.
- Definir los requisitos de seguridad detalladamente.
- Revisión de la arquitectura de seguridad propuesta para cumplir con los requisitos.
- La adquisición de un sistema que esté diseñado para satisfacer los requisitos de seguridad especificados e incluya la capacidad de ser actualizado para satisfacer nuevas normas de seguridad.
- Probar los sistemas de seguridad durante la fase de prueba e instalación.

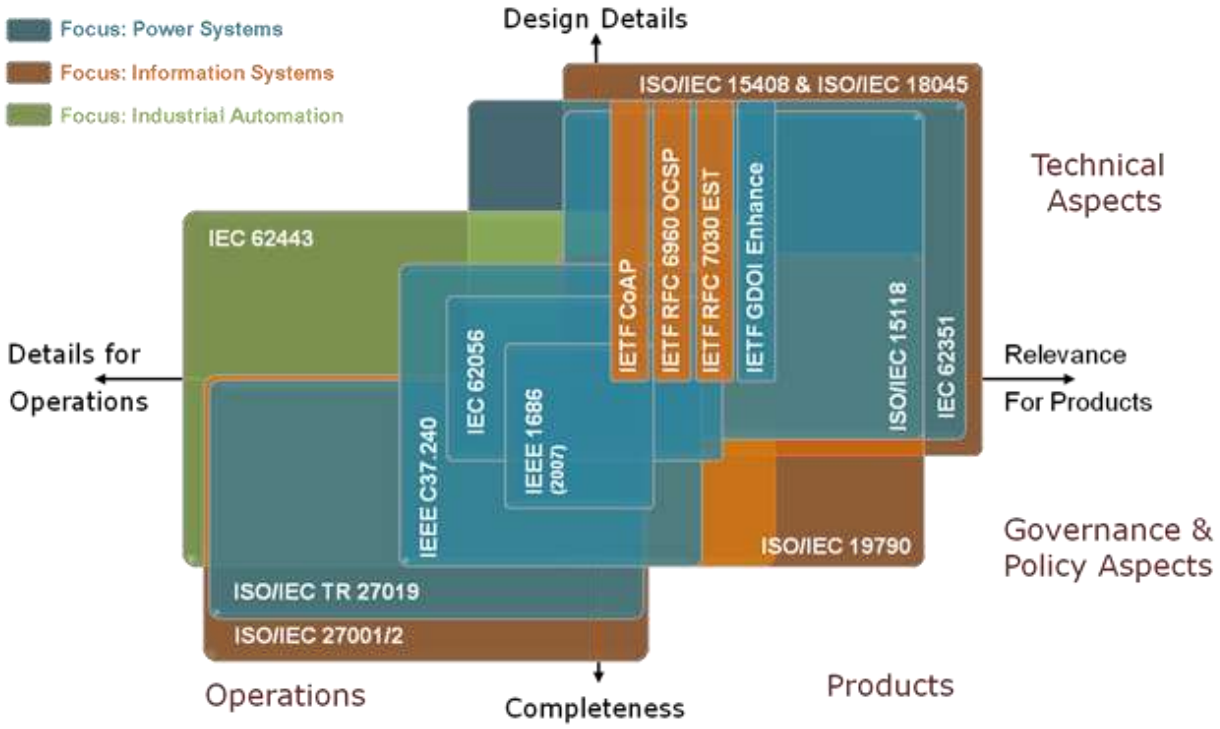
- La obtención de una evaluación independiente de la situación de seguridad antes del despliegue final.
- Desarrollo de un plan para mitigar los riesgos de las vulnerabilidades identificadas.
- Instalación de un sistema con funciones de gestión y control de la seguridad.
- Seguimiento y evaluación periódica de la eficacia de los controles de seguridad.
- Migración a las actualizaciones de seguridad adecuadas, según se produzca la madurez de estándares y productos.
- Monitorización de los canales de comunicación.
- Detección de los picos de usos (lectura del medidor) para detectar posibles fallos o la manipulación de los dispositivos.
- Realización de dispositivos seguros que se sincronicen regularmente con la red para detectar alteraciones, posibles problemas y fallos de los dispositivos.
- Las pruebas de seguridad se realizarán utilizando las últimas técnicas de *hacking* para tratar de entrar en los sistemas, identificando posibles vulnerabilidades, y validando de forma remota la autenticidad del software que se ejecuta en los contadores.
- La historia de la seguridad en redes complejas lleva a la conclusión de que no todas las vulnerabilidades son descubiertas.

### ***Normativa de ciberseguridad***

Las normas de ciberseguridad aplicables a las RI pueden organizarse de distinta forma. En este caso se han elegido dos enfoques. En el primero de ellos (Figura 1) se muestra la interacción entre las normas atendiendo a los siguientes términos:

- **Detalles para la operación**: El estándar define medios de tipo procedimental y organizacional, aplicables a todos o parte de los actores implicados. Puede haber requerimientos implícitos para sistemas y componentes sin detallar opciones de implementación.
- **Relevante para los productos:** El estándar influye directamente en la funcionalidad de los componentes o sistemas y debe ser considerado durante la fase de diseño o desarrollo del producto.
- **Detalles de diseño:** El estándar describe la implementación de los medios de seguridad con suficiente detalle como para alcanzar la interoperabilidad entre productos de diferentes vendedores.
- **Completitud**: El estándar abarca no solo algunos aspectos de seguridad, sino que aborda todos los aspectos relativos a la misma, incluyendo medios técnicos y organizacionales.

**Figura 1. Estándares de ciberseguridad**



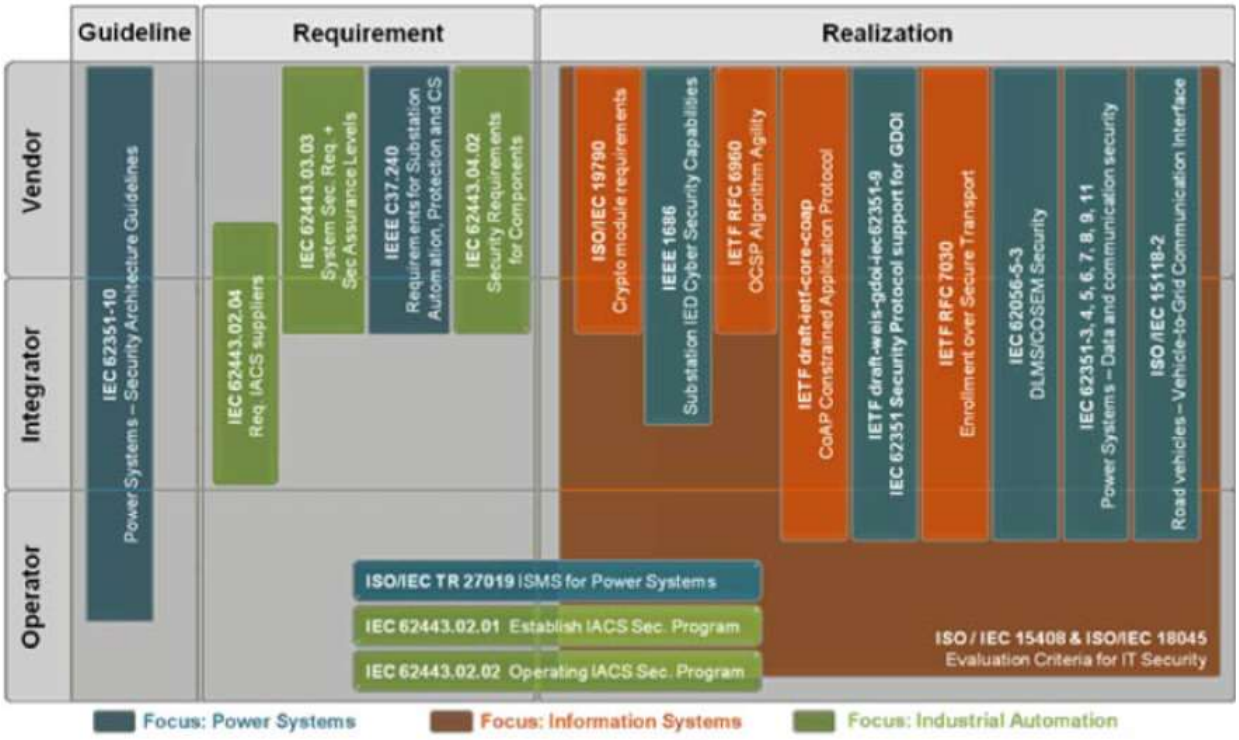

*Fuente: CENELEC*

El segundo enfoque muestra la aplicabilidad y el alcance de cada una de las normas desde una perspectiva un tanto diferente. La diferenciación en la Figura 2 es de la siguiente manera:

- **Guía:** El documento proporciona directrices y mejores prácticas para implementaciones de seguridad. Esto también puede comprender prerrequisitos disponibles para la implementación.
- **Requisito:** El documento contiene los requisitos genéricos para productos, soluciones o procesos. No se incluyen requisitos de implementación.
- **Realización**: El documento define la implementación de medidas de seguridad (realizaciones específicas). Nota, si es factible la distinción, el nivel de detalle del documento crece desde el lado izquierdo al derecho de la columna.
- **Proveedor**: El estándar aborda aspectos técnicos pertinentes para los productos o componentes.
- **Integrador:** El estándar define aspectos de integración, que tienen implicaciones en el diseño técnico, es relevante para los procesos de los proveedores (requieren ciertas características para ser compatibles), o exige interoperabilidad de los productos (por ejemplo, las implementaciones de protocolos).
- **Operador:** El estándar define aspectos de operación y / o de procedimiento, que se centran principalmente en la realización de servicios y aprovisionamiento en un sitio de operador.

Algunas de las normas sólo cubren parcialmente una determinada zona vertical. La interpretación de una cobertura en parte es que la norma puede no proporcionar requisitos explícitos para el vendedor / integrador / operador. Normas que cubren múltiples áreas horizontales abordan los requerimientos y también proporcionan aproximaciones a la solución en un nivel abstracto. Para la implementación pueden necesitarse normas o directrices adicionales.

**Figura 2. Estándares de ciberseguridad más importantes y su campo**




*Fuente: CENELEC*

Como se ha mostrado hay varias normas disponibles y maduras para utilizarlas en aplicaciones de redes inteligentes. Sin embargo todavía persiste la necesidad de investigar en nuevas normas y su cobertura de las necesidades específicas de las RI. Por lo tanto, el análisis de los huecos normativos, es un proceso continuo, lo que requerirá una mayor investigación sobre las normas existentes y futuras que aborden la evolución de las necesidades de seguridad de la información de las RI.

## ***Lista de estándares***

Para la evaluación general de la seguridad, se usa la norma ISO 27001/2, que especifica la evaluación de los riesgos para un sistema de cualquier tipo y la estrategia para el desarrollo del sistema de seguridad que mitigue esos riesgos. Por otra parte, la norma ISO 28000 especifica la gestión de la seguridad específicamente para una cadena de suministro.

***IEEE 1686: Norma IEEE para capacidades de seguridad cibernética en dispositivos electrónicos inteligentes (IED) de subestaciones.***

Esta norma procede del NERC CIP (Corporación para la Confiabilidad Eléctrica de América del Norte - Protección de Infraestructuras Críticas). La norma es aplicable a cualquier IED en el que se requiera "seguridad, responsabilidad y capacidad de auditoría en la configuración y mantenimiento de la IED".

La norma propone diferentes mecanismos de protección de los IED. El IED deberá:

- Ser protegido por combinaciones únicas de ID de usuario y contraseña. La contraseña debe tener un mínimo de 8 caracteres con al menos una letra mayúscula y minúscula, un número y un carácter alfanumérico.

- No debe existir ningún medio para saltarse la protección usuario ID / contraseña. Los mecanismos tales como "contraseñas maestras, rutinas de autodiagnóstico que automáticamente se ejecutan en caso de fallos de hardware o de software y vías alternativas de acceso sin contraseña como jumpers o interruptores de configuración" no deben estar presentes.
- Soportar diferentes nivel de utilización de las funciones y características del IED basado en perfiles de usuario según las combinaciones usuario ID / contraseña.
- Cerrar automáticamente la sesión de un usuario, después de un periodo de inactividad.
- Registrar en una memoria cíclica secuencial (primero en entrar, primero en salir) una lista eventos en el orden en el que ocurren.
- Supervisar la actividad relacionada con la seguridad y hacerla disponible al SCADA usando protocolos de comunicación en tiempo real.

***IEC 62351: Gestión de sistemas de energía y el intercambio de información asociada -seguridad de datos y comunicaciones***

IEC 62351 consiste en una serie de documentos que especifican los tipos de medidas de seguridad para los sistemas y redes de comunicaciones incluyendo distintos perfiles, tales como TCP / IP, Especificación de Mensajes para Fabricación (MMS) y IEC 61850. Algunas medidas de seguridad incluidas en la norma son:

- Autenticación para minimizar la amenaza de ataques, los descuidos y las acciones de los empleados descontentos;
- La autenticación de entidades a través de firmas digitales;
- Confidencialidad de las claves de autenticación y de mensajes a través de encriptación;
- Detección de manipulación;
- Prevención de la reproducción y la suplantación de identidad;
- Seguimiento de la infraestructura de comunicaciones en sí misma.

**Tabla 4. Estándares de ciberseguridad**

| Capa/tipo | Standard | Comentarios |
|---|---|---|
| General | IEC 62351-1 | Explica la serie de estándares IEC 62351 |
| General | IEC 62351-2 | Glosario de términos de IEC 62351 |
| Componente, comunicaciones, información, función | IEC 62351-3 | Uso TCP/IP, perfil TLS |
| Componente, comunicaciones, información, función | IEC 62351-4 | Uso TCP/IP y MMS |
| Componente, comunicaciones, información, función | IEC 62351-5 | Uso de EN 60870-5 protocolos serie |
| Componente, comunicaciones, información, función | IEC 62351-6 | Uso de GOOSE y SMV |
| Componente, comunicaciones, información, función | IEC 62351-7 | Protocolos y funciones para gestión de red con SNMP. |

| | | |
|---|---|---|
| Componente, comunicaciones, información, función | IEC 62351-8 | Control de acceso basado en roles y credenciales en el contexto de IEC 62351 |
| Componente, comunicaciones, información, función | IEC 62351-11 | Se centre en la seguridad de los ficheros XML para asegurar que el receptor dispone de información sobre la sensibilidad de los datos recibidos |
| Componente, comunicaciones, información, función | IEC 62351-10 | Aplicación de seguridad en sistemas de potencia |
| General | IEEE P2030 | Guía de interoperabilidad entre tecnología energética y de información con el Sistema de potencia eléctrico |

*Fuente: CIRCE*

## 1.2 Interoperabilidad

***Introducción***

El desarrollo de la red inteligente será una transición a largo o medio plazo, pues el punto de partida es un sistema eléctrico operativo que irá mejorando progresivamente. En el lado de los consumidores la tendencia va hacia un despliegue progresivo de contadores inteligentes, mientras que en la red de distribución se instalan equipos para vigilar y controlar la red, para medir la calidad de energía, etc.

La RI como sistema no puede ser diseñada desde cero, sino como un proceso progresivo de transformación. Esto significa que los modelos de negocio y las funciones del mercado, por un lado, y los componentes tecnológicos, por otra parte, han de ser transformados desde su estado actual de una manera paulatina. Debido a la escala del sistema y su importancia económica, un error de planificación en el funcionamiento y funcionalidad del sistema, podría suponer altos costes. A fin de permitir un proceso de migración bien estructurado, los requisitos para migrar a la red inteligente desde el sistema actual, tienen que ser establecidos usando un modelo apropiado.

Los ciclos de vida de la componente TIC y del equipamiento eléctrico primario pueden ser diferentes. Las componentes de las TIC utilizadas en la red actualmente, tienen una vida útil de entre 10 y 15 años, mucho menor que la vida media del equipamiento eléctrico que es de más de 30 años. Además de eso, una de las principales preocupaciones es la obsolescencia tecnológica debido a la velocidad cada vez mayor de aparición de las nuevas evoluciones de los componentes de TIC poniendo en riesgo la viabilidad económica de las inversiones en elementos de la red basados en componentes de TIC.

En el sector de las TICs la próxima gran tendencia serán las arquitecturas de back-office, basadas en estándares abiertos, interoperabilidad y un diseño modular de componentes que puedan interactuar con mayor facilidad. Las innovaciones en las áreas de computación en la nube, la tecnología de agentes, Internet de las cosas, entre otras, también permitirán esta transición y serán un catalizador para sistemas verdaderamente distribuidos y arquitecturas descentralizadas más simples. Las arquitecturas centralizadas serán reemplazadas cada vez más por variantes distribuidas / descentralizados interoperables entre sí.

A medida que se añaden más componentes TICs a la infraestructura eléctrica, la interoperabilidad es un requisito clave para una red inteligente robusta, fiable y segura. La manera de lograr la interoperabilidad

pasa por la especificación detallada del sistema, a través del uso de estándares, y su testeo por medio de pruebas sistemáticas.

Aunque la mayoría de los equipos de red inteligente se basan en estándares (inter)nacionales, esto no se traduce automáticamente en una infraestructura de red inteligente interoperable. Esto se debe en parte a la falta de comprensión de lo que significa la interoperabilidad, lo que puede esperarse de ella y lo que se debe hacer para implementarla.

Este documento define primero diversos términos y discute conceptos relacionados con la interoperabilidad como la conformidad, la compatibilidad y la intercambiabilidad y proporciona una metodología para alcanzar el nivel deseado de interoperabilidad.

La interoperabilidad entre sistemas en una red inteligente debe ser considerada y especificada mediante los casos de uso, para que los desarrollos sean interoperables por diseño. Los casos de uso sirven de base para la especificación de requisitos funcionales, requisitos no funcionales, casos de prueba y perfiles de prueba.

Con respecto a la normalización, el usuario (operador de red, proveedor de servicios de energía, grupos de usuarios, etc.) necesitará especificar en detalle cómo se utilizará la norma específica (o conjunto de normas) y qué opciones de las mismas se emplearán con el fin de lograr el caso de uso deseado. Esta es la etapa de creación de perfiles.

La definición de un perfil de aplicación puede ser un paso importante para lograr la interoperabilidad ya que puede reducir el número de opciones y la complejidad de la norma completa. La interoperabilidad en el dominio de red inteligente se ve facilitada por el uso de un modelo de arquitectura, como por ejemplo el modelo de SGAM.

Para probar si el sistema es interoperable dentro de la red inteligente, se deben realizar dos tipos de pruebas: pruebas de conformidad y pruebas de interoperabilidad.

Las pruebas de conformidad consisten en un proceso independiente, para garantizar que el sistema se ajusta a las normas o perfiles seleccionados. Después de las pruebas de conformidad, el sistema se conectará con otros sistemas en la red inteligente y se realizarán las pruebas de interoperabilidad para asegurar que las funcionalidades operan correctamente dentro de los límites establecidos.

***Recomendaciones generales***

- Para evitar malentendidos, se recomienda utilizar una única definición de términos relacionados con la interoperabilidad.
- Si la compatibilidad hacia atrás dentro de las versiones de un estándar no es posible, debe considerarse la posible necesidad de una estrategia de migración.
- El diseño del sistema se debe basar siempre en las necesidades de los usuarios. Por lo tanto la creación de perfiles debe ser una responsabilidad de los grupos de usuarios directamente interesados.
- Es necesaria la adecuada formación de todos los interesados para lograr un entendimiento común sobre cómo generar perfiles, siguiendo una metodología concreta.
- Para alcanzar el nivel necesario de interoperabilidad puede ser necesario que los usuarios dispongan de prototipos para evaluar la conformidad, sobre todo para los dispositivos más relevantes del sistema.

## ***Recomendaciones para la implementación***

### *Análisis funcional*

- Seleccionar los casos de uso aplicables de tal manera que los casos de uso y los diagramas de secuencia relacionados puedan considerarse suficientes para definir los requisitos funcionales. Si no hay ningún caso de uso disponible, es necesario crearlos primero.
- Definir en qué capas se requiere interoperabilidad para cumplir con los requisitos funcionales de un caso de uso (negocios, funcional, información, comunicación y componentes).

### *Selección de estándares y especificaciones*

- Definir las interfaces físicas requeridas y los canales de comunicación entre objetos.
- Seleccionar las normas para cada interfaz dentro de cada capa requerida e identificar las deficiencias en las pruebas de conformidad o en el conjuntos de normas.

### *Perfiles basados en normas y especificaciones; el perfil se basa en los requerimientos del negocio / funcionales.*

- Construir perfiles de interoperabilidad para cada (conjunto de) normas y especificaciones con posible retroalimentación en el desarrollo de la normalización; esto incluye los perfiles básicos de aplicación (BAP) y Perfiles básicos de interoperabilidad de aplicaciones (BAIOPs).
- Aplicar los perfiles en el diseño de sistemas y fase de pruebas.
- Administrar perfiles bajo la responsabilidad de los grupos de usuario, incluyendo:
    - Aclaración sobre las responsabilidades y roles de los diferentes actores que están involucrados para crear y gestionar perfiles.
    - Gestión del cambio, mantenimiento y control de versiones de los perfiles actualizados con experiencias de campo, pruebas y otras realimentaciones.
    - Comunicación de los cambios a los interesados afectados.

Si no existen grupos de usuarios para ciertas áreas de redes inteligentes, deben, no obstante, crearse para satisfacer los requisitos de interoperabilidad.

Después de que los perfiles han sido desarrollados por los grupos de usuarios, debe procederse a la implementación en proyectos reales. El usuario que participa en el proyecto es el responsable del desarrollo y mantenimiento de perfiles de aplicación. El usuario también será responsable de las experiencias de retroalimentación, implementaciones y opciones de los grupos de usuarios.

Dado que tanto la creación y aplicación práctica de los perfiles pueden conducir al descubrimiento de nuevas lagunas de normalización, los grupos de usuarios responsables deberían retroalimentar sus lecciones aprendidas directamente a los comités de normalización correspondientes, ya sea a nivel nacional o internacional, si procede.

Un perfil requiere un diseño, formato, sintaxis y estructura adecuado para garantizar la aplicación por diferentes usuarios de una manera inequívoca.

## ***Recomendaciones sobre las pruebas***

- Para verificar el nivel deseado de interoperabilidad se necesitan pasar las siguientes pruebas: tipo de test, pruebas de código, pruebas de integración, prueba del sistema, prueba de aceptación de fábrica, prueba de aceptación en campo.

- Se recomienda que todas las pruebas realizadas sean debidamente documentadas, de modo que terceros puedan repetir las pruebas y verificar los resultados.

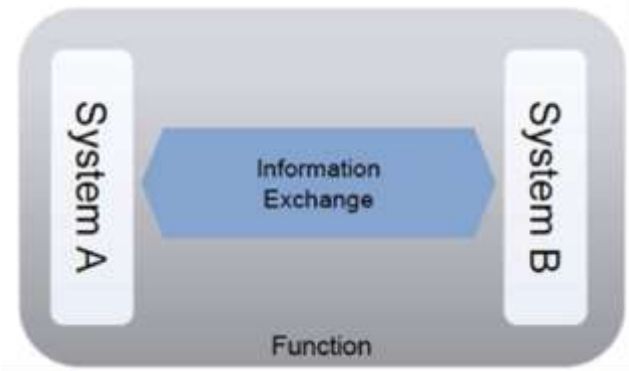
## ***Conceptos y terminología***

La interoperabilidad es la capacidad de dos o más redes, sistemas, aplicaciones, componentes o dispositivos de los mismos o diferentes fabricantes, de intercambiar y posteriormente utilizar esa información con el fin de realizar las funciones requeridas (IEEE 610).

Si dos o más sistemas son capaces de comunicar e intercambiar datos, están exhibiendo interoperabilidad sintáctica. Los formatos de datos específicos (por ejemplo, XML), los protocolos de comunicación (TCP / IP) y similares son herramientas fundamentales de la interoperabilidad sintáctica. Esto también es válido para los formatos de datos de bajo nivel, como por ejemplo, asegurar que los caracteres alfabéticos se almacenan en un mismo formato ASCII o Unicode (para inglés o texto internacional) en sistemas de comunicación. La interoperabilidad sintáctica es una condición necesaria para hacer posible una mayor interoperabilidad.

Este concepto se ilustra en la Figura 3.

**Figura 3. Interoperabilidad sintáctica**



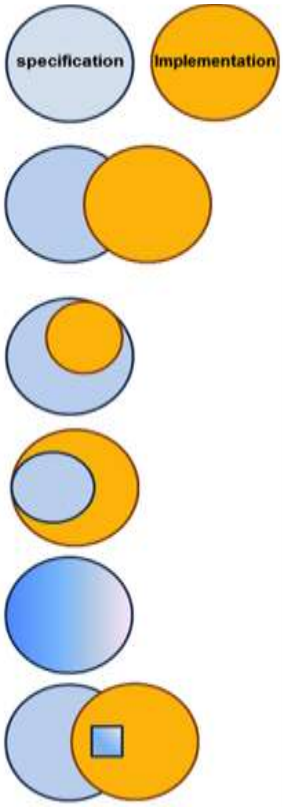

*Fuente: IEEE 610*

Al estar formulado de manera general, este concepto es válido también para RI. Los avances tecnológicos y la competencia pueden cambiar la naturaleza y la interoperabilidad de los componentes en una red inteligente.

Aunque la interoperabilidad debe ser un objetivo primario, podría ser necesario aceptar un menor grado de interoperabilidad de la red inteligente, si un producto, sistema o nuevo estándar ofrece beneficios que superan cualquier desventaja en términos de interoperabilidad.

La Figura 4 muestra una imagen clara de los términos utilizados al hablar de interoperabilidad en redes inteligentes, dispositivos, sistemas y subsistemas.

**Figura 4. Interoperabilidad. Definición de términos**




**Irrelevante:** La implementación no tiene nada que ver con la especificación**.**

**Consistente**: La implementación tiene algunas características soportadas por la norma. Sin embargo se implementan características fuera de norma y parte de la norma no se implementa.

**Cumplimiento:** Toda la aplicación está de acuerdo con los requisitos o normas especificadas. Sin embargo, algunos de los requisitos de los estándares especificados no se pueden implementar.
**Conformidad**. Todas las características de la norma / especificación se implementan adecuadamente, pero se añaden algunas características que pueden no estar incluidas en la norma / especificación.

**Total conformidad**. Todas las características de la norma / especificación se implementan adecuadamente, y no hay características implementadas que no estén incluidas en la norma / especificación.

**No conforme**. Se implementan algunas características de la norma pero no según se especifica en ella.

*Fuente: Interoperabilidad, WIKITEL*

Adicionalmente se definen:

## ***Pruebas de conformidad***

El acto de determinar en qué medida una implementación se ajusta a los requerimientos. Una condición importante para lograr la interoperabilidad es la correcta aplicación de las normas. Esto puede ser verificado mediante pruebas de conformidad.

Se determina si una aplicación se ajusta a un perfil según se establece en el protocolo de declaración de conformidad de la implementación (PICS). Las pruebas pueden serlo de interoperabilidad si el perfil cubre los requisitos de interoperabilidad adicionales a los requisitos de pruebas de conformidad de las normas aplicadas. Las pruebas de conformidad son un requisito previo para las pruebas de interoperabilidad.

## ***Perfil de interoperabilidad***

Un perfil es un documento que describe cómo se implementan las normas o especificaciones para soportar los requisitos de una aplicación particular, función o contexto.

## ***Pruebas de Interoperabilidad***

Las pruebas de interoperabilidad se realizan para verificar que las entidades que se comunican dentro de un sistema son interoperables, es decir, son capaces de intercambiar información de manera semántica y sintácticamente correcta. Durante las pruebas de interoperabilidad, las entidades se ponen a prueba según los perfiles definidos.

## ***Conformidad***

Conformidad significa que la implementación de un producto, proceso o servicio incluye todos los requisitos especificados en las normas y además, la implementación se realizado de acuerdo con lo establecido en el estándar o norma elegida. Es usual que los estándares incluyan la forma de evaluar la conformidad:

- Se describe la función y el comportamiento del producto, en lugar de su diseño.
- Proporciona especificaciones cuantificables precisas.
- Establece pruebas y métodos fiables y reproducibles.

La conformidad se puede evaluar con un estándar nacional o regional, o, en general con cualquier especificación. La conformidad con los estándares permite que exista interoperabilidad, pero no la garantiza.

## ***Compatibilidad***

La compatibilidad se refiere a la capacidad de dos o más sistemas o componentes para realizar sus funciones sin necesidad de modificación o transformación alguna, compartiendo el mismo entorno (IEEE 610)

Dos componentes (o sistemas) también pueden ser compatibles, pero realizar funciones completamente separadas. No tienen que comunicarse entre sí, sino que simplemente están ubicados en el mismo entorno - así que la compatibilidad no se refiere a la interoperabilidad.

## ***Intercambiabilidad***

La intercambiabilidad es la capacidad de dos o más dispositivos o componentes de ser intercambiados sin realizar cambios en otros dispositivos o componentes en el mismo sistema y sin que resulte degradado el rendimiento del mismo. Los dos dispositivos no se comunican, pero uno puede sustituir al otro: intercambiabilidad no es equivalente interoperabilidad.

A medida que más y más componentes de TIC están conectados a la infraestructura eléctrica, la interoperabilidad es un requisito clave para un sistema robusto, fiable y seguro. La conformidad del sistema o la compatibilidad no es suficiente para lograr este objetivo.

La interoperabilidad no necesita resultar en intercambiabilidad por varias razones; la huella hardware y eléctrica necesaria para la intercambiabilidad puede estar en contradicción con los requisitos de rendimiento, configuración y capacidad de desarrollo tecnológico. Las mejoras en interoperabilidad puede implicar la pérdida de la capacidad de intercambio.

Generalmente es suficiente tener interoperabilidad, en lugar de intercambiabilidad. Sin embargo, en ciertas situaciones, puede ser necesaria la intercambiabilidad.

### ***La interoperabilidad en la red inteligente: El modelo SGAM***

La RI considerado como sistema, muestra una alta complejidad en relación con aspectos organizativos y tecnológicos. Varios actores participan en la planificación y construcción del sistema, representando a varias organizaciones y dominios de ingeniería. Por lo tanto, un desafío clave de la red inteligente es la integración, que afecta a los componentes de generación, transporte, distribución, almacenamiento y consumo de energía eléctrica y a los sistemas y aplicaciones de información de apoyo.

Para crear la red inteligente como un sistema de sistemas operativo, las funcionalidades e interfaces de sus componentes se deben especificar de antemano. El cumplimiento de requisitos supone un factor decisivo para las actividades de ingeniería adicionales, por lo que es esencial una metodología adecuada para la especificación y gestión de requisitos. Se asegura así la trazabilidad de las decisiones de diseño y requisitos del sistema, se apoya la colaboración entre las partes interesadas mediante la asignación de responsabilidades, se permite la estructuración del sistema en software y hardware y, finalmente, se facilita comprobar si la implementación realizada cumple la especificación.

La RI como un sistema no puede ser diseñada desde cero. En su lugar, el desarrollo de la RI debe caracterizarse por un proceso de transformación. Esto significa que los modelos de negocio y las funciones del mercado, por un lado, y los componentes técnicos y la arquitectura del sistema, por otra parte, han de ser transformados progresivamente desde su estado actual.

La interoperabilidad representa un requisito esencial para la red inteligente, ya que se trata de integrar diferentes activos y aplicaciones en un sistema funcional. Con el fin de apoyar la obtención y gestión de requisitos, se debe utilizar una estructura adecuada.

El modelo SGAM es una posibilidad para ello.

## 1.3 Metodología e identificación de casos de uso para facilitar la interoperabilidad

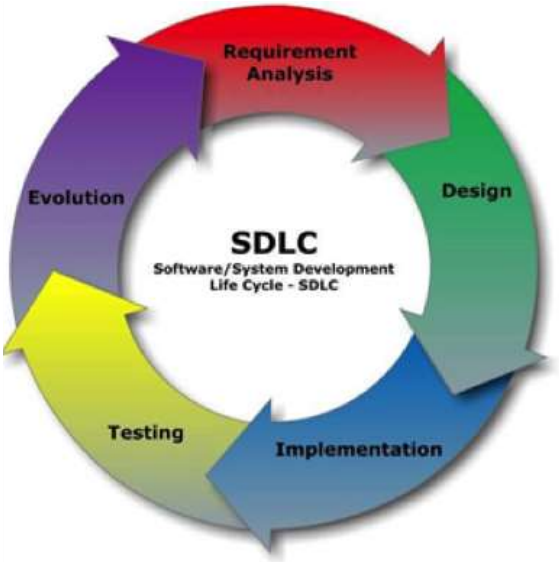
Como ya se ha discutido en la sección anterior, el uso de estándares facilita la interoperabilidad a través del diseño cuando se aplica la metodología correcta. El uso de estándares no resultará en un sistema interoperable. Hay otros factores que deben tenerse en cuenta para alcanzar la interoperabilidad tales como:

- El diseño de un sistema de red inteligente o la transformación de uno existente en uno interoperable utilizando metodologías como SGAM.
- Recogida de requisitos de interoperabilidad durante la identificación de casos de uso.
- Validación de la interoperabilidad del sistema a través de pruebas.

### ***Diseño del sistema***

El Ciclo de Vida de Desarrollo de Software para sistemas TICs es una metodología ampliamente utilizada que garantiza la entrega de software de alta calidad o un sistema eficaz y eficiente. Esta metodología se puede aplicar también al desarrollo de los sistemas de la RI. La Figura 5 muestra el ciclo de vida de desarrollo del sistema.

**Figura 5. Ciclo de diseño de un sistema**



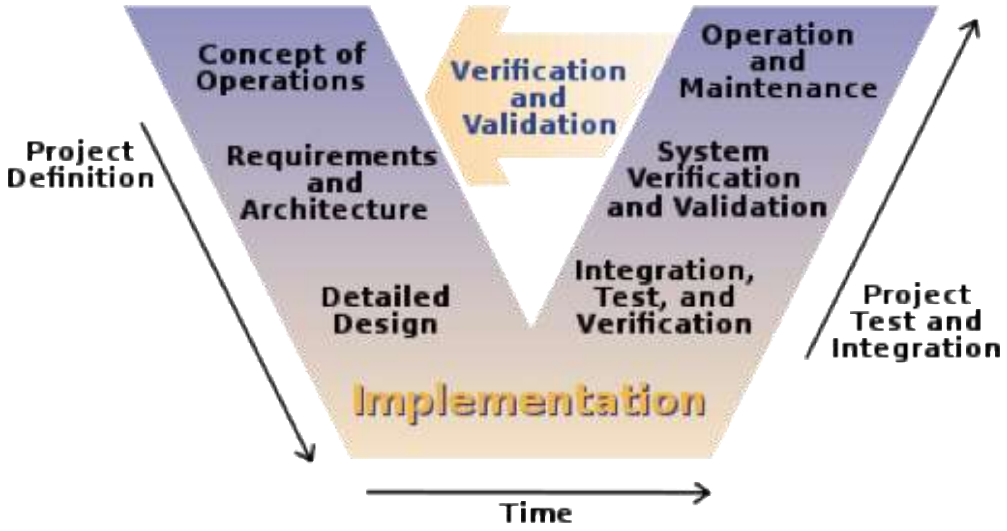

*Fuente: https://es.wikipedia.org/wiki/Systems_Development_Life_Cycle*

Hay cinco etapas en el ciclo de vida:

- Análisis de requerimientos.
- Diseño.
- Implementación.
- Pruebas.
- Evolución.

Cada etapa tiene sus propias actividades, tareas, entradas, resultados y entregables. Dependiendo de qué método se utiliza para el desarrollo del ciclo de vida (por ejemplo, modelo de cascada, modelo en V (Figura 6, etc.), el proceso puede ser ligeramente diferente. En general, en la etapa de análisis de requisitos se desarrolla una descripción del comportamiento del sistema o software, y en algunos casos se podrán obtener conclusiones iniciales sobre la viabilidad técnica. La descripción del comportamiento del sistema o software se puede realizar a través de casos de uso y especificaciones de requisitos funcionales y no funcionales.

**Figura 6. Modelo en V**




*Fuente: https://en.wikipedia.org/wiki/V-Model_(software_development)*

En la etapa de diseño, se considerará el concepto de solución y su arquitectura. La realización de la solución se desarrollará durante la etapa de implementación. En la fase de prueba, se validarán las soluciones implementadas. Los defectos del sistema o software se reportarán para su posterior corrección. Tras la instalación y puesta en marcha del sistema o software en un entorno de producción, se pueden recoger experiencias prácticas de mantenimiento y operación, que permitan, en la siguiente iteración del ciclo de vida, incluir nuevos requisitos para ampliar o mejorar el sistema o software con respecto a su facilidad de uso, rendimiento, etc.

De acuerdo con la metodología del ciclo de vida de desarrollo de sistemas, los requisitos y especificaciones se generan en la primera etapa. Para conseguir sistemas TIC interoperables en la RI, los requisitos de interoperabilidad se deben incluir en esta etapa.

El modelo SGAM define el desarrollo de casos de uso como punto de partida para la definición de requisitos funcionales y técnicos. Las cinco capas de interoperabilidad pueden desarrollarse a partir de este modelo.

Dado que el desarrollo del ciclo de vida es un proceso iterativo, pueden aparecer nuevas versiones de estándares o productos, por lo que la compatibilidad con versiones anteriores de las normas y productos tienen gran influencia sobre la interoperabilidad del sistema. Por lo tanto una herramienta de gestión de versiones coherente puede ayudar a los usuarios a comprobar e identificar la interoperabilidad del sistema a lo largo del tiempo. En el peor de los casos, sería necesaria una migración para garantizar aún más la interoperabilidad del sistema.

Se describe a continuación, una metodología para alcanzar la interoperabilidad de los sistemas de redes inteligentes. Desde el punto de vista del desarrollo del ciclo de vida, la compatibilidad y gestión de versiones son los factores que tienen mayor influencia sobre la interoperabilidad del sistema.

### ***Identificación, creación y selección de casos de uso.***

Un caso de uso es una descripción de las posibles secuencias de interacciones entre el sistema en discusión y sus actores externos, relacionados con una meta particular. Desde un punto de vista de

interoperabilidad, los sistemas son interoperables si dos o más sistemas son capaces de realizar cooperativamente una función específica mediante el uso de la información que se intercambia. El caso de uso describe el comportamiento exacto de los sistemas y sus interacciones.

Los casos de uso sirven de base para la identificación de un sistema, su funcionamiento, los actores, la interacción y las interfaces. Los requisitos funcionales y no funcionales se pueden desarrollar y especificar con la ayuda de descripciones de casos de uso. Además, un caso de uso proporciona una base para la definición de casos y perfiles de prueba para las pruebas de conformidad y de interoperabilidad. Y también sirve como base para las pruebas de aceptación.

IEC / PAS 62559 desarrolló un enfoque basado en casos de uso para el diseño de sistemas de energía. El SG-CG / SP (Grupo de Coordinación de RI - Proceso Sostenible) adecuó y ajustó la plantilla de caso de uso para su propósito. En base a estos resultados, el Comité Técnico IEC TC 8 decidió transformar IEC / PAS 62559 en una nueva IEC 62559 con cuatro sub-partes. La IEC 62559-1 describe un enfoque basado en casos de uso para la normalización. La IEC 62559-2 especifica las plantillas para los casos de uso, lista de los actores y la lista de requisitos. La IEC 62559-3 proporciona la definición de plantillas de casos de uso en formato serializado XML con el fin de intercambiar casos de uso entre diferentes repositorios de casos de uso o con herramientas de ingeniería como UML. El antiguo IEC/PAS 62559 se trasladó a la norma IEC 62559-4.

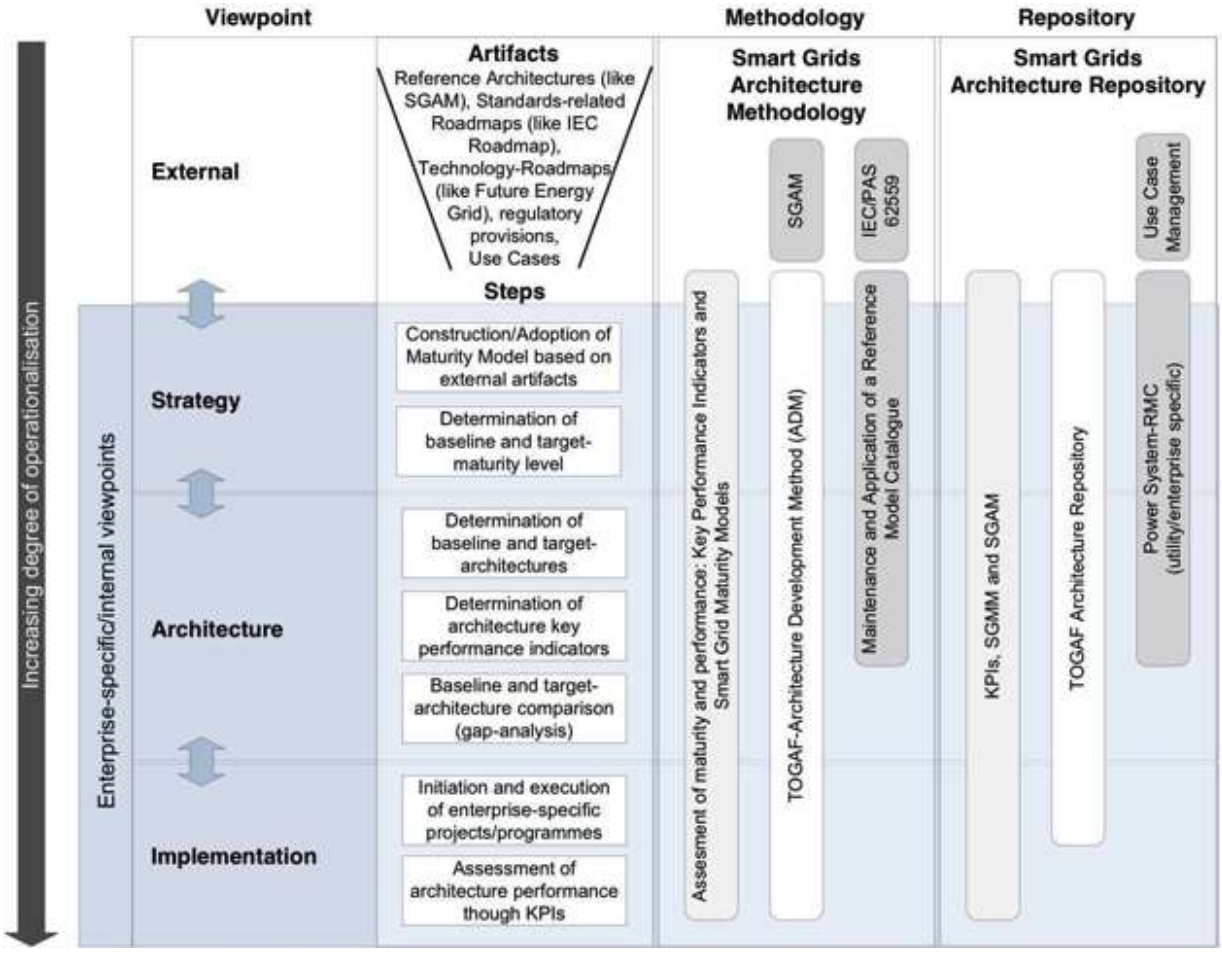
El detalle de procesos, plantillas y ejemplos de identificación, creación y selección de casos de uso se pueden encontrar en la norma IEC 62559. Desde el punto de vista de la interoperabilidad, deben tenerse presente los siguientes aspectos durante el procesado de casos de uso:

- Revisión y validación de la narrativa de casos de uso.
- Validación de los actores y roles intervinientes en los casos de uso. La definición de los actores y roles debe ser compatible con las definiciones recogidas en el estándar de RI que se elija, para que estos puedan ser interpretados por todas las partes correcta y claramente.
- La discusión de los escenarios o pasos a incluir en los casos de uso. Para ello es recomendable el uso de los pasos indicados en la plantilla de la norma IEC 62559-2 y las características del documento de interoperabilidad. En la descripción de los pasos debería haber una clara correlación entre la narrativa y los pasos. La descripción de los pasos debe centrarse en las interacciones y los flujos de información entre los actores. Todas las interacciones y flujos de información deben ser compatibles con el estándar de RI (el caso de uso debe ser desarrollado en pasos iterativos de lo simple al detalle, en función de la finalidad). Se deben utilizar interfaces y protocolos estandarizados para el intercambio de información entre los sistemas. Existen normas disponibles para las capas de información, comunicación y componente, tal como se recoge en este informe.
- Desarrollo de requisitos a partir de los casos de uso. El proceso de mapeo de casos de uso en una arquitectura (por ejemplo SGAM) se debe utilizar para seleccionar los estándares, interfaces y protocolos pertinentes. Los casos de uso describen las funciones del sistema. El proceso comienza con las capas de negocio / funcionales (funciones, procesos y actores). El primer paso para el mapeo será la identificación de dominios y zonas, que se ven afectados por los casos de uso. Esquematizar la cobertura del caso de uso en el plano de red inteligente (dominios y zonas) y distribuir los sistemas o componentes en las ubicaciones apropiadas en el plano de red inteligente. El desarrollo de la capa de componentes consiste en mapear el diagrama de casos de uso (actores y sistemas) a un dominio SGAM. Para la capa de información, es importante partir de la descripción de casos de uso para identificar qué datos o información tienen que ser intercambiados entre los componentes y funciones. Basado en el tipo de información intercambiada, se define el modelo de datos atendiendo al estándar correspondiente. Después de

completar la asignación de la capa de información, el paso final es el desarrollo de la capa de comunicación. Sobre la base de la ubicación del sistema en el dominio SGAM se pueden definir los protocolos de comunicación.

La Figura 7 esquematiza el proceso explicado. Los planes de ruta proporcionan un punto de partida, a partir del cual se añaden los casos de uso y plantillas estructuradas, así como ciertos estándares fundamentales. Sobre esto tratan los repositorios de casos de uso, el IEC PAS 62559 y los modelos SGAM. A partir de esto, tiene que realizarse la implementación y posteriormente evaluar el éxito y los costes. Existen modelos para chequear la interoperabilidad entre los componentes como los SGIMM, métodos de desarrollo de arquitectura y los entornos como TOGAF, modelos funcionales SGAM y otros catálogos.

**Figura 7. Selección y generación de casos de uso**




*Fuente: SGAM, Proceso de mapeo de casos de uso en una arquitectura*

## 1.4 Metodología general de definición de perfiles

La interoperabilidad, en general, se puede aplicar entre las interfaces de cualquier capa que se requiera para cumplir con un caso de uso. Esto significa que primero deben definirse las capas implicadas para un caso de uso dado y detallarse toda la funcionalidad.

Sobre la base de las capas SGAM, los estándares pueden considerarse desde una perspectiva de capa de negocio o de función. Dependiendo del caso de uso, lo dicho es de aplicación principalmente a los estándares y especificaciones que deben ser considerados para la interconexión de objetos dentro de un sistema en:

- Capa de negocio.
- Capa de funciones.
- Capa de la Información.
- Capa de Comunicación.
- Capa de componentes.

Los perfiles son documentos que describen cómo se implementan las normas o especificaciones para soportar los requisitos de un caso de uso particular, o un conjunto de casos de uso. Las recomendaciones en el proceso de definición de un perfil se recogen en las siguientes etapas:

**a) Análisis funcional**

- Selección del caso de uso aplicable o un conjunto de casos de uso, ya que el caso de uso y los diagramas de secuencia relacionados podrían considerarse suficiente como para definir los requisitos funcionales. Si no hay ningún caso de uso disponible en las distintas librerías de consulta, es necesario crearlo primero.
- Definir en qué capas (información, comunicación o componentes) se requiere la interoperabilidad para cumplir con los requisitos funcionales del caso o conjunto de casos de uso.

**b) Normas y selección especificación**

- Definir las interfaces físicas requeridas y los canales de comunicación entre objetos.
- Seleccionar el conjunto de estándares para cada interfaz dentro de cada capa requerida, usando una herramienta que facilite el diseño de la interoperabilidad (por ejemplo la descrita en (CEN-CENELEC-ETSI Smart Grid Coordination Group, 2014) e identificar las deficiencias en las pruebas de conformidad / cumplimiento en el conjunto de estándares.

**c) Perfiles basados en estándares**

- Construir perfiles de interoperabilidad para cada conjunto de normas y especificaciones con posible retroalimentación en el desarrollo de la normalización.
- Aplicar los perfiles en el diseño de sistemas y fase de pruebas.
- Administrar perfiles.

## 1.5 Selección de estándares y especificaciones

### *Definición de interfaces físicas requeridas y canales de comunicación entre los objetos*

Por definición un perfil de interoperabilidad es un documento que describe cómo se implementan las normas o especificaciones para soportar los requisitos de un caso de uso particular, o un conjunto de casos de uso, por lo tanto, es crucial seleccionar previamente los estándares o especificaciones requeridas.

Las normas relevantes para diferentes aplicaciones dentro de cada capa se pueden seleccionar con una herramienta como la descrita en (CEN-CENELEC-ETSI Smart Grid Coordination Group, 2014). Por tanto, es importante que los casos de uso se desarrollen generalmente bajo la aplicación de la metodología y la

plantilla de la norma IEC 62559-2, y se procesen de acuerdo con un modelo, por ejemplo el SGAM, incluyendo el mapeo de los sistemas en el plano de red inteligente del modelo elegido.

### ***Selección de las normas de uso con una herramienta de apoyo***

Una herramienta de apoyo para el diseño de la interoperabilidad ayuda a identificar las normas pertinentes mediante el filtrado de capas, sistemas y zonas. La aplicación de la herramienta requiere el uso de ciertas convenciones utilizadas para determinar la capa de componente, la comunicación y la información de un sistema de acuerdo con el modelo elegido. Esto da lugar a múltiples conjuntos de normas para cada caso de uso en el que todos los estándares requeridos dentro de un conjunto deben ser interoperables y pueden requerir un perfil específico de interoperabilidad.

La selección de las normas también se necesita para representar los requisitos de la fase de diseño del sistema según el Modelo en V (Figura 7). En su caso, las normas para el análisis de requerimientos, el diseño del sistema, el diseño de arquitectura y el diseño de los módulos pueden evaluarse con el apoyo de la herramienta. Al revés, los estándares seleccionados también deben tomarse en consideración para las fases de prueba correspondientes al modelo en V (pruebas de cumplimiento, de conformidad, interoperabilidad y aceptación).

## 1.6 Perfiles

### ***Definición de un perfil***

Un perfil es una especificación que regula la información intercambiada dentro de un contexto de comunicaciones específico. Los perfiles se desarrollan para servir a las necesidades de información de ciertos grupos de usuarios. Estos grupos de usuarios pueden ser diversos y pueden caracterizarse ya sea por el contexto geográfico o por el dominio de la aplicación. Ejemplos de tales grupos de usuarios podrían ser, por ejemplo los operadores de transmisión o los operadores de distribución. Incluso podrían ser empresas individuales, es decir, empresas eléctricas o los propios fabricantes. Todos ellos pueden desarrollar sus propios perfiles, como subconjuntos de perfiles más genéricos de un grupo de usuarios. No obstante, por lo general, el objetivo es obtener perfiles de una amplia aceptación.

Uno de los propósitos más importantes de un perfil es ayudar a garantizar la interoperabilidad entre los sistemas. Mediante la adopción e implementación de un perfil aceptado es posible soslayar la laxitud de los estándares abiertos, que a veces pueden ser vagos o tener especificaciones ambiguas. El uso de perfiles supone elegir una de las posibles interpretaciones.

Un *companion* es un concepto que está estrechamente relacionado con un perfil, pero por lo general sólo se refiere al estándar básico. Un ejemplo de un *companion* es COSEM que incluye un conjunto de especificaciones que definen las capas de transporte y aplicación del protocolo DLMS o IEC 60870-5-104, que describe cómo se utiliza el estándar de telecontrol IEC 60870-5 a través de TCP / IP.

### ***Generación de Perfiles***

En general, la creación de perfiles dentro de un estándar o entre estándares y especificaciones ayuda a mejorar la interoperabilidad y cumplir con las expectativas de los diferentes proyectos en los que éstos se implementarán.

Las aplicaciones de redes inteligentes pueden ser diferentes, dependiendo del tipo de usuario, la región y la filosofía. Las partes implicadas necesitan directrices y herramientas para mejorar la interoperabilidad en

los proyectos y por lo tanto el desafío es encontrar un concepto / directriz común, para mejorar la interoperabilidad y cumplir con las expectativas de los diferentes proyectos.

Para facilitar el objetivo de la interoperabilidad, es necesaria una interpretación común de los estándares y el uso idéntico de elementos funcionales en las capas necesarias para cumplir las funciones de una aplicación. Esto puede lograrse mediante la definición de perfiles dentro de grupos de usuarios organizados alrededor de las áreas clave de la tecnología de redes inteligentes. Un grupo de usuarios se compone de las partes interesadas, por ejemplo, empresas, operadores, proveedores, organismos de certificación, laboratorios de ensayo, integradores de sistemas y los reguladores).

El proceso para crear un perfil comienza con un conjunto de casos de uso, la identificación de la necesidad de una interacción estandarizada entre un grupo de sistemas / aplicaciones para lograr un propósito comercial. La fuerza impulsora detrás de la creación de perfiles puede ser el organismo de normalización en sí, puede ser un grupo de usuarios que comparten un interés similar o dominio de aplicación, o una empresa individual que requiere la interoperabilidad de múltiples sistemas en un dominio de aplicación específico.

En la mayoría de los casos, un grupo de usuarios se reunirá periódicamente para discutir el alcance/propósito del problema y suministrar experiencia de campo para desarrollar las especificaciones técnicas que formarán el perfil.

El proceso de desarrollo y/o implementación de un perfil es de hecho similar a la de desarrollar un estándar común. Se seguirá el proceso de análisis de requisitos y casos de uso de desarrollo descrito.

El documento de perfil resultante puede ser presentado para su aprobación a una comunidad de usuarios más grande y/o a la organización de normalización. En tal caso, el perfil resultante en sí puede llegar a ser estandarizado. Sucesivamente, se puede crear una especificación de pruebas para el perfil, de modo que se puedan realizar pruebas de conformidad.

La metodología de definición de un perfil parte de un conjunto de pasos previos:

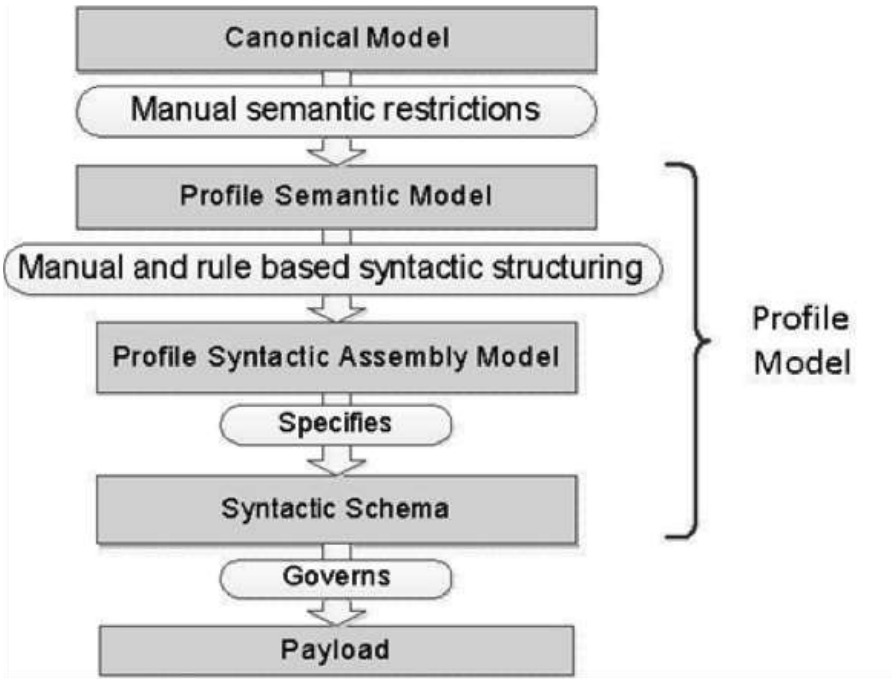
- El problema ya ha sido analizado para identificar los intercambios funcionales que deben ser estandarizados.
- Se han identificado los requisitos de datos de cada intercambio funcional.
- El modelo de información canónica se ha modificado según sea necesario con el fin de ser capaz de incluir todos los datos requeridos.

Un requisito fundamental para la metodología de creación de un perfil es que debe producir una especificación precisa y comprobable de los intercambios de datos entre las partes involucradas. Cuando se envían datos a través de la red, cada parte transmite paquetes de datos que incluyen tanto información de cabecera, como datos reales. La cabecera identifica principalmente la fuente y el destino del paquete, mientras que a los datos reales se les conoce como la carga útil. Teniendo en cuenta las capas inferiores del modelo OSI, la información del encabezado, o datos de cabecera, solo se utiliza en el proceso de transmisión, y se extrae del paquete cuando llega a su destino. Por lo tanto, la carga útil son los únicos datos recibidos por el sistema de destino.

Un ejemplo de definición de un perfil de la capa superior del modelo OSI para el estándar IEC “Common Information Model” se muestra en la Figura 8.

.

**Figura 8. Definición de un perfil CIM**




*Fuente: IEC "Common Information Model"*

El propósito de la especificación de un perfil para un intercambio de información basado en un estándar, es proporcionar toda la información que se requiere para generar e interpretar tramas de datos con información útil, por parte de los emisores y receptores de información, además de establecer la manera en la que una parte imparcial pueda juzgar el cumplimiento del perfil.

Esto requiere dos cosas, rigurosamente separadas, en la metodología de creación de perfiles:

- Un modelo semántico del perfil que especifica los elementos estructurales que capturan el contenido de la información. Lo que incluye los nombres de los campos de datos y la relación entre los campos de datos que componen los datos útiles.
- El modelo sintáctico que especifica cómo se serializa el modelo semántico para que pueda ser transferido desde el productor al consumidor, donde las partes pueden estar en diferentes entornos computacionales.

La recomendación es que el diseño, el formato, la sintaxis y la estructura de un perfil sean estandarizados para facilitar su aplicación por diferentes usuarios de una manera inequívoca y así simplificar la complejidad del modelo basado en cinco capas de interoperabilidad.

Un perfil debe contener al menos las siguientes características:

- Nombre del perfil.
- Requisitos, límites y escalabilidad.
- Topología de la red de comunicación (por ejemplo, sobre la base de la capa de componentes).
- Lista de los sistemas y tecnologías en su caso.
- Normas y especificaciones.
- Las consideraciones de seguridad.

- Los parámetros de configuración.
- Mejor enfoque según la práctica actual.

Como la entrada proporcionada por los estándares y especificaciones se basa en documentos, un perfil puede requerir, además, características adicionales como formatos de datos lectura directa por máquinas, etc.

### ***Perfiles de funciones básicas de la aplicación (BAP)***

Un perfil de aplicaciones básicas (BAP) se usa en la fase de diseño del modelo en V y se basa en la descripción de las funciones básicas de una aplicación dentro de un sistema/subsistema específico.

El término "básico" significa en este contexto, que se recomienda descomponer una función de aplicación en partes elementales (básicas) que deben ser la base para la definición de los perfiles de aplicación.

Un BAP es un acuerdo en la selección e interpretación de las partes relevantes de las normas y especificaciones aplicables y está destinado a ser utilizado como bloques de construcción para las especificaciones interoperables de usuario / proyecto.

Las ideas clave de BAPs son:

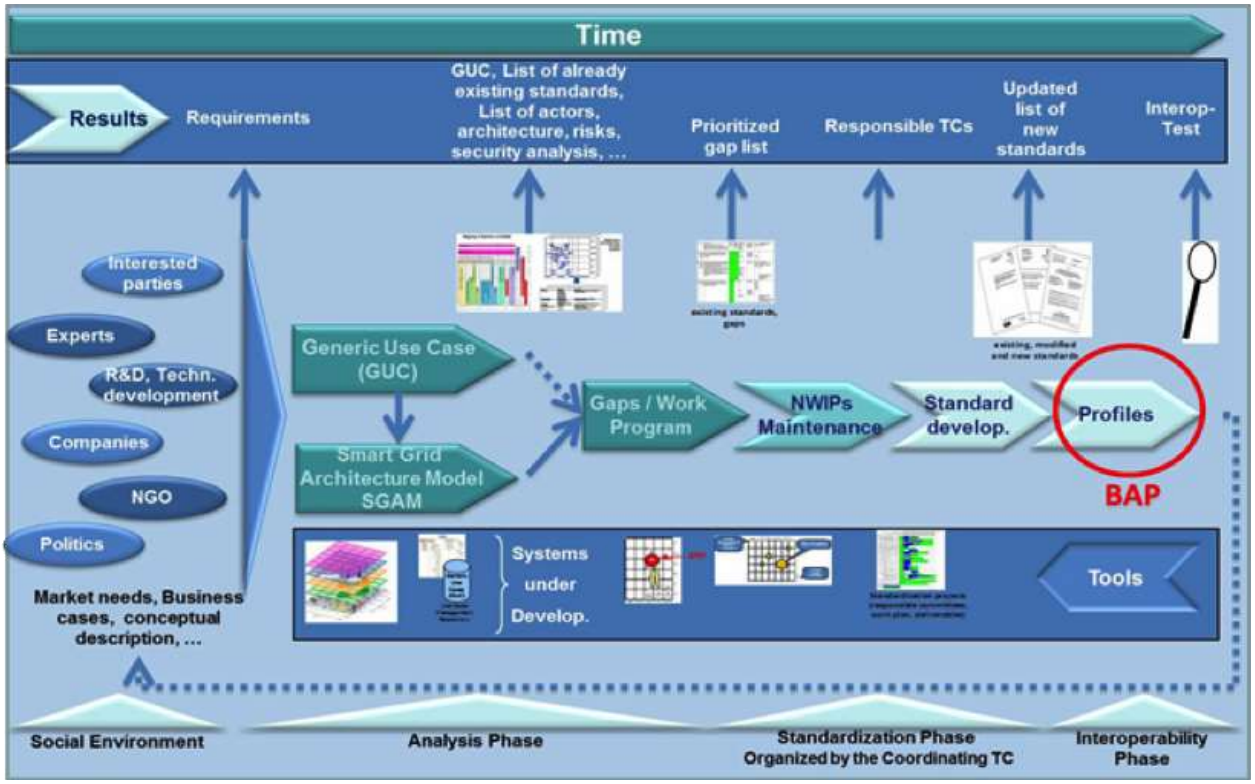
- BAPs son elementos dentro de un marco modular para sistemas/subsistemas específicos de aplicación.
- Los diferentes BAPs se utilizan en proyectos reales como bloques de construcción.
- Podría ser necesaria una etapa de refinamiento específica adicional al BAP para cumplir algunos requisitos específicos en la fase de implementación. Estos requisitos adicionales deben ser tenidos en cuenta en el grupo de usuarios y pueden dar lugar a nuevos BAP o versiones revisadas de los mismos sobre la base de experiencias de usuario y decisiones del grupo.

Los BAPs son válidos para los sistemas/subsistemas específicos de la aplicación (por ejemplo de automatización de subestaciones, gestión DER, energía hidroeléctrica y almacenamiento). Están diseñados para representar un común denominador de una implementación específica de red inteligente, pero no están dirigidos a cubrir todas las posibles opciones de implementación.

Los BAPs no deben tener opciones; todos los criterios seleccionados son, por tanto, obligatorios para alcanzar la interoperabilidad. Si se necesitan variantes de un determinado BAP para una función, se deben definir distintos BAP para esa función.

Los BAP se construyen sobre la base de las normas internacionales y también pueden tener una influencia en el desarrollo de normas por posible retroalimentación y aplicación de las lecciones aprendidas. La Figura 9 muestra la ubicación de los BAP en el flujo de trabajo de un proceso de normalización.

**Figura 9. BAP en el flujo de estandarización**




*Fuente: Fuente: https://en.wikipedia.org/wiki/V-Model_(software_development)*

Los BAP pueden incluir:

- Descripción de la función de aplicación relacionada.
- Modelos de datos relevantes.
- Servicios de comunicaciones.
- Requisitos de los componentes relacionados.
- Diagramas de interacción, si la función de aplicación se divide en sub-funciones que pueden distribuirse en diferentes dispositivos físicos.

Los BAPs incluyen la especificación del comportamiento funcional a modo de caja negra, algoritmos, código funcional y definiciones detalladas de la instancia.

## ***Perfil de interoperabilidad (IOP)***

Tal como se ha definido anteriormente, un perfil IOP es un documento que describe cómo se implementan las normas o especificaciones para soportar los requisitos de una aplicación particular, una función, una comunidad o contexto. Un perfil define un subconjunto de una entidad (por ejemplo, estándar, modelo, reglas). Puede contener una selección de modelos y servicios de datos, así como una asignación de protocolos. Además, un perfil puede definir instancias (por ejemplo, tipos de dispositivos específicos) y los procedimientos (por ejemplo, las lógicas programables, secuencias de mensajes, etc.).

El objetivo de los perfiles es reducir la complejidad, aclarar las especificaciones vagas o ambiguas y mejorar la interoperabilidad. Los perfiles IOP, por lo general, se aplican a ambos lados del modelo en V en términos de perfiles de aplicaciones básicas (BAP) para la fase de diseño y como versiones extendidas (ver BAIOP posteriormente) en la fase de prueba como se muestra en la Figura 10.

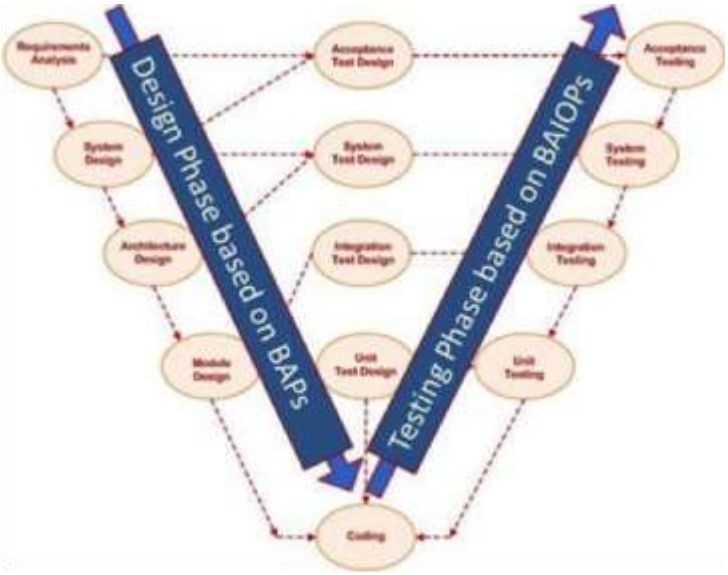
## ***Perfil Básico de Interoperabilidad de aplicación (BAIOP)***

Para ayudar a la interoperabilidad, un BAP puede extenderse a las pruebas de interoperabilidad. La versión extendida del BAP se conoce como perfil básico de interoperabilidad de aplicación (BAIOP).

Para conseguir la interoperabilidad, las pruebas basadas en un BAP tienen que cubrir:

- La configuración del dispositivo.
- La configuración de pruebas de la infraestructura de comunicación (topología).
- Los casos de prueba BAP relacionados.
- Las descripciones específicas de capacidad (por ejemplo PICS, PIXIT, MICS en caso de IEC 61850).
- El marco de ingeniería usado para el modelado de datos (casos) y la infraestructura de comunicación (topología, mapeado del servicio de comunicaciones).

**Figura 10. Modelo en V, incluyedo BAP y BAIOP**




*Fuente: Fuente: https://en.wikipedia.org/wiki/V-Model_(software_development)*

La definición y el uso común de los BAP y BAIOPS deben conducir a determinadas ventajas para todos los actores involucrados en un proyecto de redes inteligentes, por ejemplo:

- El beneficio para las empresas del sector y los grupos de usuarios radica en la posibilidad de armonizar las diversas variantes de funcionalidad de las aplicaciones de la empresa a un denominador común para cada función básica de aplicación. Se reduce así el riesgo de problemas de interoperabilidad causados por productos o sistemas, dado que se deben seleccionar entre los que cumplen los perfiles BAP y que han sido probados de acuerdo con BAIOPs.
- El beneficio para los vendedores que utilicen BAPs estandarizados en sus productos es una reducción de la implementación de variantes de un mismo proyecto o aplicación, para atender las

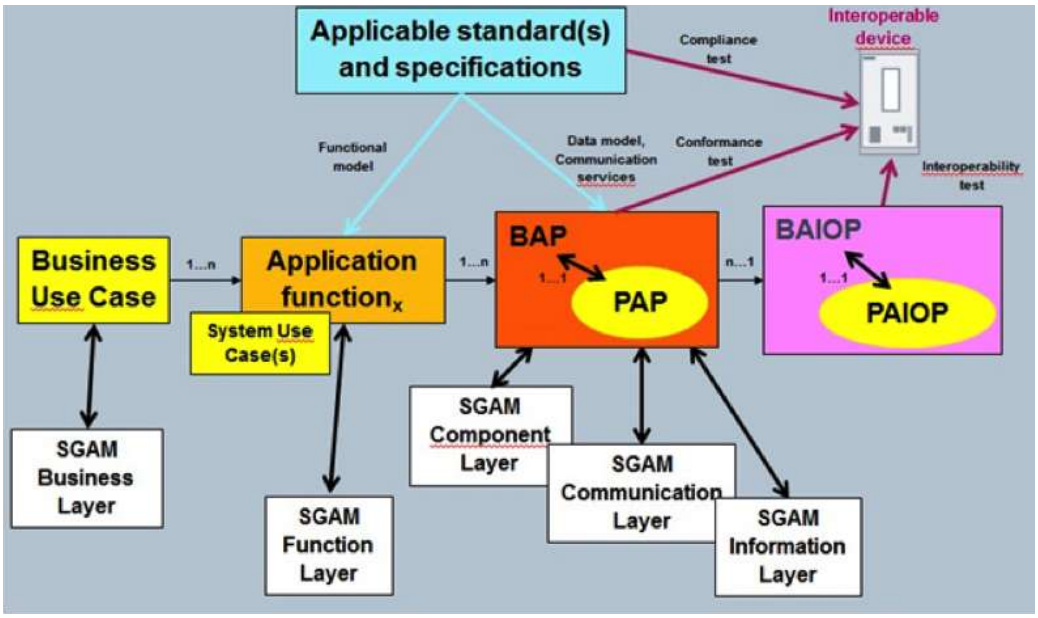
peculiaridades de los distintos clientes. Por lo tanto se reduce la complejidad de los productos, los costes de desarrollo y los esfuerzos de parametrización. Los BAIOPs se pueden utilizar para las pruebas internas antes de que el producto se ponga en el mercado.

- El beneficio para los Organismos de Certificación es la capacidad de realizar pruebas de interoperabilidad basadas en BAIOPs en beneficio de los usuarios.
- El beneficio para los integradores de sistemas es que pueden seleccionar específicamente productos conformes con los BAPs y probados de acuerdo con los BAIOPs, de forma que se deberían reducir los esfuerzos para la integración de los subsistemas o dispositivos.

## 1.7 Proceso para pasar de un caso de uso a un dispositivo interoperable.

La Figura 11 ilustra el proceso para pasar de un caso de uso a un dispositivo interoperable en el modelo SGAM mediante BAP y BAIOPs, donde PAP significa perfil de aplicación para un proyecto en particular.

**Figura 11. Del caso de uso a la Interoperabilidad en capas SGAM**




*Fuente: SGAM*

### ***Gestión de perfiles***

Es importante la gestión de perfiles con el fin de garantizar que los perfiles se aplican y se entienden de la misma manera por todos los actores implicados. También para evitar que perfiles divergentes para la misma finalidad se desarrollen y apliquen en paralelo. La gestión incluye principalmente:

- las responsabilidades y roles de los diferentes actores que están involucrados en la creación y gestión de perfiles.
- gestión del cambio y el control de versiones de los perfiles.
- comunicación de los cambios a los interesados afectados.

Por tanto, la recomendación general es que los propios grupos de usuarios deben encargarse de la creación y gestión de perfiles. Esto también significa que las lecciones aprendidas deben ser retroalimentadas por los usuarios de los perfiles de los grupos de usuarios correspondientes. También implica una adecuada compatibilidad hacia atrás dentro de este proceso. El grupo de usuarios debe ser responsable de la gestión de cambios y el control de versiones de los perfiles y comunicar los cambios a los interesados afectados y otros grupos de usuarios, de una manera adecuada, por ejemplo, por boletines de noticias o información web.

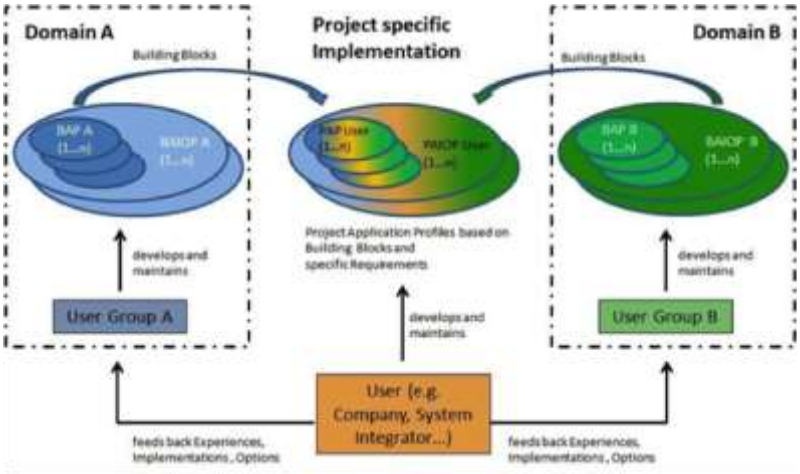
## ***La aplicación de perfiles en proyectos reales***

Como ya se ha mencionado, BAPs y BAIOPs son elementos de un entorno modular para hacer interoperables aplicaciones de sistemas/subsistemas específicos y se pueden combinar como bloques de construcción en proyectos reales. El usuario implicado en el proyecto (por ejemplo, una empresa o integrador de sistemas) es responsable del desarrollo y mantenimiento de perfiles de aplicación de proyectos (PAP) y de los perfiles de interoperabilidad de aplicación de proyectos (PAIOP) basados en estos bloques de construcción, pero, con posibles refinamientos para cumplir con todos los requisitos del proyecto. El usuario también debe retroalimentar su experiencia, la implementación y nuevas opciones a los grupos de usuarios correspondientes, lo que puede dar lugar a una revisión de los BAP y BAIOPs originales.

Para reducir los esfuerzos de implementación del proyecto, es deseable que los PAP y PAIOPs consten en lo posible de BAP y BAIOPs ya existentes y, solo en casos extremos, añadir alguna modificación.

Cuando la ejecución de un proyecto se demora por mucho tiempo, se debe realizar un chequeo regular de los nuevos BAP y BAIOPs lo que puede dar lugar a la revisión y posterior implementación de los PAP y PAIOPs dentro del proyecto. Por tanto, se recomienda utilizar solo los últimos perfiles como bloques de construcción para mejorar la interoperabilidad. La Figura 12 ilustra este proceso.

**Figura 12. Flujo de generación de perfiles específicos para un proyecto.**




*Fuente: SGAM*

## 1.8 Ejemplos de creación de BAPs

Esta sección contiene un ejemplo de creación de BAPs.

### ***Experiencia de creación de BAPs en E-Mobility***

Este apartado se centra en las pruebas de los sistemas de E-Mobility y su interoperabilidad con las redes inteligentes.

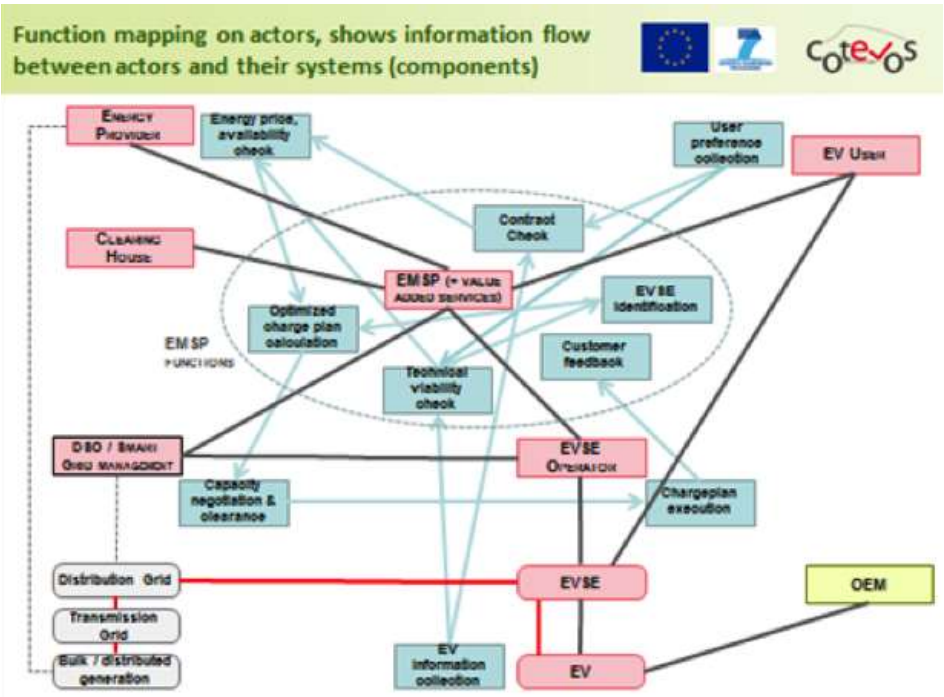
Como se describe en la Figura 11 el punto de partida son los casos de uso. La atención se centra en los sistemas de E-Mobility. Los casos de uso que se utilizan son el caso "carga y descarga inteligente" y el caso de uso "garantizar la interoperabilidad y el establecimiento.

El primer paso es el mapeo de los actores del sistema en la arquitectura de referencia. Esta asignación en la capa de negocio de SGAM es sencilla y fácil, ya que los casos de uso definen claramente los actores y está disponible una arquitectura completa.

El siguiente paso es la definición de las funciones requeridas en base al análisis paso a paso ya descrito en el caso de uso. Identificar las funciones de la aplicación del caso de uso es bastante tedioso, pero no es una tarea compleja. Como se describe en la Figura 11 en esta etapa ya se pueden identificar algunos estándares posibles relativos a la información intercambiada por las funciones.

El tercer paso es el mapeo de estas funciones y su flujo de información en el sistema desde los actores a otros componentes físicos; esto se traduce en la Figura 13.

**Figura 13. Mapeo de funciones en actores y componentes con los flujos de información**

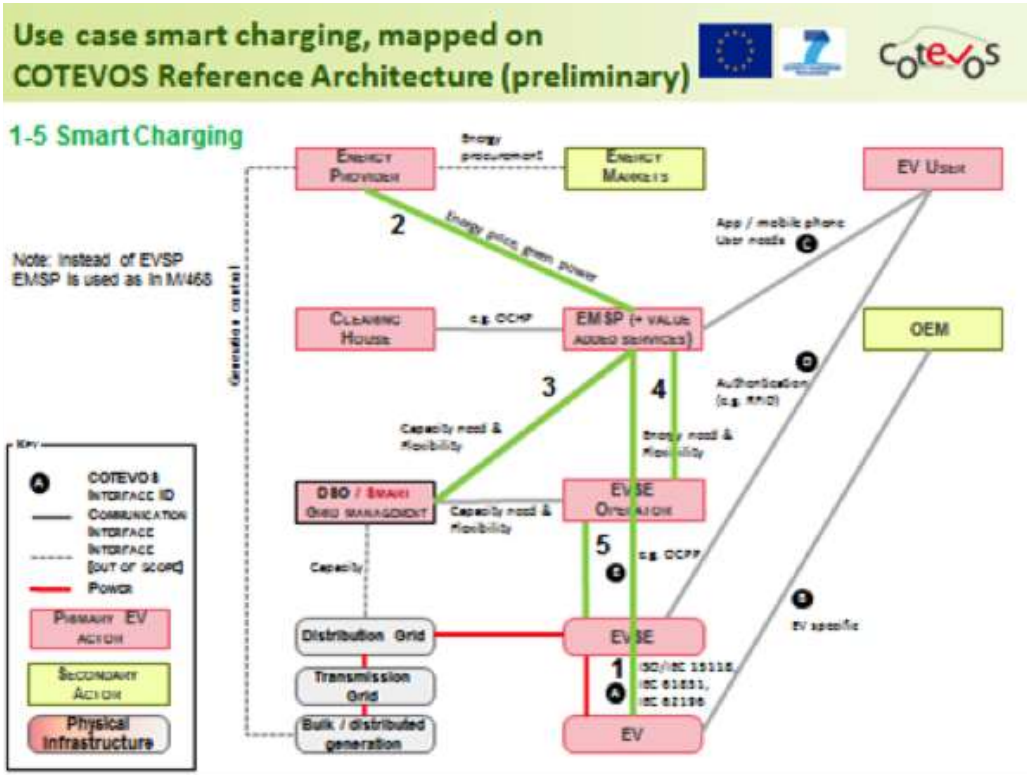



*Fuente: http://cotevos.eu/framework/*

Tras estos pasos ya se dispone de los flujos requeridos de información y las interfaces entre los componentes y los sistemas son claras. Los flujos de información pueden combinarse cuando se

intercambian entre los mismos componentes o sistemas en la arquitectura. Esto lleva a 5 interfaces de comunicación necesarios para el caso de uso de carga inteligente que se muestran en la Figura 14.

**Figura 14. Caso de uso de carga inteligente mapeado en la Arquitectura de Referencia**




*Fuente: http://cotevos.eu/framework/*

Este es el material suficiente para comenzar a crear una o más BAP. Sería posible crear un BAP completo para este caso de uso, pero eso llevaría a tantos BAPs como casos de uso, además, cualquier alternativa en las interfaces conducirían a un nuevo BAP completo (no puede haber alternativas / opciones dentro de un BAP). Como los BAPs definidos pueden utilizarse como bloques de constructivos, la mejor opción es crear un BAP por cada flujo de información. Este primer caso de uso conduce a 5 BAPs diferentes.

Un segundo caso de uso también supondría 5 BAPs, pero tres de ellos puede combinarse con uno de los BAP del caso de uso anterior. Así que en total con solo 7 BAPs es posible cubrir estos 2 casos de uso.

# 2. Lista de estándares que se consideran disponibles para su utilización en los modelos de RI

De acuerdo con la tabla 82 del documento SGCG/M490/G (CEN-CENELEC-ETSI, 2014), los siguientes son los estándares de comunicaciones disponibles (principalmente enfocados en las capas 1,2 y 3 del modelo OSI para el despliegue de arquitecturas de RI.

**Tabla 5. Estándares de comunicación disponibles para aplicación en RI**

| Layer | Category (ies) | Standard | Comments |
|---|---|---|---|
| General | | ISO/IEC 7498-1 | (1994) Information Technology – Open Systems Interconnect – Basic Reference Model: The Basic Model |
| General | | ITU-T I.322 | (02/99) - Generic protocol reference model for telecommunication networks |
| Communication | IP MPLS | IETF RFC 5654 | Requirements of an MPLS Transport Profile |
| Communication | IP MPLS | IETF RFC 5921 | A Framework for MPLS in Transport Networks |
| Communication | IP MPLS | IETF RFC 3031 | Multiprotocol Label Switching Architecture |
| Communication | IP MPLS | IETF RFC 3032 | MPLS Label Stack Encoding |
| Communication | IP MPLS | IETF RFC 4090 | Fast Reroute Extensions to RSVP-TE for LSP Tunnels, http://www.ietf.org/rfc/rfc4090.txt |
| Communication | IP MPLS | IETF RFC 6178 | Label Edge Router Forwarding of IPv4 Option Packets |
| Communication | IPv4, IPv6 | IETF RFC 791 | Internet Protocol |
| Communication | IPv4, IPv6 | IETF RFC 2460 | Internet Protocol, Version 6 (IPv6) Specification |
| Communication | IPv4, IPv6 | IETF RFC 4944 | Transmission of IPv6 Packets over IEEE 802.15.4 Networks -. http://www.rfc-editor.org/rfc/rfc4944.txt |
| Communication | IPv4, IPv6 | IETF RFC 6272[2] | Internet Protocols for the Smart Grid. http://www.rfc-editor.org/rfc/rfc6272.txt |
| Communication | IPv4, IPv6 | IETF RFC 6282 | Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks |
| Communication | IPv4, IPv6, IP MPLS | IETF RFC 5086 | Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN) |
| Communication | IPv4, IPv6, IP MPLS | IETF RFC 4553 | Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP) |
| Communication | IEEE 802.11 | IEEE 802.11 | A list of standards is available under this link http://standards.ieee.org/about/get/802/802.11.html |

[2] RFC 6272 is an informational RFC. It is listed in this table because it makes reference to several standard track RFCs which are relevant for Smart Grids.

| | | | |
|---|---|---|---|
| Communication | IEEE 802.1 | IEEE 802.1 | A list of standards is available under this link http://standards.ieee.org/about/get/802/802.1.html |
| Communication | IEEE 802.3 | IEEE 802.3 | A list of standards is available under this link http://standards.ieee.org/about/get/802/802.3.html |
| Communication | IEEE 802.16 | IEEE 802.16 | A list of standards is available under this link http://standards.ieee.org/about/get/802/802.16.html |
| Communication | IEEE 802.15.4 | IEEE 802.15.4 | A list of standards is available under this link http://web.archive.org/web/20080224053532/http://shop.ieee.org/ieeestore/Product.aspx?product_no=SS95552 |
| Communication | ETSI TS 102 887 | ETSI TS 102 887 | - Electrocompatibility and radio spectrum Matters (ERM); Short Range Devices; Smart Metering Wireless Access Protocol (SMEP). Part 1; PHY Layer<br>- Electrocompatibility and radio spectrum Matters (ERM); Short Range Devices; Smart Metering Wireless Access Protocol (SMEP). Part 2; MAC Layer |
| Communication | RPL/6LowPan | IETF RFC 4919 | IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals |
| Communication | RPL/6LowPan | IETF RFC 6550 | (ROLL) RPL IPv6 Routing Protocol for Low-Power and Lossy Network.<br>A list of Internet RFCs is available under: http://tools.ietf.org/wg/roll<br>draft-ietf-roll-minrank-hysteresis-of -11 2012-06-30 RFC Ed Queue<br>draft-ietf-roll-security-framework draft-ietf-roll-p2p-measurement<br>draft-ietf-roll-p2p-rpl<br>draft-ietf-roll-trickle-mcast |
| Communication | RPL/6LowPan | IETF RFC 6551 | (ROLL) Routing metrics |
| Communication | RPL/6LowPan | IETF RFC 6552 | (ROLL) Objective Function Zero |
| Communication | RPL/6LowPan | IETF RFC 6206 | (ROLL) Trickle |
| Communication | RPL/6LowPan | IETF RFC 6775 | Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) |

| | | | |
|---|---|---|---|
| Communication | EN 13321 | EN 13321-2 | prEN 13321-2:2012-02: Open Data Communication in Building Automation, Controls and Building Management - Home and Building Electronic System Part 2: KNXnet/IP Communication |
| Communication | Narrow band PLC (Medium & Low voltage) | EN 61334 | Distribution automation using distribution line carrier systems |
| Communication | EN 50090 | EN 50090-2-1 | System overview-Architecture (1994) |
| Communication | EN 50090 | EN 50090-3-1 | Aspects of application-Introduction to the application structure (1994) |
| Communication | EN 50090 | EN 50090-3-2 | Aspects of application-User process for HBES Class 1 (2004) |
| Communication | EN 50090 | EN 50090-4-1 | Media independent layers-Application layer for HBES Class 1 (2004) |
| Communication | EN 50090 Narrow band PLC (Medium & Low voltage) | EN 50090-4-2 | Media independent layers–Transport layer, network layer and general parts of datalink layer for HBES Class 1 (2004) |
| Communication | EN 50090 | EN 50090-4-3 | Media independent layers -Communication over IP |
| Communication | EN 50090 | EN 50090-5-1 | Media and media dependent layers-Power line for HBES Class 1 (2005) |
| Communication | EN 50090 | EN 50090-5-2 | Media and media dependent layers-Network based on HBES Class1, Twisted Pair (2004) |
| Communication | EN 50090 | EN 50090-7-1 | System management-Management procedures (2004) |
| Communication | EN 14908 | EN 14908-1 | Control network protocol stack |
| Communication | EN 14908 | EN 14908-2 | Twisted-pair channel for networked control systems |
| Communication | EN 14908 Narrow band PLC (Medium & Low voltage) | EN 14908-3 | Power Line channel in the EN 50065-1 CENELEC C-Band |
| Communication | EN 14908 | EN 14908-4 | Transporting over Internet Protocol (IP) networks |
| Communication | EN 14908 Narrow band PLC (Medium & Low voltage) | ETSI TS 103 908 | Power Line channel in the EN 50065-1 CENELEC A-Band |
| Communication | LTE/LTE-A | ETSI TS 136 300 / 3GPP TS 36.300 | LTE Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 http://www.3gpp.org/ftp/Specs/html-info/36300.htm (ITU-R endorsement) |
| Communication | LTE/LTE-A | ETSI TS 136 201 / 3GPP TS 36.201 | Evolved Universal Terrestrial Radio Access (E-UTRA); LTE physical layer; General description. (ITU-R endorsement) |
| Communication | LTE/LTE-A | ETSI TS 136 211 / 3GPP TS 36. 211 | 211 Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation. (ITU-R endorsement) |

| | | | |
|---|---|---|---|
| Communication | LTE/LTE-A | ETSI TS 136 212 / 3GPP TS 36.212 | Evolved Universal Terrestrial Radio Access (E-UTRA); Multiplexing and channel coding. (ITU-R endorsement) |
| Communication | LTE/LTE-A | ETSI TS 136 213 / 3GPP TS 36.213 | Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures. (ITU-R endorsement) |
| Communication | LTE/LTE-A | ETSI TS 136 214 / 3GPP TS 36.214 | Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer; Measurements. |
| Communication | LTE/LTE-A | ETSI TS 136 216 / 3GPP TS 36.216 | Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer for relaying operation (ITU-R endorsement) |
| Communication | LTE/LTE-A | ETSI TS 123 401 / 3GPP TS 23.401 | General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access |
| Communication | 3G / WCDMA / UMTS / HSPA | ETSI TS 121 101 | Overview of Technical Specifications and Technical Reports for a UTRAN-based 3GPP system (3GPP TS 21.101) |
| Communication | GSM / GPRS / EDGE | ETSI TS 141 101 | Overview of Technical Specifications and Technical Reports for a GERAN-based 3GPP system (3GPP TS 41.101) |
| Communication | LTE/LTE-A, GSM/GPRS/EDGE , 3G/WCDMA/UMTS/ HSPA | ETSI TS 122 368 / 3GPP TS 22.368 | Service requirements for Machine-Type Communications (MTC); Stage 1 |
| Communication | LTE/LTE-A, GSM/GPRS/EDGE , 3G/WCDMA/UMTS/ HSPA | ETSI TS 123 682 / 3GPP TS 23.682 | Architecture Enhancements to facilitate communications with Packet Data Networks and Applications |
| Communication | LTE/LTE-A | ETSI TS 123 402 / 3GPP TS 23.402 | Architecture Enhancements for Non-3GPP Accesses (Release 10) |
| Communication | LTE/LTE-A, GSM/GPRS/EDGE , 3G/WCDMA/UMTS/ HSPA | ETSI TS 129 368 3GPP TS 29.368 | Tsp interface protocol between the MTC Interworking Function (MTC-IWF) and Service Capability Server (SCS) |
| Communication | GSM/GPRS/EDGE | ETSI EN 301 502 | Global System for Mobile communications (GSM);Harmonized EN for Base Station Equipment covering the essential requirements of article 3.2 of the R&TTE Directive |
| Communication | GSM/GPRS/EDGE, | ETSI EN 301 511 | Global System for Mobile communications (GSM);Harmonized EN for mobile stations in the GSM 900 and GSM 1800 bands covering essential requirements under article 3.2 of the R&TTE directive |

| | | | |
|---|---|---|---|
| Communication | LTE/LTE-A, 3G/WCDMA/UMTS/ HSPA | ETSI EN 301 908 | Parts 1,2,3,6,7,3,11,13, 14,15,18 - IMT cellular networks; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive |
| Communication | CDMA2000/UMB | ETSI EN 301 908 | Parts 4, 5, 12, 16, 17 - IMT cellular networks; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive |
| Communication | DSL/PON | IEEE 802.3 | 802.3 application for GEPON |
| Communication | DSL/PON | IEEE 802.3av | 802.3av application for 10GEPON |
| Communication | DSL/PON | ITU-T G.991.1 | High bit rate digital subscriber line (HDSL) transceivers |
| Communication | DSL/PON | ITU-T G.991.2 | Single-pair high-speed digital subscriber line (SHDSL) transceivers |
| Communication | DSL/PON | ITU-T G.992.1 | Asymmetric digital subscriber line (ADSL) transceivers |
| Communication | DSL/PON | ITU-T G.992.2 | Splitterless asymmetric digital subscriber line (ADSL) transceivers |
| Communication | DSL/PON | ITU-T G.992.3 | Asymmetric digital subscriber line transceivers 2 (ADSL2) |
| Communication | DSL/PON | ITU-T G.992.4 | Splitterless asymmetric digital subscriber line transceivers 2 (splitterless ADSL2) |
| Communication | DSL/PON | ITU-T G.993.1 | Very high speed digital subscriber line transceivers (VDSL) |
| Communication | DSL/PON | ITU-T G.993.2 | Very high speed digital subscriber line transceivers 2 (VDSL2) |
| Communication | DSL/PON | ITU-T G.993.5 | Self-FEXT cancellation (vectoring) for use with VDSL2 transceivers |
| Communication | DSL/PON | ITU-T G.994.1 | Handshake procedures for digital subscriber line (DSL) transceivers |
| Communication | DSL/PON | ITU-T G.995.1 | Overview of digital subscriber line (DSL) Recommendations |
| Communication | DSL/PON | ITU-T G.996.1 | Test procedures for digital subscriber line (DSL) transceivers |
| Communication | DSL/PON | ITU-T G.996.2 | Single-ended line testing for digital subscriber lines (DSL) |
| Communication | DSL/PON | ITU-T G.997.1 | Physical layer management for digital subscriber line (DSL) transceivers |
| Communication | DSL/PON | ITU-T G.998.1 | ATM-based multi-pair bonding |
| Communication | DSL/PON | ITU-T G.998.2 | Ethernet-based multi-pair bonding |
| Communication | DSL/PON | ITU-T G.998.3 | Multi-pair bonding using time-division inverse multiplexing |
| Communication | DSL/PON | ITU-T G.999.1 | Interface between the link layer and the physical layer for digital subscriber line (DSL) transceivers |
| Communication | DSL/PON | ITU-T G.998.4 | Improved Impulse Noise Protection (INP) for DSL Transceivers |
| Communication | DSL/PON | ITU-T G.983.1 | Broadband optical access systems based on Passive Optical Networks (PON) |
| Communication | DSL/PON | ITU-T G.983.2 | ONT management and control interface specification for B- PON |

| | | | |
|---|---|---|---|
| Communication | DSL/PON | ITU-T G.983.3 | A broadband optical access system with increased service capability by wavelength allocation |
| Communication | DSL/PON | ITU-T G.983.4 | A broadband optical access system with increased service capability using dynamic bandwidth assignment |
| Communication | DSL/PON | ITU-T G.983.5 | A broadband optical access system with enhanced survivability |
| Communication | DSL/PON | ITU-T G.984.1 | Gigabit-capable passive optical networks (GPON): General characteristics |
| Communication | DSL/PON | ITU-T G.984.2 | Gigabit-capable Passive Optical Networks (G-PON): Physical Media Dependent (PMD) layer specification |
| Communication | DSL/PON | ITU-T G.984.3 | Gigabit-capable Passive Optical Networks (G-PON): Transmission convergence layer specification |
| Communication | DSL/PON | ITU-T G.984.4 | Gigabit-capable passive optical networks (G-PON): ONT management and control interface specification |
| Communication | DSL/PON | ITU-T G.984.5 | Gigabit-capable Passive Optical Networks (G-PON): Enhancement band |
| Communication | DSL/PON | ITU-T G.984.6 | Gigabit-capable passive optical networks (GPON): Reach extension |
| Communication | DSL/PON | ITU-T G.984.7 | Gigabit-capable passive optical networks (GPON): Long reach |
| Communication | DSL/PON | ITU-T G.987.1 | 10-Gigabit-capable passive optical networks (XG-PON): General requirements |
| Communication | DSL/PON | ITU-T G.987.2 | 10-Gigabit-capable passive optical networks (XG-PON): Physical media dependent (PMD) layer specification |
| Communication | DSL/PON | ITU-T G.987.3 | 10-Gigabit-capable passive optical networks (XG-PON): Transmission convergence (TC) layer specification |
| Communication | EN 60870-5 | EN 60870-5-4<br>EN 60870-5-3<br>EN 60870-5-2<br>EN 60870-5-1 | Telecontrol equipment and systems - Part 5 – lower layers of communication |
| Communication | EN 60870-5 | EN 60870-5-101 | Telecontrol equipment and systems - Part 5-101: Transmission protocols - Companion standard for basic telecontrol tasks |
| Communication | EN 60870-5 | EN 60870-5-102 | Telecontrol equipment and systems. Part 5-102: transmission protocols. Companion standard for the transmission of integrated totals in electric power systems |
| Communication | EN 60870-5 | EN 60870-5-103 | Telecontrol equipment and systems - Part 5-103: Transmission protocols - Companion standard for the informative interface of protection equipment |

| | | | |
|---|---|---|---|
| Communication | EN 60870-5 | EN 60870-5-104 | Telecontrol equipment and systems - Part 5-104: Transmission protocols - Network access for EN 60870-5- 101 using standard transport profiles |
| Communication | SDH/OTN | ITU-T G.707 | Network node interface for the synchronous digital hierarchy (SDH) |
| Communication | SDH/OTN | ITU-T G.7042 | Link capacity adjustment scheme for virtual concatenated signals. |
| Communication | SDH/OTN | ITU-T G.7041 | Generic Framing Procedure (GFP) |
| Communication | SDH/OTN | ITU-T G.709 | Interfaces for the Optical Transport Network (OTN) |
| Communication | SDH/OTN | ITU-T G.798 | Characteristics of optical transport network hierarchy equipment functional blocks |
| Communication | SDH/OTN | ITU-T G.781 | Synchronization layer functions |
| Communication | SDH/OTN | ITU-T G.872 | Architecture of optical transport networks |
| Communication | SDH/OTN | ITU-T G.783 | Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks |
| Communication | SDH/OTN | ITU-T G.803 | Architecture of transport networks based on the synchronous digital hierarchy (SDH) |
| Communication | IEC 61850 | EN 61850-8-1 | Ed. 2.0 2011- 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 |
| Communication | IEC 61850 | EN 61850-9-2 | Ed. 2.0:2011- Communication networks and systems in substations - Part 9-2: Specific Communication Service Mapping (SCSM) - Sampled values over ISO/IEC 8802-3 |
| Communication | IEC 61850 | IEC 61850-90-1 | Ed. 1.0:2010 - Communication networks and systems for power utility automation - Part 90-1: Use of IEC/EN 61850 for the communication between substations |
| Communication | IEC 61850 | IEC 61850-90-4 | Communication networks and systems for power utility automation - Network engineering guidelines |
| Communication | IEC 61850 | IEC 61850-90-5 | Ed. 1.0:2012 - Communication networks and systems for power utility automation - Part 90-5: Use of IEC/EN 61850 to transmit synchrophasor information according to IEEE C37.118 |
| Communicatio n, Information | IEC 61850 | EN 61850-7-1 | Ed. 2.0:2011- Communication networks and systems for power utility automation - Part 7-1: Basic communication structure - Principles and models |
| Communication | EN 13757 | EN 13757-4 | Communication systems for meters and remote reading of meters – Part 4: wireless meter readout (radio meter reading for operation in SRD bands) |

| | | | |
|---|---|---|---|
| Communication | EN 13757 | EN 13757-5 | Communication systems for meters and remote reading of meters – Part 5: wireless relaying |
| Communication | Narrow band PLC (High & very High voltage) | IEC 62488-1 (Formerly EN60663) - Part 1 | Planning of analogue and digital power line carrier systems operating over EHV/HV/MV electricity grids. |
| Communication | Broadband PLC | ISO/IEC 12139-1 | Telecommunications and information exchange between systems — Powerline communication (PLC) — High speed PLC medium access control (MAC) and physical layer (PHY) |
| Communication | Broadband PLC | ITU-T G.9960 ITU-T G.9961 ITU-T G.9962 ITU-T G.9963 ITU-T G.9964 | Unified high-speed wireline-based home networking : ITU-T G.9960 (PHY) ITU-T G.9961 (DLL) ITU-T G.9962 (MIMO ) ITU-T G.9963 (MIMO G.hn) ITU-T G.9964 (PSD) |
| Communication | Narrow band PLC (Medium & Low voltage) | ITU-T G.9901 | ITU-T G.9901 (NB-PLC PSD) |
| Communication | Narrow band PLC (Medium & Low voltage) | ITU-T G.9902 | ITU-T G.9902 (G.hnem) |
| Communication | Narrow band PLC (Medium & Low voltage) | ITU-T G.9903 | ITU-T G.9903 (G3-PLC) |
| Communication | Narrow band PLC (Medium & Low voltage) | ITU-T G.9904 | ITU-T G.9904 (PRIME) |
| Communication | Narrow band PLC (Medium & Low voltage) | ITU-T G.9905 | ITU-T G.9905 (Routing) |
| Communication | Narrowb and wireless‖ | ITU-T G.9959 | ITU-T G.9959 (Z-Wave) Short range narrowband digital radio communication transceivers – PHY & MAC layer specifications |
| Communication | G.fast | ITU-T G.9700 | Fast access to subscriber terminals (FAST) - Power spectral density specification (G.fast PSD) |
| Communication | Broadband PLC | IEEE 1901 | Broadband over Power Line Networks |
| Communication | Broadband PLC | IEEE 1901.2 | Standard for Low Frequency (less than 500 kHz) Narrow Band Power Line Communications for Smart Grid Applications |

| | | | |
|---|---|---|---|
| Communication | M2M | ETSI TR 101 531 | Machine-to-Machine communications (M2M); Reuse of Core Network Functionality by M2M Service Capabilities - |
| Communication | M2M | ETSI TR 102 935 | Machine-to-Machine communications (M2M);. Applicability of M2M architecture to Smart Grid Networks |
| Communication | M2M | ETSI TR 102 966 | Machine-to-Machine communications (M2M); Interworking between the M2M Architecture and M2M Area Network technologies |
| Communication | M2M | ETSI TR 103 167 | Machine-to-Machine Communications (M2M); Threat analysis and counter-measures to M2M service layer |
| Communication | M2M | ETSI TS 101 584 | Machine-to-Machine Communications (M2M);. Study on Semantic support for M2M Data |
| Communication | M2M | ETSI TS 102 689 | Machine-to-Machine communications (M2M); M2M service requirements |
| Communication | M2M | ETSI TS 103 092 | Machine-to-Machine communications (M2M); OMA DM compatible Management Objects for ETSI M2M |
| Communication | M2M | ETSI TS 103 093 | Machine-to-Machine communications (M2M); BBF TR-069 compatible Management Objects for ETSI M2M |
| Communication | M2M | ETSI TS 103 104 | Machine-to-Machine communications (M2M); Interoperability Test Specification for CoAP Binding of ETSI M2M Primitives |
| Communication | M2M | ETSI TS 103 107 | ETSI TS 103 107 Machine-to-Machine communications (M2M); Service layer interworking with 3GPP2 networks |
| Communication | M2M | ETSI TS 103 603 | Machine-to-Machine communications (M2M); Service layer interworking with 3GPP networks |

*Fuente: Tabla 82 del documento SGCG/M490/G - Estándares para Redes Inteligentes (CEN-CENELEC-ETSI, 2014)*