UNIVERSITAT POLITÈCNICA DE VALÈNCIA

TESIS DOCTORAL

Aplicaciones de SWE en entornos industriales

Autor: Pablo Giménez Salazar

Director: Carlos E. Palau Salvador

Valencia, Febrero 2015

Resumen

Esta tesis se ha creado en el marco de la interoperabilidad de las redes de sensores en entornos industriales, mediante la utilización del estándar SWE (Sensor Web Enablement). Se ha desarrollado a partir de la participación en diferentes proyectos de investigación, dentro del grupo de investigación SATRD (Sistemas y Aplicaciones de Tiempo Real Distribuidos) del Departamento de Comunicaciones de la UPV.

Ha pasado mucho tiempo desde la aparición de los primeros sensores que únicamente eran capaces de responder frente a un estímulo, hasta el concepto de sensor web, donde los sensores pueden ser configurados de forma remota, realizar acciones y procesar e integrar datos de otros sensores. Hoy en día, la utilización de redes de sensores o WSN (Wireless Sensor Networks) está ampliamente extendida en diversos ámbitos, para recopilar información, que luego pueda ser utilizada por otras aplicaciones.

A medida que aumenta su utilización, surge la necesidad de combinar o agregar datos de sensores de distintas WSN, lo cual no siempre es posible, debido a la falta de interoperabilidad entre los distintos fabricantes. Es por ello que OGC (Open Geospatial Consortium) fundó SWE, con el fin de desarrollar estándares para el acceso a sensores a través de Internet y así mejorar la interoperabilidad.

Por estos motivos, en esta tesis se ha especificado una arquitectura IoT (Internet of Things) de forma genérica, para que se pueda extender a múltiples entornos. La arquitectura I3WSN se ha diseñado para la monitorización y el control de sistemas, garantizando la interoperabilidad entre los distintos elementos gracias a la integración de los estándares de SWE.

Tras el diseño, se ha llevado a cabo la aplicación de la arquitectura en tres contextos distintos, asociados a tres proyectos de investigación. El primero de ellos, con el objetivo de monitorizar y gestionar la salud de los trabajadores en entornos industriales, a partir de datos del entorno y datos médicos, dentro del proyecto FASyS (Fabrica Absolutamente Segura y Saludable). El segundo, para garantizar el nivel de aseguramiento de un entorno smart grid, a partir de la captura de la información de seguridad de todos sus elementos, en el proyecto UniverSEC. Y por último, para gestionar de forma eficiente e inteligente el transporte de contenedores de mercancías, a partir de los datos de tráfico en tiempo real, en el proyecto STIMULO.

Resum

Aquesta tesi ha estat creada en el marc de la interoperabilitat de les xarxes de sensors en entorns industrialitzats, utilitzant l'estàndard SWE (Sensor Web capacitació). S'ha desenvolupat des de la participació en diversos projectes d'investigació, dins del grup d'investigació SATRD (Sistemes i Aplicacions de Temps Real Distribuïts) del Departament de Comunicació de la UPV.

Ha passat molt temps des de l'aparició dels primers sensors que només eren capaços de respondre a un estímul, fins al concepte de sensor web, on els sensors es poden configurar remotament, realitzar accions i processar i integrar les dades d'altres sensors. Avui en dia, l'ús de xarxes de sensors o WSN (Wireless Sensor Networks) està àmpliament estesa en diversos àmbits, per a recollir informació, que després puga ser utilitzada per altres aplicacions.

A mesura que augmenta el seu ús, sorgeix la necessitat de combinar o afegir dades de sensors de diferents WSN, que no sempre és possible, degut a la falta d'interoperabilitat entre els diferents fabricants. És per això que OGC (Open Geospatial Consortium) va fundar SWE, per desenvolupar estàndards per l'accés de sensors a Internet i així millorar la interoperabilitat.

Per aquests motius, en aquesta tesi s'ha especificat una arquitectura IoT (Internet of Things) de forma genèrica, per tal que es puga estendre a múltiples entorns. L'arquitectura I3WSN s'ha dissenyat per la monitorització i el control de sistemes, garantint la interoperabilitat entre els diferents elements gràcies a la integració dels estàndards de SWE.

Després el disseny, s'ha dut a terme l'aplicació de l'arquitectura en tres contextos diferents, associats amb tres projectes d'investigació. El primer d'ells, amb la finalitat de monitoritzar i gestionar la salut dels treballadors en entorns industrials, a partir de dades ambientals i dades mèdiques, dins del projecte FASyS (Fabrica Absolutamente Segura y Saludable). El segon, per garantir el nivell d'assegurament d'un entorn de smart grid, a partir de la captura de la informació de seguretat de tots els seus elements, en el projecte UniverSEC. I finalment, per gestionar de manera eficient i intel·ligent el transport de contenidors de mercaderies, a partir de les dades de trànsit en temps real, en el projecte STIMULO.

Abstract

This thesis has been created within the framework of the interoperability of the networks of sensors in industrial environments, using standard SWE (Sensor Web Enablement). It has developed from the participation in different research projects, within the research group SATRD (Distributed Real Time Systems and Applications) of the Communications Department of the UPV.

Has gone a long time since the appearance of the first sensors that were only able to respond to a stimulus, to the concept of sensor web, where sensors can be remotely configured, perform actions and process and integrate data from other sensors. Nowadays, the use of networks of sensors or WSN (Wireless Sensor Networks) is widespread in several fields, to gather information, which can then be used by other applications.

As it increases its use, it is necessary to combine or add data from sensors of different WSN, which is not always possible, due to the lack of interoperability between different manufacturers. That is why OGC (Open Geospatial Consortium) founded SWE, in order to develop standards for access to sensors via the Internet and thus improve the interoperability.

For these reasons, in this thesis is specified an IoT architecture (Internet of Things) generically, so that it can be extended to multiple environments. The I3WSN architecture is designed for monitoring and control systems, ensuring interoperability between the different elements through the integration of SWE standards.

After the design, the application of the architecture is carried out in three different contexts, associated with three research projects. The first of them, in order to monitor and manage the workers' health in industrial environments, based on environmental and medical data, within the project FASyS (Fabrica Absolutamente Segura y Saludable). Secondly, to ensure the level of assurance of a smart grid environment, from the capture of the security information of all its elements, in the UniverSEC project. Finally, to manage efficiently and intelligently transport freight containers, from traffic data in real time, in the project STIMULO.

Agradecimientos

A mi familia, que siempre me ha apoyado
en todas las decisiones importantes

A Natalia, que siempre está cuando la necesito

A mi director de tesis, Carlos, por la oportunidad que
me ha dado y por confiar en mí durante estos años

A mis compañeros del laboratorio, por hacer los días más
entretenidos y por toda la ayuda que me han prestado

A mis amigos de Teleco, sin los cuales,
todos estos años no habría sido lo mismo

Índice

Índice de figuras

Índice de tablas

1. Introducción

1.1. Introducción

Las redes de sensores o WSN (Wireless Sensor Networks), son una de las tecnologías más utilizadas en la actualidad y están muy integradas en la vida cotidiana, debido a que pueden proporcionar multitud de datos en una amplia variedad de campos y a la aparición de nuevos sensores de bajo coste. El uso de tecnologías como big data [1] y stream processing [2] permitirá aprovechar todos estos datos.

En la actualidad, el uso de WSN está muy extendido en diversos ámbitos, principalmente para monitorización del entorno, ya sea en entornos de seguridad, eficiencia energética, automoción, domótica, o entornos industriales. Ofrecen muchos beneficios que se han puesto de manifiesto en diversos estudios. Cada WSN está formada por múltiples sensores de todo tipo, con conexión a Internet y que actúan como un grupo (concepto *sensor web* [3]).

Debido a que antes de la aparición de SWE (Sensor Web Enablement) [4] [5] no existía ningún estándar capaz de integrar los datos de distintas WSN, OGC (Open Geospatial Consortium) desarrolló la iniciativa SWE para promover la interoperabilidad y desarrollar estándares para acceder y controlar sensores y redes de sensores a través de Internet. Este nuevo estándar, permite realizar tareas de forma homogénea como: el descubrimiento de sensores, determinar las propiedades físicas medidas por un sensor o la calidad de dichas medias, solicitar y enviar medidas de forma estándar, etc.

Esta tesis, se centra en la especificación de una arquitectura que integre el estándar SWE en distintos entornos, en los que las redes de sensores están presentes y se utilizan ampliamente (ej. transporte mercancías, sistemas críticos como las redes de energía y entornos industriales de fabricación), pero en los que tradicionalmente se han empleado soluciones adhoc para su integración, en lugar de emplear mecanismos estándar. La utilización de soluciones tipo SWE, garantiza una mejor gestión de la información, así como la interoperabilidad sin adaptación de productos hardware y software de distintos fabricantes. El desarrollo del presente trabajo ha supuesto un análisis teórico/práctico de la aplicabilidad de SWE para su utilización en diversos escenarios y casos de uso relacionados con los entornos anteriormente mencionados. Para lo cual, ha sido necesario diseñar una arquitectura genérica basada en el paradigma de SWE, para poder aprovechar al máximo las ventajas que ofrecen sus especificaciones.

La idea de permitir la comunicación entre dispositivos heterogéneos, o recoger datos de gran cantidad de objetos variados que interactúan con el entorno físico a través de Internet para su posterior utilización, son los principales objetivos de Internet of Things (IoT) [6] [7]. Para ello, en esta tesis, se van a utilizar las especificaciones y servicios de SWE como vía para la obtención y almacenamiento de los datos generados, a partir de los cuales, se puedan crear aplicaciones que sirvan para mejorar la seguridad y efectividad.

De este modo, en esta tesis se ha llevado a cabo la aplicación de la arquitectura basada en el estándar SWE, en tres contextos asociados a tres proyectos de investigación

directamente relacionados con los casos de uso y escenarios de las áreas de aplicación indicadas:

- FASyS (Fábrica Absolutamente Segura y Saludable) [8], para mejorar la seguridad y la gestión de riesgos de las personas en entornos industriales;
- UniverSEC (Cockpit para la monitorización y auditoría continua de la seguridad de las operaciones de infraestructuras de comunicación abiertas, basadas en Perfiles de Aseguramiento de la Seguridad (SAC)) [9], con la finalidad de garantizar la seguridad en un entorno de smart grid mediante la captura de información para la evaluación del nivel de aseguramiento;
- STIMULO (Sistema de transporte logístico inteligente multimodal) [10], para gestionar de forma inteligente el transporte de mercancías de forma que sea más eficiente y eficaz.

Dejando abierta la posibilidad de extender las propuestas realizadas y los resultados obtenidos a otras áreas de aplicación: monitorización del medioambiente; gestión de edificios, producción industrial; seguridad y protección de infraestructuras críticas,…

1.2. Motivación de la Tesis

El trabajo desarrollado en la presente tesis, ha sido de investigación aplicada, dirigido y enfocado principalmente a diferentes escenarios (aplicación en casos de uso). Por ello, la importancia de crear una arquitectura integrada con la tecnología estándar de SWE, que facilite la especificación de nuevos sistemas para todo tipo de ámbitos.

Las motivaciones que han llevado a la realización de la presente tesis son las siguientes:

- **Interoperabilidad**

En la actualidad, existen estándares (protocolos y especificaciones) que tratan de lograr interoperabilidad entre redes de sensores. Pero las redes de sensores reales son específicas de cada proveedor y las aplicaciones son propietarias, por lo tanto, son necesarias adaptaciones para poder interoperar si las diferentes redes de sensores pertenecen a distintos fabricantes. Por tanto, para poder crear redes de sensores más amplias, es imprescindible mejorar la interoperabilidad para facilitar una comunicación más rápida y efectiva entre ellas. La iniciativa OGC fundó SWE para promover la interoperabilidad, la definición de los diversos servicios y componentes.

- **Especificación de arquitectura genérica**

Diseño de una arquitectura genérica, que pueda ser utilizada en diversos escenarios y dominios de aplicación, para crear sistemas de monitorización y control. Debe poder integrar todo tipo de WSNs, para poder recopilar la mayor cantidad posible de

información, con el fin de tomar decisiones acordes con la situación. Para ello, debe estar basada en los estándares de SWE, de modo que su aplicación sea óptima.

- **Usabilidad**

La utilización de un estándar genérico y extensible facilita la aplicación, ya que es posible personalizarlo a las necesidades de casa situación. Además, tanto OGC como la comunidad de usuarios que le da soporte, actualizan y mejoran continuamente el estándar y su implementación. Por otra parte, la arquitectura definida debe tener bloques simples y adaptables, que faciliten su aplicación en todo tipo de entornos.

- **Aplicación de tecnologías semánticas**

La aplicación de tecnologías semánticas en sistemas de sensores, permite introducir una capa de alto nivel para las arquitecturas, y proporciona soporte para nuevos modelos de interacción (interoperabilidad semántica) y computación (Semantic Sensor Web). Las tecnologías semánticas permiten operar en contextos tecnológicos y físicos profundamente diferentes. La utilización de tecnologías semánticas mejora el modelo de interoperabilidad, añaden capas de inteligencia extendidas, ayudan en el proceso de adquisición del conocimiento y permiten la integración y fusión de información de fuentes semánticamente heterogéneas.

- **Seguridad de los trabajadores**

Los avances tecnológicos en seguridad en entornos industriales, han evolucionado considerablemente en los últimos años, pero todavía hay riesgos en materia de seguridad y salud de los trabajadores. Por lo tanto, los nuevos enfoques de diferentes ámbitos (jurídico, tecnológico, socioeconómico, etc.) deben ser construidos para garantizar la seguridad continua y el bienestar de los trabajadores en las fábricas de manipulación, mecanizado y montaje. El proyecto FASyS [8] tiene este objetivo principal desde un marco multidisciplinar. La aplicación de la arquitectura propuesta integra los sensores ý actuadores desplegados en la fábrica, así como diferentes fuentes de datos aplicadas al caso de uso de gestión y prevención de riesgos laborales.

- **Eficiencia de infraestructuras críticas**

El desarrollo del smart grid a partir de las redes de energía convencionales, es una gran mejora en la eficiencia y fiabilidad, pero el hecho de ser una infraestructura crítica implica requisitos de seguridad muy elevados. En un Sistema de Gestión de la Seguridad de la Información (SGSI) de este tipo, todos sus elementos deben ser monitorizados en tiempo real, a fin de evitar de forma proactiva cualquier ataque y actuar reactivamente en caso de suceder. Los diferentes componentes han sido tratados como sensores/actuadores, permitiendo la interoperabilidad con diferentes protocolos y

aplicaciones mediante los estándares SWE. La aplicación de la arquitectura propuesta se adapta a la topología y características de la red, sensores y actuadores de un entorno como un smart grid y está compuesta por un bloque destinado a la recogida continua de datos y otro para el procesamiento y visualización. El caso de uso propuesto se dirige a la mejora de la eficiencia y la seguridad en el marco del proyecto de investigación UniverSEC [9].

- **Gestión inteligente de la logística en áreas urbanas**

Las congestiones de tráfico, son uno de los desafíos más críticos en áreas urbanas referente a la movilidad, lo que acaba provocando retardos en los desplazamientos, aumento del gasto de combustible, incremento de la emisión de gases de efecto invernadero, e incluso pérdidas económicas significativas para algunas empresas. Adicionalmente, la selección de la ruta más adecuada, puede suponer una reducción del tiempo de desplazamiento, así como de las emisiones de CO2. Los sistemas de transporte inteligente (Intelligent Transport Systems, ITS), como el desarrollado en STIMULO [10], pretenden integrar las Tecnologías de Información y Comunicaciones (TIC) con la infraestructura de transporte existente, con objeto de reducir la congestión, mejorar la seguridad y reducir las emisiones de CO2. Y en el caso concreto del proyecto STIMULO, de forma adicional, determinar la hora estimada de llegada de un camión a un punto de carga y descarga (ej. zona de contenedores del Puerto de Valencia). Partiendo de la utilización de la información procedente de diferentes sensores como cámaras de tráfico, sensores de velocidad, sensores de intensidad del tráfico, crowdsensing y la información procedente de los propios vehículos. La utilización de SWE y sus estándares asociados, permiten extender la utilización de SWE a un caso de uso relacionado con las ciudades inteligentes y en concreto la movilidad inteligente.

1.3. Objetivos de la Tesis

Una breve enumeración de los objetivos que se relacionan con las motivaciones de la creación de la tesis son:

- Describir y analizar el estado del arte en el acceso a sensores y redes de sensores vía web.
- Definir mecanismos de interoperabilidad a nivel web de sensores de diferentes tipos y fabricantes.
- Diseñar y especificar una arquitectura para redes de sensores, adecuada a las características y necesidades propuestas en la tesis, teniendo en cuenta los requerimientos de los casos de uso, criterios de escalabilidad, seguridad e interoperabilidad.
- Analizar la aplicación y la usabilidad del paradigma SWE de OGC y todos sus estándares en casos de uso reales, definidos en los proyectos de investigación relacionados.

- Diseñar y desarrollar los sistemas de seguridad, integridad y privacidad de las comunicaciones para el acceso a fuentes de información distribuidas en diferentes casos de uso.
- Diseñar y aplicar la arquitectura para la gestión, el tratamiento y el análisis de información en tiempo real, ya sea sobre el estado vital de un trabajador, un sistema crítico o una flota, accesible vía web mediante la utilización de SWE y un HMI específico para cada uno de los casos de uso.
- Aplicar el modelo y arquitectura propuestos al caso de uso de mejora de la seguridad de los trabajadores dentro del concepto de fábrica del futuro (FoF), mediante la captura de información de las redes de sensores desplegadas, y la herramienta de toma de decisiones, a partir de la información obtenida.
- Aplicar el modelo y arquitectura propuestos al caso de uso de optimización en el manejo y diseño de los equipos y procesos de fabricación, mediante la información procedente de sensores desplegados en una fábrica.
- Aplicar el modelo y arquitectura propuestos al entorno smart grid y la valoración del nivel de aseguramiento, como aspecto clave de la protección de infraestructuras críticas.
- Desarrollar servicios inteligentes de gestión del tráfico, por medio de la predicción en tiempo real del estado de los componentes del sistema de transporte (infraestructura, vehículos, mercancías, usuarios…). Gestionando la información mediante el modelo y arquitectura diseñados y desarrollados.

1.4. Principales aportaciones

1.4.1. Artículos

- Jose R. Gisbert, Carlos Palau, Mikel Uriarte, Gonzalo Prieto, Jose A. Palazón, Manuel Esteve, Oscar López, Javier Correas, Mari-Carmen Lucas, **Pablo Giménez**, Agustín Moyano, Luis Collantes, Javier Gozalvez, Benjamín Molina, Oscar Lázaro, Alicia González, "Integrated System for Control and Monitoring Industrial Wireless Networks for Labour Risk Prevention", Journal of network and computer applications, vol. 39, pp. 233-252, July 2013
- **Pablo Giménez**, Benjamín Molina, Jaime Calvo-Gallego, Carlos E. Palau, Manuel Esteve, "I3WSN: Industrial Intelligent Wireless Sensor Networks for Indoor Environments", Computers in industry, vol. 65, n 1, pp. 187-199, January 2014

1.4.2. Congresos

- **Pablo Giménez**, Benjamín Molina, Carlos E. Palau, Manuel Esteve, "Semantic Sensor Web Simulator for Factory Automation", URSI 2012, Elche, September 2012

- **Pablo Giménez**, Benjamín Molina, Carlos E. Palau, Manuel Esteve, "Sensor Web Simulation and Testing for the IoT", IEEE International conference on Systems, Man, and Cybernetics (IEEE SMC 2013), Manchester, October 2013
- **Pablo Giménez**, Benjamín Molina, Carlos E. Palau, Manuel Esteve, "Security assurance en Smart Grid", URSI 2014, Valencia, September 2014
- Benjamín Molina, Carlos E. Palau, **Pablo Giménez**, Manuel Esteve, Ricardo Guerrero Gómez-Olmedo, Roberto López-Sastre, "Estimación de tráfico en tiempo real para ITS mediante técnicas de Visión Artificial", URSI 2014, Valencia, September 2014

1.4.3. Capítulos libro

- **Pablo Giménez**, Benjamín Molina, Carlos E. Palau, Manuel Esteve, Jaime Calvo, "Smart manufacturing through cloud-based smart objects and SWE", Internet of Things based on Smart Objects, pp 107-128, January 2014

1.4.4. Participación proyectos investigación

- Proyecto FASyS
  - D3.1.2 Arquitectura del sistema de comunicación
  - D3.3.2 Especificación semántica de redes de sensores e interoperabilidad en el sistema FASyS
  - D7.4.1 Diseño Definitivo del sistema de monitorización y control de la plataforma FASyS
- Proyecto UniverSEC
  - E2 Especificación de requisitos y arquitectura
  - E3.3 Protocolo de Interoperabilidad
  - E4.1 Integración de prototipos
- Proyecto STIMULO
  - E2.3 Especificación de la arquitectura
  - E4.4 Mecanismos de integración de servicios de terceros
  - E5.1 Demostrador de recogida de datos y análisis de información

1.4.5. Software

En cada uno de los proyectos, se ha generado software que posteriormente se ha podido utilizar en otros proyectos de investigación, como es el simulador de sensores, la metodología para desarrollar el HMI, etc.

1.5. Organización de la memoria

La memoria de la tesis está estructurada de la siguiente manera:

- El segundo capítulo, presenta el estado del arte de la gestión de información en redes de sensores, su empleo en diferentes aplicaciones y la gestión de la interoperabilidad. También se evalúa el estado actual de protocolos de seguridad y la aplicación de IoT.
- El tercer capítulo, especifica la arquitectura general diseñada para la aplicación de SWE a diferentes entornos, y la descripción de todos sus elementos.
- El cuarto capítulo, detalla la aplicación de la arquitectura al caso de uso de FASyS. Se describen el funcionamiento de los principales elementos del sistema de monitorización y control.
- El quinto capítulo, detalla la aplicación de la arquitectura al caso de uso de UniverSEC. En primer lugar, se describe el smart grid como una infraestructura crítica que debe tener una evaluación del nivel de security assurance para funcionar correctamente. A continuación, se especifican los componentes de sistema y su funcionamiento.
- El sexto capítulo, detalla la aplicación de la arquitectura al caso de uso de STIMULO. Se define el concepto de smart city como base del sistema para la gestión del tráfico implementado. Después se determinan los bloques del sistema ITS, las interacciones entre ellos y su funcionamiento.
- En el séptimo capítulo, se lleva a cabo la evaluación de los sistemas diseñados en los tres casos de uso. Para ello, se ponen en funcionamiento en un escenario predefinido y se evalúan los resultados.
- El octavo capítulo, comprende las conclusiones a las que se han llegado durante la elaboración de esta tesis, así como posibles líneas futuras de investigación.
- Por último, se encuentran las referencias citadas y un glosario con los acrónimos utilizados.

2. Estado del arte

2.1. Introducción

Internet of Things, se basa en la conexión de diferentes sensores y objetos a Internet, para que sea posible su control, administración y acceso a la información generada a distancia y mediante protocolos y aplicaciones estándar. La integración de este tipo de información, con datos procedentes de otras fuentes en un entorno de tipo web, ha dado lugar al concepto de "Web of Things" o "Web of Objects", del que SWE es un claro exponente. Internet of Things no es en sí misma una tecnología disruptiva, la novedad de la misma radica en el despliegue de multitud de objetos inteligentes capaces de comunicarse entre sí y la posibilidad de interoperar.

Actualmente, muchos sensores tienen interfaces de tipo propietario definidos por sus fabricantes y empleados de manera selectiva, de forma que cualquier nueva API se solicita y se desarrolla bajo demanda. Este hecho requiere que, para la implantación del paradigma de la Internet of Things, sea necesario un gran esfuerzo por parte de los desarrolladores para la integración de un nuevo sensor o la realización de un nuevo proyecto, pero también por parte de los fabricantes de nuevos sensores, pasarelas o portales de integración de sensores que es finalmente donde muchas de estas informaciones son empleadas. La utilización de interfaces estándar para los sensores en el marco de Internet of Things, permitiría que las aplicaciones y servicios relacionados proliferaran exponencialmente, mejorando la economía de escala así como la interoperabilidad y reutilización. Los estándares de Sensor Web Enablement (SWE) de OGC son los únicos que se focalizan en el contenido de la información de los sensores y en facilitar la integración de los datos generados en las diferentes aplicaciones de usuario, permitiendo la evaluación de los datos por parte de los usuarios y el procesado de la misma para crear información derivada, adecuada a las necesidades específicas de cada caso de uso y escenario.

En este capítulo, se proporciona un estado del arte exhaustivo de todos los estándares, protocolos, especificaciones y aplicaciones que han sido necesarios en el desarrollo de esta tesis. En primer lugar, se analizará el paradigma SWE propuesto por OGC y que ha sido el marco en el que se ha definido la arquitectura empleada en la tesis. A continuación, se estudian diferentes estándares en el campo de la monitorización industrial y también referente a seguridad industrial. Después, se investigan distintas técnicas y procesos para la gestión del tráfico en sistemas ITS. Por último, se estudia el concepto de Internet of Things.

2.2. SWE y aplicaciones

2.2.1. De sensores heterogéneos a *sensor web*

La definición del concepto de sensor desde la perspectiva de la ingeniería, es la de un dispositivo que recibe un estímulo y responde con una señal eléctrica. Dicho estímulo se trata de una propiedad física, la cual es observada por el sensor. [11]

Esta primera definición de sensor, debe ser extendida desde una perspectiva computacional, que nos indica que un sensor es una entidad que observa una propiedad

física (ej., temperatura, humedad, presión, o nivel de agua) y produce una representación digital de la misma. Pero además, un sensor puede recibir comandos para realizar ciertas acciones, como pueden ser cambiar la frecuencia de muestreo, cambiar el ángulo de visión en una cámara, etc.

Cuando varios sensores están reunidos en una única plataforma y conectados, se pueden considerar como un sistema de sensores [12], y su vez, un sistema de sensores puede referirse globalmente como un único sensor [13]. Algunos ejemplos de sistemas de sensores son estaciones meteorológicas con sensores conectados, o una combinación de frecuencia cardiaca y sensores de presión arterial para una persona. Una red de sensores se compone de un número de sensores o sistemas de sensores espacialmente distribuidos y que se comunican entre sí [14] [15].

Del mismo modo, se acuña el término de objeto inteligente (smart object), que son dispositivos de uso diario que están mejorados por un dispositivo electrónico que les dota de una cierta inteligencia local así como conectividad a Internet. El dispositivo electrónico es el componente computacional que se une al elemento físico y que permite salvar la brecha entre el mundo físico y el digital. Por lo tanto, se puede decir, que un objeto inteligente puede ser tanto un sistema empotrado como un Cyber-Physical System (CPS). Los datos que son generados por los objetos inteligentes son finalmente integrados, procesados y utilizados por otros objetos inteligentes y por aplicaciones de usuario, como sería el caso de ***sensor web*** [16].

El término *sensor web* fue acuñado inicialmente en los laboratorios JPL (Jet Propulsion Laboratory) de la NASA en 1997 [3], para describir una novedosa arquitectura de sensores inalámbricos donde cada uno de los nodos podía actuar y coordinarse como un único grupo. Otra de las características de estos nuevos sistemas diseñados en la NASA era su comportamiento asíncrono, lo que representaba una propiedad deseable en la mayoría de las implementaciones de sensores en la práctica. Adicionalmente, cada uno de los nodos que componían el sistema era equivalente en términos de hardware [17], por lo que la arquitectura diseñada no requería ningún dispositivo adicional de enrutamiento para permitir la comunicación entre nodos.

Desde un punto de vista formal, *sensor web* es una entidad autónoma capaz de percibir (sentir) una o más propiedades físicas de su entorno, de tal forma que es capaz de interpretar y reaccionar ante las medidas obtenidas sobre dicha propiedad física. Aunque *sensor web* no requiere la presencia del WWW para funcionar, sí es típico el empleo del WWW para interconectar varios nodos, es decir, se utiliza a efectos de interoperabilidad e integración de la información [18].

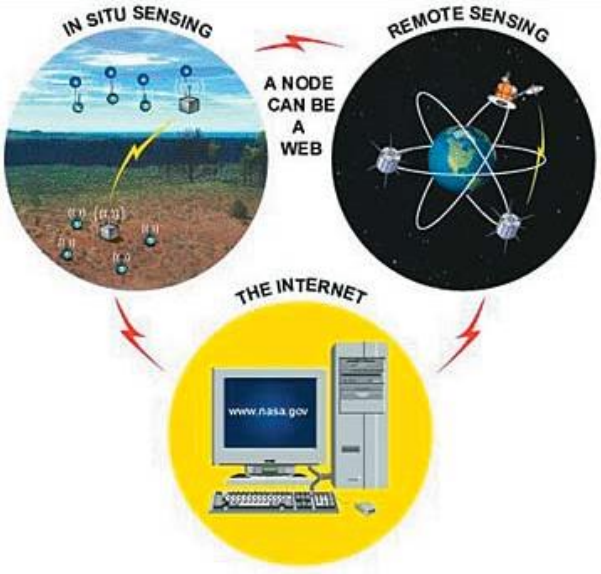

Figura 1. Concepto general de *sensor web* [19]

Un nodo perteneciente a *sensor web* es básicamente un sistema físico que soporta un sensor y, de esta forma, puede ser fijo o móvil, terrestre o acoplado a un satélite. En ocasiones, es incluso posible acceder en tiempo real a dicho nodo sensor a través de Internet. La comunicación entre nodos es tanto omnidireccional como bidireccional. La comunicación omnidireccional implica que no hay un flujo dirigido de la información, mientras que la comunicación bidireccional permite contactar (y, a veces, controlar) otros nodos, así como recibir información de ellos. De esta forma, la información en *sensor web* puede ser de cuatro tipos distintos:

- Datos en bruto (raw data) obtenidos en los nodos sensores.
- Datos post-procesados de un nodo o un grupo de nodos.
- Comandos de control introducidos en el sistema por un usuario externo a través de un nodo portal.
- Comandos introducidos en el sistema por otro nodo (ej. M2M).

En cualquiera de los casos anteriores, la idea principal, es que *sensor web* procese internamente este flujo de datos continuo, genere conocimiento a partir de estos datos, y reaccione ante dicho conocimiento. Dicho en otros términos, es posible la fusión de datos en tiempo real, y que el sistema reaccione como un conjunto único colectivo coordinado ante el flujo de datos entrantes. Por ejemplo, en lugar de disponer de una serie de sensores detectores de humos dispersos y descoordinados, *sensor web* puede reaccionar como un detector de fuego único y coordinado, aunque esté espacialmente distribuido siempre que se cumplan las condiciones de comunicación, interoperabilidad e integración de los nodos.

El esquema principal de interconexión se muestra en la Figura 2, donde los sensores se conectan a los nodos. Dichos nodos se comunican mediante una red inalámbrica, para conformar una red mallada, donde todos los nodos son equivalentes y cada nodo puede ser usado como pasarela hacia otra red.

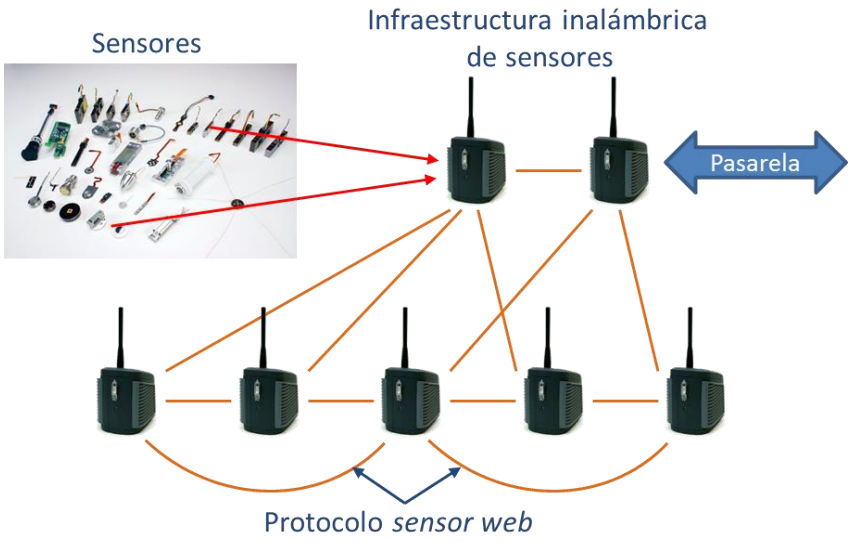

Figura 2. Representación esquemática de *sensor web*

Es importante recalcar el hecho de que, aunque el hardware de un nodo pueda ser bastante sofisticado, es el proceso de intercambio de información entre los nodos, y la suma de sus capacidades, lo que dota a *sensor web* de su inteligencia. Esto es similar a cómo se produce el fenómeno de la percepción en el cerebro, a partir de la interacción de un conjunto complejo de neuronas que intercambian señales electro-químicas [20], en lugar de emplear la inteligencia individual de cada neurona.

Las propiedades de *sensor web* son las siguientes [21] [22]:

- El intercambio de datos redundante sin enrutamiento, permite que cualquier nodo se comporte como una pasarela hacia el exterior. Dado que todos los componentes de *sensor web* contienen la misma información, cualquier usuario con acceso a uno de los nodos será capaz de obtener la misma visión de conjunto.
- Referencia temporal común y única, que requiere que exista una sincronía en los relojes individuales de los nodos.
- El comportamiento síncrono del sistema reduce la latencia entre la obtención de los datos y la notificación. Cada nodo tiene la misma conciencia situacional al final de cada ciclo de medida. Dado que cada nodo puede actuar como punto de acceso al sistema, esto implica que todos los usuarios finales obtienen información actualizada en cada ciclo de medida.
- Las rutas de comunicación redundantes proporcionan una estructura robusta sin prácticamente ningún punto singular de fallo. Dado que todos los nodos son potencialmente pasarelas o puntos de acceso a la infraestructura, la pérdida de un nodo particular no afecta a la gestión y la operación global.
- El intercambio de datos redundante sin enrutamiento permite la recuperación ante fallos de un nodo sensor. Puesto que todos los nodos contienen un microprocesador y son conscientes de todas las medidas del sistema, en cada periodo de medición, cada nodo es capaz de analizar de manera local condiciones

globales en todo *sensor web*. Es por ello, por lo que le es posible evaluar de forma inmediata al sistema una medida aparentemente anómala y detectar (y descartar) falsos positivos, para distinguir entre una mala tendencia frente a una situación crítica que suponga una evacuación de personas.

- Las rutas de comunicaciones redundantes permiten que el sistema se despliegue de una manera rápida y sencilla. No es necesario ninguna habilidad especial para configurar *sensor web* dado que todos los nodos son esencialmente lo mismo, en contraste con otros esquemas de despliegue de red que requieren hardware especial para hacer de pasarelas o routers. Como resultado, una vez se conecta un nodo madre para proporcionar una señal de reloj, el resto de nodos, se pueden dispersar según dicte las exigencias de la situación.

Por tanto, *sensor web* se ha convertido rápidamente en una plataforma de referencia estable con la que enlazar múltiples sensores. A medida que los sensores se producen en masa, baja potencia consumida y baja su coste, aumentan el número de aplicaciones que lo utilizan.

Sensor web es un macro instrumento, ideal para la monitorización y exploración in situ del medio ambiente, donde nodos relativamente simples interactúan entre sí para conseguir operaciones y comportamientos más complejos. La idea clave sobre *sensor web* es que cada nodo puede ser, en sí mismo, un servicio web, y que conduce al concepto de interweb. Esto permite un análisis local para crear control distribuido en un nivel sin precedentes. Las aplicaciones no están centradas únicamente en un solo sector, sino que el concepto es flexible y se puede usar tanto en entornos terrestres, acuosos, atmosféricos o incluso espaciales. El comportamiento cooperativo entre los nodos permite tener una capacidad de procesado baja, relativamente barato, y ser prescindibles individualmente.

2.2.2. *Sensor web* en sentido amplio

La denominación inicial de *sensor web* [23], ha sufrido una evolución conforme avanzaba Internet, la tecnología web y más explícitamente Internet of Things y la integración de smart objects en diferentes aplicaciones. Es un tipo especial de infraestructura de información centrado en Web para recopilar, modelar, almacenar, recuperar, compartir, manipular, analizar y visualizar información sobre los sensores y las observaciones de los sensores. La falta de estandarización, sin embargo, es la barrera principal para la progresión de *sensor web*.

En la actualidad, el término *sensor web* se emplea mayoritariamente para referirse a sensores conectados a Internet y con capacidad de integrarse en entornos WWW. Se han realizado diferentes especificaciones en este sentido, pero la de más amplio impacto es SWE y el conjunto de especificaciones y estándares de OGC [24], un consorcio internacional que reúne a la industria, sector académico y organizaciones gubernamentales encargadas de desarrollar estándares geoespaciales abiertos. OGC define sensor web como "redes de sensores accesibles vía web y los datos de los

sensores que se pueden descubrir y acceder utilizando protocolos estándar desde diferentes aplicaciones".

En este contexto, la arquitectura de red está basada en IP y permite conectar de manera individual los nodos sensores. La arquitectura propuesta por OGC, es conceptualmente diferente a la arquitectura anteriormente comentada [3] y requiere el uso de esquemas que permitan integrar diferentes nodos, de la misma forma que TCP/IP permite integrar diferentes dispositivos hardware.

La principal aplicación de *sensor web* en entornos actuales, es la de integrar datos de sensores públicos y/o privados en aplicaciones que generalmente se comunican mediante el protocolo HTTP (especialmente navegadores), con el fin de lograr el conocimiento de la situación. Esta capacidad de integración se basa en esquemas web que permiten una fácil interoperabilidad. Los sensores deben tener conectividad IP, que es una de las bases del Internet of Things, y en caso de no disponer de ella, es necesario que dispongan de una pasarela que habilite dicha conectividad.

2.2.3. Estándares de interoperabilidad

Se entiende la interoperabilidad como la condición necesaria para permitir la relación entre productos o sistemas diferentes (sistemas heterogéneos), sin ningún tipo de ambigüedad, para poder intercambiar datos o coordinar procesos. Esta interoperabilidad se puede encontrar presente en cualquier sistema, ya sea informático, geográfico, ferroviario o de otro tipo.

Las redes de sensores tienen un componente de distribución que requiere de capacidad de comunicación entre ellos, con la finalidad de permitir la comunicación nodo a nodo (M2M) y para realizar la integración entre sensores o grupos de ellos y aplicaciones. La integración de sensores de diferentes fabricantes, requiere de la utilización de estándares para garantizar la integración y la interoperabilidad. La interoperabilidad en el ámbito de las redes de sensores debe realizarse a diferentes niveles: (i) dispositivo, (ii) red, (iii) middleware y (iv) semántica.

La interoperabilidad a nivel de dispositivo y red, requiere de estandarizar la comunicación de los sensores en los niveles más bajos del modelo de referencia [25]. En un principio se consideraba el interfaz RS-232 como el estándar dominante [26], aunque ahora los sensores se equipan con un interfaz Ethernet (IEEE 802.3).

El entorno de aplicación en el que se utilicen las redes de sensores influye en las redes de comunicaciones a emplear (ej. la electrónica de consumo, la automatización industrial o la automoción), en todos ellos se utilizan cada vez más los protocolos de comunicación inalámbrica de corto alcance con bajo consumo de energía [27], como por ejemplo ZigBee [28], WirelessHART [29] o ISA100.11a [30] en combinación con IEEE 802.15.4 o Bluetooth (IEEE 802.15.1) [31].

La necesidad de dotar de interactividad a nivel de red entre nodos, ha llevado a añadir más funcionalidades a los mismos, para facilitar la comunicación y el acceso a los

sensores, como es el caso del protocolo Universal Plug and Play (UPnP) [32] y Digital Living Network Alliance (DLNA) [33]. Utilizando UPnP se puede implementar una arquitectura de red distribuida de dispositivos que les permite entrar y dejar una red de forma automática. La especificación UPnP fue desarrollada por el Foro UPnP, un consorcio industrial formado por más de 900 empresas. Su enfoque está más orientado a las redes domésticas, es decir, para conectar dispositivos electrónicos como portátiles, impresoras, escáneres o teléfonos. El objetivo de DLNA es proporcionar interoperabilidad robusta en la electrónica de consumo, como son ordenadores y dispositivos móviles, mediante una red troncal de control y comunicaciones basada en tecnologías y estándares existentes. DLNA utiliza marco del protocolo de control de dispositivos UPnP, que proporciona una forma simple para crear redes de dispositivos en el hogar. Las directrices de interoperabilidad de DLNA utilizan la arquitectura de Audio y Video (AV) de UPnP para proporcionar la gestión de los contenidos y una solución para el control de dispositivos. Por ejemplo, la televisión o la impresora de un usuario pueden buscar y reproducir o visualizar el contenido que se comparte en una red doméstica por el dispositivo servidor.

Devices Profile for Web Services (DPWS) [34] es un estándar similar a UPnP/DLNA, aunque más relacionado con la tecnología de servicios web, incluyendo múltiples extensiones, que le permiten integrar servicios para dispositivos en diferentes entornos de aplicación. De hecho, DPWS es una versión ligera del conjunto de estándares WS-* [35], lo que facilita la ejecución de servicios web en dispositivos con recursos limitados. El objetivo, es permitir la comunicación entre máquinas (M2M) e integrar directamente los dispositivos con los procesos de negocio. Las áreas de aplicación de DPWS son también la electrónica de consumo, pero también la automatización en los procesos de fabricación industrial. Un ejemplo de implementación de un conjunto de herramientas para DPWS es WS4D [36].

De forma similar a DLNA, CoAP (Constrained Application Protocol) [37] es un protocolo del IETF que se utiliza en dispositivos electrónicos muy simples para comunicarse de forma interactiva a través de Internet. Principalmente, se diseñó para pequeños sensores de baja potencia, interruptores, válvulas y componentes similares que necesitan ser controlados o supervisados de forma remota, a través de Internet. CoAP es un protocolo de capa de aplicación que está diseñado para su uso en dispositivos con acceso a Internet con recursos limitados, tales como nodos WSN.

Para garantizar la interoperabilidad entre sistemas, se pueden utilizar modelos de datos y metadatos, así como sistemas de comunicación basados en estándares. Además, para permitir una mayor flexibilidad, pueden existir mecanismos que permitan desarrollar una capa de abstracción semántica que facilite la interoperabilidad. Entre los modelos de representación de datos utilizados actualmente podrían destacar JSON [38], XML [39] o YAML [40]. Todos estos modelos están enfocados a crear un marco para la representación de datos entre los sistemas involucrados.

El estándar IEEE 1451 [41] [42], es una familia de estándares de alto nivel organizado alrededor de un conjunto de arquitecturas y protocolos comunes para permitir la

interoperabilidad en las redes de sensores inteligentes. El objetivo principal de esta familia de estándares, es permitir el acceso a los datos del transductor a través de un conjunto común de interfaces, si los transductores están conectados a sistemas cableados o inalámbricos.

2.2.4. SWE de OGC

La información que normalmente se recibe de los distintos sensores, además de sus atributos espaciales y temáticos, también tienen una varianza temporal. La capacidad de poder usar y aprovechar estos (SDI, Spatial Data Infrastructures) [43] depende considerablemente de la posibilidad de soportar el acceso en tiempo real a información que varía en el espacio y en el tiempo. Los datos de sensores (sensor data) son, posiblemente, la geoinformación variante en el tiempo y espacio más importante. Existe un gran número de casos de uso donde la disponibilidad de fuentes de datos recogidas por sensores es esencial, por ejemplo en los casos de gestión de riesgos. A través de servicios tradicionales de OGC, es posible, solicitar información de sensores, pero sólo de una forma limitada, como en los siguientes ejemplos:

- Un mapa de la temperatura de un Web Map Service (WMS) [44] de una cierta área de interés e instante en el tiempo.
- Acceder a datos de tipo raster como imágenes de satélite o los resultados de modelos de dispersión mediante Web Coverage Service (WCS) [45].
- Acceder a datos vectoriales, por ejemplo, la traza de un vehículo mediante Web Feature Service (WFS) [46].

La integración de los activos de los sensores en las SDI hace que sea posible acoplar datos disponibles del sensor con otros recursos espacio-temporales (por ejemplo, mapas, raster, así como datos vectoriales) al nivel de aplicación, lo que maximiza la efectividad de información para apoyo a la decisión. Sin embargo, SDI no disponía de un marco genérico para integrar datos de sensores, por lo que resultó necesaria la ampliación de las especificaciones de SDI para contemplar esta situación. Es por ello, por lo que OGC puso en marcha la iniciativa SWE, con el objetivo de desarrollar estándares para acceder y controlar sensores y redes de sensores a través de Internet, con una visión de tipo ‘plug-and-play’. SWE es un conjunto de interfaces y codificaciones estandarizados, que permite integrar conjuntos de sensores heterogéneos en la infraestructura del sistema a través de interfaces basados en web y estándares de comunicaciones. Estos estándares permiten la incorporación de sensores modernos en un sistema sin complicaciones y frágiles interfaces punto a punto. Permite la fusión de múltiples modelos y formatos de datos en un modelo común de datos y representación. Los servicios SWE pretenden también normalizar la visión de *sensor web*.

Las redes de sensores, tal y como se conciben en la actualidad, son muy dependientes del problema a resolver y del escenario a desplegar. Lo que supone que vengan caracterizadas por un enfoque y funcionalidad limitados, y conteniendo datos que no son fácilmente compartibles con otros sistemas; lo que se traduce en sistemas

propietarios y con dificultades para interoperar, sobre todo en el ámbito del descubrimiento, el acceso a las observaciones, la recepción de alertas y la asignación de tareas. La integración de un sensor nuevo en estos sistemas es típicamente una tarea altamente costosa, debido a servicios y codificaciones incompatibles. Para poder acometer la visión 'plug-and-play' propuesta por OGC, se requieren las siguientes funcionalidades:

- Descubrimiento de sensores y datos de sensores.
- Determinación de las capacidades de los sensores y la calidad de las medidas.
- Acceso a los parámetros de los sensores que permiten al software procesar las observaciones automáticamente.
- Acceso a medidas en tiempo real, así como a medidas de ventanas temporales en codificaciones estandarizadas.
- Configuración de sensores y simulaciones para adquirir observaciones de interés.
- Suscripción y publicación de alertas llevadas a cabo por los sensores y basadas en algún tipo de criterio (notificación basada en eventos).

La arquitectura SWE de OGC consta de dos bloques principales: el **modelo de información** y el **modelo de servicio**. El primero de ellos consiste en los modelos conceptuales y las codificaciones, mientras que el segundo estriba en la especificación de servicios. La separación en estos dos bloques representa un punto de vista lógico sobre la arquitectura SWE, aunque ello no quiere decir que no existan enlaces entre ambos. La Figura 3 muestra ambos modelos, sus componentes y su interrelación.

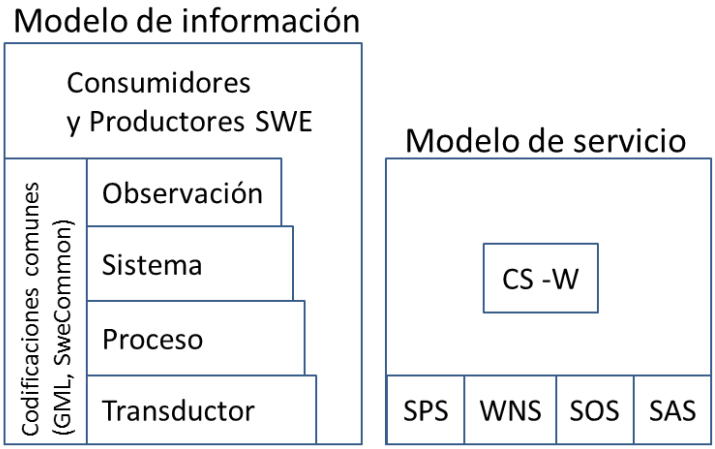

Figura 3. Bloques principales de la arquitectura SWE

Modelo de información

El modelo de información de SWE representado en la Figura 3 engloba los componentes conceptuales descritos en el estándar:

- **Transductores**: representan la interfaz entre el mundo real y el mundo digital, por lo que forman los elementos básicos de una red de sensores y su interacción con las aplicaciones que usan y acceden a dichos datos. Los transductores que

convierten fenómenos en datos se denominan comúnmente sensores, mientras que los transductores que convierten datos en fenómenos, se llaman transmisores o actuadores.

- **Procesos**: dependiendo de una serie de métodos predefinidos y parámetros, un proceso es capaz de generar una o más salidas a partir de una o más entradas. Es decir, que el estándar SWE no es un entorno pasivo, sino que permite el almacenamiento de la información y el consumo y procesado de la misma.
- **Sistema**: consiste en un conjunto de transductores y procesos, para los cuales se ha definido una posición relativa a un sistema de coordenadas interno definido. Al relacionar el sistema de coordenadas interno con sistema geográfico de referencia, el sistema, sus componentes y sus medidas producidas pueden ser georeferenciadas.
- **Observación**: el acto de observar un fenómeno es lo que se denomina observación. Ésta contiene información relativa al histórico de la medida, el valor resultante, el tiempo en que se tomó la medida y el fenómeno observado. Es la información que se almacena y sobre la que se ejecutan los procesos.

El volumen de información contenido en los elementos anteriormente citados se va enriqueciendo desde los datos en bruto (transductores), hasta los datos procesados (observación). Cada capa lógica del modelo de información conforma la base de otra capa. Por ejemplo, la información servida por los transductores representa la entrada de los procesos. Las aplicaciones tienen acceso a todas estas capas, aunque deberían usar la información de las capas superiores para garantizar un mayor grado de interoperabilidad, flexibilidad y enriquecimiento de la información. Los componentes de cada capa emplean elementos del tipo SweCommon, un formato de datos definido por SWE que contiene elementos comunes y que está basado en GML (Geography Markup Language) [47].

A continuación, se describen las especificaciones que forman la base del modelo de información:

- Transducer Markup Language (TML): este lenguaje proporciona la descripción de los datos del sensor, así como la información necesaria para comprender el proceso de obtención de datos. También se emplea en archivar e intercambiar datos de sensores. La especificación TML [48] define un modelo a partir del cual se puede enviar (en formato streaming), archivar, agregar y analizar de manera eficiente los datos de sensores siguiendo un formato común. El formato de los datos en bruto proporcionados por los sensores no se envían sin formato, sino que más bien TML define una estructura que permite describir tanto el formato de datos empleado, como los metadatos del sensor. Estos últimos contienen –entre otros – información que permite a la aplicación determinar el tiempo y la localización de la medida. TML permite decodificar, procesar y analizar datos de sensores sin necesidad de acceder a información adicional de otras fuentes. TML está especialmente diseñado para transmitir streams de datos, por ejemplo, streams de vídeo [49]. Los

datos pueden ser enviados (en formato streaming) desde un archivo o directamente desde el sensor. No obstante, en el contexto de SWE, TML se usa principalmente para enviar datos en vivo desde el sensor al cliente.

- Sensor Model Language (**SensorML**): este lenguaje describe un formato común [50] para la descripción de sensores y sistemas de sensores lo que facilita el descubrimiento de sensores, así como el análisis y procesado de datos de sensores. La idea principal en SensorML es que los sensores pueden ser modelados como procesos. Los modelos de proceso definen entradas y salidas, el sistema de referencia empleado, parámetros disponibles y el método de un proceso. Adicionalmente, se pueden introducir metadatos en un proceso. Estos metadatos contienen, por ejemplo, información general empleada en la identificación y clasificación de un proceso (y por ello de un sensor), y también contiene información acerca de las propiedades y capacidades de un proceso. Un proceso describe, o bien el procedimiento de medida actual, o un método que analiza los datos y genera información adicional.

  En términos generales, SensorML permite:

  - La descripción de la información que es requerida para la exploración de sensores, sistemas de sensores y procesos.
  - El archivo de parámetros del sensor, relevantes para una medida.
  - El procesado y análisis de datos de sensores bajo demanda. A través de los procesos SensorML se pueden realizar los pasos necesarios de procesado en tiempo real, basándose en la descripción del sensor y definiciones adicionales del proceso. Los posibles fallos introducidos durante el procesado pueden ser corregidos en todo momento. SensorML fomenta el desarrollo de librerías de proceso que puedan ser usadas por usuarios para procesado de datos.

- Observaciones y medidas (**O&M**, Observation & Measurements): la especificación O&M [51] proporciona un modelo estándar para representar e intercambiar resultados de observación. O&M es principalmente un modelo conceptual que describe la relación entre diferentes aspectos del proceso de captura de datos. En términos de O&M, una observación es un evento que tiene lugar en un momento temporal determinado y que genera un valor de un fenómeno observado. Además del momento temporal y el valor de la medida, O&M es capaz de describir otras propiedades de la medición, por ejemplo, el proceso empleado en generar la medida así como la ubicación y la calidad de la medida. O&M considera que el valor medido es una aproximación de un atributo de una propiedad de interés (FoI, Feature of Interest) observada. Se puede incluir información adicional como metadatos para un mayor análisis e interpretación de los datos. El formato O&M no sólo permite la definición de observaciones, sino también de fenómenos. Basándose en estas definiciones se pueden diseñar diccionarios que definan los fenómenos a emplear en un dominio de aplicación específico. Este tipo de

diccionarios forman la base para un completo conocimiento de los datos que los sensores capturan.

- SweCommon: dentro del marco de trabajo descrito por OGC SWE se requieren elementos para describir tiempo, fenómenos, posición, datos y otros parámetros. Es por ello, por lo que estos son definidos como un conjunto de tipos básicos en la especificación SweCommon. SweCommon establece las bases del modelo de información, y también es empleado en el modelo de servicio. Dentro de la especificación SweCommon, la información de posición no sólo incluye localización, sino que puede incluir también orientación, velocidad (lineal) aceleración (lineal), velocidad angular, aceleración angular, así como una marca de tiempo.

Modelo de servicio

El modelo de servicio describe los servicios del marco de trabajo descrito por OGC SWE. El objetivo de los servicios, es permitir a las diferentes aplicaciones y/o despliegues de sensores alternativos poder acceder de un modo interoperable a la información generada y almacenada, así como poder realizar operaciones sobre ella. Dichos servicios son los siguientes:

- Sensor Observation Service (**SOS**) [52]: el objetivo principal de este servicio es proporcionar almacenamiento y acceso a las observaciones de los sensores y sistemas de sensores de una forma estándar que sea consistente para todos los sistemas sensores, incluyendo sensores in-situ, remotos, fijos y móviles. SOS cumple con la especificación O&M para modelar observaciones de sensores, así como con la especificación SensorML para modelar sensores y sistemas sensores (metadatos de sensores). El SOS permite organizar un cierto número de observaciones en lo que se denomina "Observation Offering", que es algo análogo al concepto de capa en el Web Map Service, puesto que cada "offering" pretende ser un grupo de observaciones relacionadas que no se solapan ni espacial, ni temáticamente. En contraste con un WFS, el formato de un registro proporcionado por el SOS, solamente puede ser O&M o SensorML. De esta forma, las implementaciones de SOS son independientes de dominios de usuario o aplicaciones específicas y pueden ser usados desde cualquier cliente SWE compatible, sin necesidad de disponer de un conocimiento previo.

  La especificación dispone las diferentes operaciones SOS en varios perfiles: perfil básico (core profile); perfil transaccional (transactional profile); perfil mejorado (enhanced profile) y perfil completo (entire profile). El soporte del perfil básico es obligatorio para cualquier implementación SOS, mientras que el resto de perfiles son opcionales. Un SOS que soporte todas las operaciones, implementa el perfil completo.

Tabla 1. Perfiles del SOS

Perfil básico (funcionalidad básica del SOS)	Identificación de sensores disponibles con cierta capacidad de filtrado de parámetros (GetCapabilities)
	Acceso a los datos de sensores (GetObservation)
	Acceso a la descripción de los sensores (DescribeSensor)
Perfil transaccional (transactional profile)	Registro de un sensor nuevo (InsertSensor)
	Inserción de una nueva medida (InsertObservation)
Perfil mejorado (enhanced profile)	Un mecanismo eficiente de solicitar repetidamente datos de sensores (GetResult)
	Una descripción detallada de un FOI asociado a una medida (GetFeatureOfInterest)
	El tiempo para el cual se dispone de medidas para un FOI (GetFeatureOfInterestTime)
	Solicitar el esquema XML que define el formato de los FOIs (DescribeFeatureOfInterest)
	Solicitar el esquema XML que define el formato de las observaciones (DescribeObservationType)
	Solicitar el esquema XML que define el formato de las medidas (DescribeResultModel)

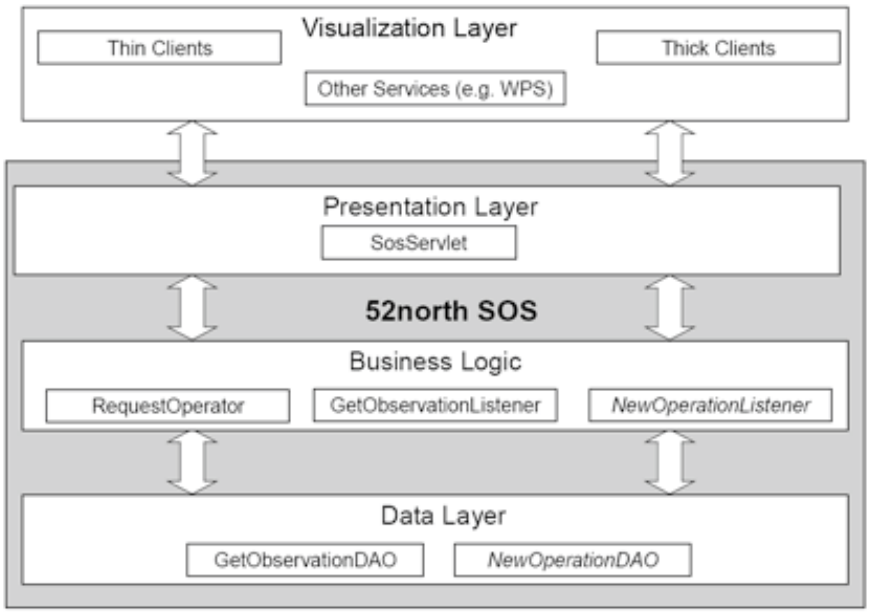

Figura 4. Arquitectura del SOS [53]

- Sensor Alert Service (SAS) [54]: es un sistema de notificación por eventos, como se observa en la Figura 5. Un productor puede anunciar nuevos tipos de eventos al sistema de notificación de eventos y, posteriormente, publicar otros nuevos. El consumidor se puede suscribir al servicio para alguno de los eventos disponibles. De esta forma, el consumidor será notificado automáticamente cada vez que tenga

lugar un evento al que previamente se suscribió. Es posible identificar varios tipos de eventos: la simple generación de una medida puede ser considerado como un evento, así como la superación de un valor umbral definido por el usuario o un mensaje de estado procedente de un sensor (por ejemplo el estado de la batería). La especificación SAS define operaciones sólo para la gestión del servicio de notificación de eventos. Se emplea un servidor de mensajería para el envío de las notificaciones a los clientes. Dado que este subservicio no es parte de la especificación SAS, su implementación queda a la elección de proveedor del servicio SAS.

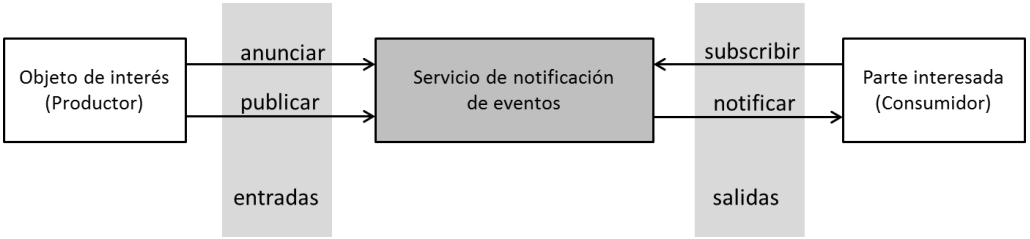

Figura 5. Sistema de notificación de eventos

El Sensor Event Service (SES) es una mejora del SAS. Ambos se utilizan para proporcionar acceso basado en la publicación/suscripción de datos de los sensores y mediciones. Las principales mejoras son la utilización de SOAP, el aumento de las capacidades de filtrado y la funcionalidad de conversión de unidades automática.

- Sensor Planning Service (SPS) [55]: este servicio ofrece una interfaz estándar para el control de los sensores. Por ello la interfaz contiene operaciones como:

  - Acceso a metadatos del servicio (GetCapabilities)
  - Obtener los parámetros de tareas de un sensor (DescribeTasking)
  - Inspeccionar la viabilidad de una tarea (GetFeasability)
  - Enviar una tarea (Submit)
  - Modificar una tarea (Modify)
  - Cancelar una tarea (Cancel)
  - Obtener el estado actual de una tarea (GetStatus)

  Dado que el tiempo requerido en completar una tarea se desconoce a priori, el SPS puede usar el servicio WNS para comunicarse con el cliente de una forma asíncrona. El almacenamiento de los datos recogidos queda fuera del ámbito del SPS. Para permitir a un cliente descubrir los datos recogidos en su tarea, el SPS ofrece la operación DescribeResultAccess.

- Web Notification Service (WNS) [56]: este servicio proporciona una interfaz para una comunicación asíncrona con un usuario o un servicio web. En general, los servicios web soportan una comunicación síncrona con el cliente. Si asumimos que enviamos una tarea al SPS que requiere un cierto tiempo para su ejecución (por ejemplo, obteniendo imágenes de satélite), entonces debemos disponer de una forma de saber cuándo se completó dicha tarea. En este caso el servicio WNS se

puede usar. WNS soporta la transmisión de notificaciones a través de varios protocolos de transporte. Los mensajes se pueden enviar a través de HTTP, mensajería instantánea (XMPP), e-mail, SMS, fax e incluso teléfono. Para conocer los protocolos que soporta un servicio concreto de WNS se emplea la operación GetCapabilities. La especificación distingue dos patrones de comunicación: notificación unidireccional y bidireccional.

- Catálogo de Servicios Web (CSW) [57]: esta especificación define un modelo abstracto de servicio para la gestión y búsqueda de metadatos. El modelo se basa en:
  - OGC Common Catalogue Query Language: define un lenguaje mínimo y abstracto de consulta de metadatos que debe ser soportado por todos los servicios de catálogo compatibles con OGC [58].
  - General Catalogue Interface Model: define los interfaces para la gestión de los catálogos, la búsqueda de metadatos, la gestión de sesiones y la mediación con metadatos que no pueden ser accedidos de forma directa. Estos interfaces se pueden implementar vía varios protocolos (actualmente se encuentran soportados CORBA, Z39.50 y HTTP).

  El perfil de aplicación del catálogo (CSW AP) define qué protocolo se debe emplear y qué interfaces del modelo de interfaz se deben implementar. De esta forma, el modelo queda extendido dependiendo de las necesidades del usuario y el dominio de aplicación. Actualmente existen dos perfiles de aplicación, uno de ellos basado en ebRIM [59] y otro basado en ISO19115/ISO19119 [60].

  Durante la búsqueda de metadatos, los catálogos acceden a sus conjuntos de metadatos, bien propios o externos, pues el acceso a otros CSWs también es posible. Esto permite una búsqueda distribuida. Los catálogos son un componente esencial de la infraestructura orientada a servicio de OGC y, en el contexto SWE, estos catálogos permiten la búsqueda espacial y temporal de medidas y sensores que midan un cierto fenómeno [61].

2.2.5. Aplicaciones de redes de sensores y de SWE

Aplicaciones de redes de sensores

Los últimos años, han supuesto una evolución considerable en la investigación de las redes de sensores debido a los avances en los sistemas informáticos y de comunicaciones. Hoy en día, es posible producir pequeños sensores con un coste muy bajo, equipados con procesadores de bajo consumo de energía que les da más autonomía, al mismo tiempo que se han diseñado y estandarizado diferentes protocolos inalámbricos que proporcionan escalabilidad e interoperabilidad, lo que permite el desarrollo de redes de sensores inalámbricas y redes ad-hoc para numerosas aplicaciones en múltiples escenarios de aplicación. Este avance ha posibilitado que se pueda implementar y llevar a cabo el concepto de Internet of Things o Web of Things [62].

Las aplicaciones de las redes de sensores son muy numerosas y están distribuidas en diferentes ámbitos como salud, militar, vigilancia del medio ambiente o sistemas de transporte. Las acciones que se llevan a cabo normalmente con estas redes de sensores implican tareas como la vigilancia, el seguimiento o control. Por lo general, las aplicaciones de redes de sensores consisten en el despliegue de nodos de comunicación inalámbrica en la región en la que está destinada a recopilar datos a través de sus componentes de observación conectados a los nodos destinados a la aplicación concreta para la que ha sido diseñada.

Las aplicaciones militares y de defensa fueron las primeras a las que se aplicaron las redes de sensores inalámbricos y han servido de base para el desarrollo de las redes de sensores de un propósito más general. Las redes de sensores inalámbricos son una parte integral de los sistemas de mando militar, control, comunicaciones, informática, inteligencia, vigilancia, reconocimiento y objetivos (C4ISRT, de sus siglas en inglés). En la Cold War SOund SUrveillance System (SOSUS) se desplegó un sistema de sensores acústicos en lugares estratégicos del fondo del océano para detectar y realizar un seguimiento de los submarinos soviéticos espías. SOSUS todavía se sigue usando por la Administración Nacional Oceanográfica y Atmosférica (NOAA) para el seguimiento de los acontecimientos en el océano como la actividad sísmica o seguimiento de animales [63]. La investigación moderna sobre redes de sensores comenzó alrededor de 1980, con el programa de Redes de Sensores Distribuidos (DSN, de sus siglas en inglés) en la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA, de sus siglas en inglés) [64].

Otro de los ámbitos de aplicación pioneros en la utilización de redes de sensores fue la monitorización medioambiental, donde se utilizan sensores intrínsecamente distribuidos en el espacio, como por ejemplo, la temperatura o la velocidad del viento. Algunos ejemplos son: Glacsweb, una tecnología desarrollada por la Universidad de Southampton que utiliza redes de sensores para monitorizar el comportamiento de los glaciares con el fin de comprender el cambio climático y su efecto sobre la elevación del nivel del mar [65]; o FloodNet que es un sistema de alerta para hacer predicción de inundaciones basadas en las lecturas de nivel de agua recogidos por un conjunto de sensores, con el fin de mejorar los tiempos de alerta y minimizar los daños por las inundaciones [66].

Uno de los campos más importante en los que se ha aplicado las redes de sensores es la salud. Gracias a algunas nuevas aplicaciones, es posible la monitorización de integrada de pacientes, nuevos diagnósticos, proporcionar interfaces para las personas con discapacidad o la gestión de fármacos en los hospitales. Por ejemplo, hay sistemas para la obtención de datos fisiológicos de forma no invasiva como pueden ser temperatura, peso o ECG [67] [68]. Esto puede ser muy útil en caso de personas mayores, los cuales tienen más probabilidad de sufrir algún problema grave. Gracias a la monitorización en tiempo real y al seguimiento puede llegar mejorar su nivel de vida [69] [70].

Aplicaciones de SWE

La utilización de implementaciones reales de SWE para descubrir y utilizar los datos de cualquier tipo de sensores, empieza a estar muy extendido debido a las facilidades que ofrece para la interoperabilidad. Existen numerosos estudios que acreditan sus ventajas y su utilidad [71] [72] [73], incluso propuestas para mejorar el estándar SOS, añadiéndole semántica [74].

Por ejemplo, uno de los proyectos que utiliza SWE es EO2HEAVEN (Earth Observation and ENVironmental modelling for the mitigation of HEAlth risks), cuyo objetivo es contribuir a una mejor comprensión de las complejas relaciones entre los cambios ambientales y su impacto en la salud humana, mediante la monitorización de los cambios inducidos por las actividades humanas, con énfasis en la atmósfera, ríos, lagos y la contaminación marina [75].

La NASA ha trabajado en algunos proyectos para mejorar la tecnología de sensores web en satélites los cuales utilizan el estándar SensorML para la geolocalización y otros fines. Algunos de estos proyectos están basados en el uso del conjunto de estándares SWE de OGC.

Otro ejemplo, es el proyecto GENESIS, el cual utiliza SWE para monitorizar la calidad en ríos, lagos y costas así como la calidad del aire, para poder mejorar el medio ambiente [76].

Existen otros muchos casos en los que se aplica SWE como son estudios oceanográficos donde es necesario almacenar multitud de datos marinos [77], para servicios de cloud computing como el Google Fusion Tables (GTF) [78], la gestión de datos e imágenes de satélites [79], almacenamiento de datos de UAVs [80], etc.

También se han desarrollado aplicaciones para procesar datos ya almacenados con SWE, como el proyecto INTAMAP el cual permite interpolar espacialmente puntos medidos de forma automática [81].

Un campo de estudio actual es smart cities, en el que se utilizan las tecnologías de la información para mejorar el rendimiento, bienestar y costes en una ciudad. En ese ámbito, el proyecto enviroCAR utiliza SWE para investigar el efecto de la conducción en el consumo de combustible, la producción de CO2 o el ruido de emisiones de los coches, con el fin de ser más eficiente y reducir el consumo de combustible.

Implementaciones del SOS

Entre las implementaciones del SOS, la más utilizada y la que hemos seleccionado para la implementación de la arquitectura de la tesis es la del 52north [53]. Este organismo fue fundado por el Instituto de Geoinformática de la Universidad de Münster, y tiene una amplia comunidad que mantiene y actualiza las distintas versiones del SOS. El SOS del 52north desarrolla toda la funcionalidad especificada en su estándar y dispone de una completa documentación. Permite una instalación sencilla gracias a un formulario web para distintas plataformas.

Existen otras implementaciones como son PySOS, desarrollado por la comunidad de investigación oceánica, y la única implementado en Python; MapServer SOS [82], de la popular web de aplicaciones espaciales abiertas; Deegree SOS [83], que forma parte de la versión de desarrollo del marco de servicios web OGC deegree conocido como deegree3; etc. Pero todas estas implementaciones ofrecen funcionalidades muy limitadas y hace tiempo que dejaron de ofrecer soporte.

2.2.6. Sensor web semántico

El término sensor web semántico fue acuñado por Berners-Lee [84] y lo describe como una extensión de *sensor web* al cual se le incorporan tecnologías de web semántica. Para ello, a los datos de los sensores se les añaden metadatos semánticos para incrementar la interoperabilidad, así como para proveer información esencial para facilitar el razonamiento y la clasificación. Estos metadatos semánticos pueden ser datos espaciales, temporales o temáticos.

Mientras que los lenguajes previstos por SWE de OGC proporcionan anotaciones para conceptos espaciales y temporales simples como coordenadas espaciales o instantes temporales, algunos conceptos más abstractos, como la región espacial, intervalo temporal, o cualquier entidad temática específica del dominio, se beneficiaría de una representación ontológica.

Esta funcionalidad se puede lograr haciendo más explícito el significado de los datos. Para este propósito, algunos lenguajes se han desarrollado para representar datos de una manera que las máquinas pueden leer y entender el contenido. Estos lenguajes son por ejemplo el Resource Description Framework (RDF) [85] o el más avanzado Web Ontology Language (OWL) [86], que permiten la especificación de ontologías que se utilizan para definir y restringir el significado de los términos y vocabularios.

La aplicación de tecnologías semánticas en sistemas de sensores, por una parte, introduce una capa de alto nivel para las arquitecturas y, por la otra, proporciona soporte para nuevos modelos de interacción (interoperabilidad semántica) y computación (semantic sensor web) [87]. Esta capa debería integrar las infraestructuras informativas web, mejorando, de forma sustancial, la capacidad de descubrir, catalogar, clasificar, compartir, manipular y analizar datos procedentes de los sensores (o informaciones asociadas). Al mismo tiempo, se asegura un alto nivel de interoperabilidad entre sistemas a través de interacciones semánticas. Para ello, proporciona un marco en el que se pueda mejorar el significado de las observaciones de los sensores, añadiendo anotaciones semánticas al estándar SWE. Estas anotaciones proporcionan descripciones más significativas y mejor acceso a los datos de los sensores, permitiendo conocer mejor la situación global del sistema monitorizado [88] [89].

Independientemente del concepto de semantic sensor web, las tecnologías semánticas, se aplican, actualmente, en arquitecturas avanzadas de redes de sensores como soporte a diferentes sistemas, con diferentes objetivos: soporte avanzado a la descripción y procesamiento de datos [90], gestión avanzada de datos [91], interoperabilidad avanzada

[92], representación dinámica de situaciones y estados de sistemas [93], modelos de lenguaje [94], análisis inteligente de datos y clasificación [95].

Cualquier entorno semántico es el resultado de la unión de dos aspectos básicos: modelo de interoperabilidad (Interoperabilidad Semántica) e Ingeniería del Conocimiento (semántico en este caso). Normalmente un esquema semántico se conoce como Ontología y se define como la formulación de un exhaustivo y riguroso esquema conceptual dentro de uno o varios dominios dados, con la finalidad de facilitar la comunicación y el intercambio de información entre diferentes sistemas y entidades. La ingeniería del conocimiento es un tema de investigación abierto y de gran interés en el seno de la comunidad científica internacional [96]. Una discusión exhaustiva al respecto se considera fuera de los objetivos fundamentales del documento.

2.3. Monitorización industrial

La industria posee cada vez procesos productivos más automatizados, complejos y en los que coexiste una gran diversidad de elementos: autómatas, ordenadores, accionamientos neumáticos, robots, etc. Además los sistemas de producción fuertemente centralizados y poco flexibles que se utilizaban hace varias décadas ya no son admisibles. Esto dio lugar hace unos años a la aparición de los sistemas de producción flexibles que proporcionan respuestas rápidas al mercado fuertemente cambiante en el que están inmersas las empresas. Estos sistemas de control "inteligentes" están basados en conceptos como: descentralización, autonomía, monitorización, cooperación y colaboración.

2.3.1. Supervisory Control and Data Acquisition (SCADA)

SCADA [97] viene de las siglas de "Supervisory Control And Data Adquisition", es decir: adquisición de datos y control de supervisión. Se trata de una aplicación software especialmente diseñada para funcionar sobre ordenadores en el control de producción, proporcionando comunicación con los dispositivos de campo (controladores autónomos, autómatas programables, etc.) y controlando el proceso de forma automática desde la pantalla del ordenador. Además, provee de toda la información que se genera en el proceso productivo a diversos usuarios, tanto del mismo nivel como de otros supervisores dentro de la empresa: control de calidad, supervisión, mantenimiento, etc.

En este tipo de sistemas usualmente existe un ordenador, que efectúa tareas de supervisión y gestión de alarmas, así como tratamiento de datos y control de procesos. La comunicación se realiza mediante buses especiales de carácter industrial o redes LAN. Todo esto se ejecuta normalmente en tiempo real, y están diseñados para dar al operador de planta la posibilidad de supervisar y controlar dichos procesos.

Los programas necesarios, y en su caso el hardware adicional que se necesite, se denomina en general sistema SCADA

Existen dos tipos de sistemas principalmente. Los no realimentados o de lazo abierto y los realimentados o de lazo cerrado. Los sistemas de control realimentados se llaman de lazo cerrado. El lazo cerrado funciona de tal manera que hace que el sistema se realimente, la salida vuelve al principio para que analice la diferencia y en una segunda opción ajuste más, así hasta que el error es próximo a cero. Cualquier concepto básico que tenga como naturaleza una cantidad controlada, como por ejemplo temperatura, velocidad, presión, caudal, fuerza, posición, etc. son parámetros de control de lazo cerrado. Los sistemas de lazo abierto no se comparan a la variable controlada con una entrada de referencia. Cada ajuste de entrada determina una posición de funcionamiento fijo en los elementos de control.

Componentes básicos de un sistema SCADA:

- PLC, controladores lógicos programables, adaptables a las diferentes situaciones requeridas, y más económicos que sensores específicos.
- RTU, Unidades terminales remotas, que se encargan de enlazar los sensores PLC con el sistema de supervisión, transforman señales analógicas en señales digitales.
- Sistema supervisor, que se establece en torno a un ordenador central que recolecta la información de los RTU y envía instrucciones a los elementos del sistema.
- Sistema HMI que facilita el acceso y la integración del factor de control humano en todo el sistema de control.
- Sistema de comunicaciones, que contempla todas las redes de datos y señalización que constituyen el esqueleto del sistema de cualquier sistema de control.

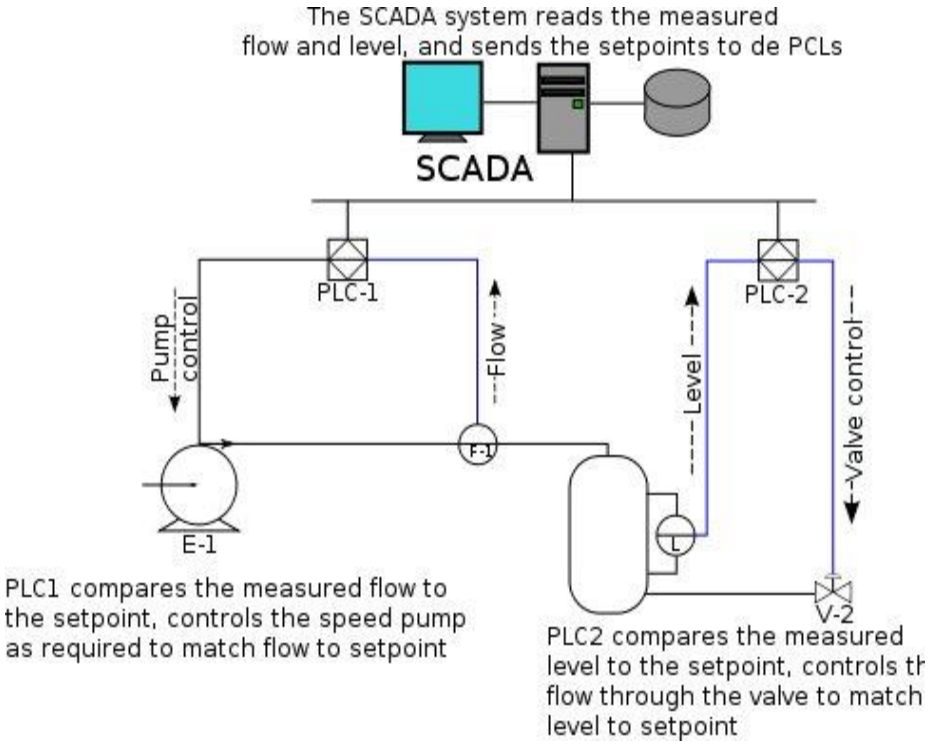

Figura 6. Esquema de un SCADA básico

Como vemos en la Figura 6 un típico sistema SCADA constaría de un control centralizado SCADA, que lee y controla los flujos y niveles de señal, y de diversos dispositivos de control PLC's que dialogan con el control SCADA, permitiendo por un lado la monitorización, y por otro, la intervención directa en los sistemas de producción. En el caso de ejemplo, se puede controlar y monitorizar tanto la apertura de una válvula, como por otro lado, el funcionamiento de una bomba hidráulica.

2.3.2. Network operations system (NOC)

En cuanto a los Network Operations Center (NOC) [98], son sistemas de gestión centralizados o distribuidos desde los que se ejerce control sobre una infraestructura basada en red. Este tipo de sistemas de control y monitorización se emplean ampliamente en redes de telecomunicación, empresas de distribución de energía y plantas de manufactura extensas. En el entorno industrial, el NOC se encarga de monitorizar los procesos productivos y gestionar los problemas que puedan aparecer en el ámbito de la prevención de riesgos laborales. Los NOCs tienen como misión principal la monitorización de redes y sistemas industriales que puedan requerir especial atención y respuesta inmediata ante diferentes eventos. Dos ejemplos serían la gestión de alertas en una fábrica y la gestión de eventos de seguridad en un entorno de comunicaciones como la red de un ISP. Los NOC más avanzados, mediante una adecuada descripción semántica de los problemas y los eventos, serían capaces de realizar una identificación, una correcta asignación de tareas a resolver.

Los centros de operaciones en los diferentes entornos tienden a resolver los problemas mediante técnicas jerárquicas, de forma que, si un evento no se resuelve en un periodo de tiempo adecuado pasa a ser resuelto por el siguiente nivel; y mediante la utilización de sistemas de apoyo a la decisión.

Las factorías están concebidas como elementos productivos muy activos, centrados en las tareas propias de su propia actividad, incorporando tecnologías avanzadas de fabricación y manipulación. Con el fin de controlar y analizar el correcto funcionamiento de los medios que intervienen, los técnicos gestores de las mismas, definen indicadores y ratios de medida, que deben monitorizar y controlar con una cierta frecuencia y que permiten tomar decisiones y analizar evoluciones y tendencias.

Sin embargo una planta productiva se compone de muchas entidades relacionadas entre sí, capaces de reaccionar ante señales propias y estímulos procedentes de otras áreas de la planta o del exterior. De esta forma, el conjunto de personas, maquinaria, materiales, procesos y otros elementos que componen la realidad de cada fábrica, son en la práctica pequeñas partes de un todo, con capacidad de actuación autónoma. Lo que nos indica que los sistemas de monitorización y control con un componente jerárquico pueden funcionar y actuar muy bien en un entorno de fabricación.

Estas entidades elementales, pueden disponer de capacidad para decidir, comunicarse con terceros, alterar los planes previstos o compararse con indicadores que midan sus prestaciones y tomar decisiones al respecto. Teniendo un conjunto de

sensores/actuadores, integrantes de un equipo, cada uno de los cuales está trabajando en base a satisfacer una serie de objetivos locales, pero estrechamente relacionado con el resto. Es por tanto relevante el despliegue de indicadores desde los objetivos de mejora para el conjunto de la fábrica, relacionados con parámetros de todo tipo, desde económicos, hasta de gestión de riesgos en cada una de las entidades existentes, de forma que aseguremos que el óptimo local, contribuye al óptimo global.

2.3.3. Manufacturing Execution System (MES).

Los Manufacturing Execution Systems (MES) [99] sirven como intermediarios entre un sistema de negocio, típicamente ERP, y el sistema de administración y control de planta, en una determinada factoría. Un MES ofrece servicios de programación y secuenciamiento de acciones, creación y auditoria de líneas de track and trace (seguimiento y localización), así como la distribución de instrucciones de trabajo para los trabajadores en planta.

Según la organización MESA (Manufacturing Enterprise Solutions Association) internacional, se puede definir MES de la siguiente Manera:

"Un Sistema de Ejecución de la Fabricación (MES), es un sistema dinámico de información que conduce de forma efectiva la ejecución de las operaciones de fabricación. A través de una información actual y precisa, el MES guía, pone en marcha e informa las actividades en planta a medida que ocurren los acontecimientos. El conjunto de funcionalidades MES gestiona operaciones de producción desde el momento del lanzamiento de la orden de fabricación hasta el punto de la entrega del producto acabado. El MES permite una atenta gestión y comunicación bidireccional de la información crítica sobre todas las actividades productivas, a través de la organización y de la cadena"

Características de MES:

- Permite gestionar y optimizar en tiempo real el entorno de fabricación de una empresa de una empresa.
- Es capaz de integrarse con el ERP para recibir las órdenes de fabricación generadas por éste.
- Ejecuta las órdenes recibidas. Interactua con el proceso productivo, a través de los sistemas de monitorización y control de planta.
- Capta y almacena la información que surge de la planta/proceso (datos, eventos, consumos, alarmas)
- Facilita al usuario final un interfaz que le permite analizar la información antes nombrada de forma personalizada.
- Retroalimenta al sistema transaccional (ERP) con información que previamente ha sido filtrada y verificada.

2.3.4. Controlador de Automatización programable (PAC)

Un PAC (del inglés Programmable Automation Controller) [100] es una tecnología industrial orientada al control automatizado, al diseño de prototipos y a la medición. El PAC se refiere al conjunto formado por un controlador (una CPU típicamente), módulos de entradas y salidas, y uno o múltiples buses de datos que lo interconectan todo.

Este controlador, combina eficientemente la fiabilidad de control de un autómata (controlador lógico programable o PLC) junto a la flexibilidad de monitorización y cálculo de un PC. A veces, incluso se le une la velocidad y personalización de la microelectrónica. Los PACs pueden utilizarse en el ámbito de investigación (prototipaje rápido de controladores o RCP), pero es sobre todo en el industrial, para control de máquinas y procesos, donde su uso está más extendido. Entre los distintos ámbitos de aplicación industrial se encuentran: múltiples lazos cerrados de control independientes, adquisición de datos de precisión, análisis matemático y memoria profunda, monitorización remota, visión artificial, control de movimiento y robótica, seguridad controlada, etc.

Los PACs se comunican usando los protocolos de red abiertos como TCP/IP, OPC (OLE for process control), SMTP, puerto serie (con Modbus por ejemplo), etc., y es compatible con los privados (CAN, Profibus, etc.).

Un ejemplo claro de utilización, es en un sistema de control de un proceso determinado. El elemento controlador es el sitio donde se toman todas las decisiones sobre las acciones a tomar. Se le puede considerar el "cerebro" del sistema. Debe tomar decisiones basadas en ciertas pautas o valores requeridos. Los valores establecidos son introducidos en el sistema por el hombre.

Los PACs surgen de la necesidad de combinar la fiabilidad y robustez de un PLC (Programmable Logic Controller) con la flexibilidad, prestaciones y funcionalidad de un PC industrial. La fiabilidad de un PLC está basada en su sólido diseño hardware y software, pero la rigidez de su arquitectura limita su capacidad de expansión, sus posibilidades de crecimiento y su integración dentro de redes corporativas. Por el contrario, los PCs industriales tienen una gran capacidad de proceso, disponen de variados periféricos, soportan múltiples protocolos de comunicaciones y presentan grandes posibilidades de ampliación y crecimiento, pero carecen de la extrema robustez de los PLCs. El PAC se desarrolla como respuesta a la necesidad de combinar las ventajas de ambos sistemas en un único equipo que permita gestionar E/S, comunicaciones, control de movimiento, etc., y ejercer de interfaz hombre máquina o HMI. Cada vez más plantas industriales utilizan controladores de automatización programables como respuesta a sus necesidades de control industrial.

2.4. Seguridad en entornos industriales

Los principales objetivos de la seguridad del sistema son prevenir la posibilidad de ocurrir accidentes en los sistemas de ingeniería y reducir sus consecuencias si se producen. El estándar de seguridad IEC 61508 [101] define la seguridad como, "la

ausencia de un riesgo inaceptable de lesiones físicas o daño a la salud de las personas, ya sea directa o indirectamente, como consecuencia de los daños a los bienes o al medio ambiente".

Bajo este nuevo prisma de fabricación competitiva sostenible, la seguridad y salud industrial, es por tanto, un factor estratégico de competitividad. Los tradicionales métodos de evaluación y gestión del riesgo quedan tremendamente limitados en este nuevo contexto. En la Fábrica del Futuro, el "riesgo tolerable" no es una opción. Esto hace necesario proponer un nuevo paradigma de seguridad y salud en la industria. Y junto con este nuevo modelo excelencia, es necesario desarrollar las tecnologías que faciliten la provisión continua, proactiva y personalizada de servicios de prevención.

2.4.1. NISTIR 7628

El Instituto Nacional de Estándares y Tecnología (NIST) apoya una de las funciones clave en el crecimiento de la red inteligente, que reúne a fabricantes, consumidores, proveedores de energía, y reguladores para desarrollar estándares interoperables.

El informe fue desarrollado como un documento de consenso por el Grupo de Trabajo de Seguridad Cibernética (CSWG) del Grupo de Interoperabilidad de redes inteligentes (SGIP), una asociación público-privada puesta en marcha por el NIST en enero de 2010. El CSWG ahora cuenta con más de 500 participantes del sector privado (incluidas las empresas de servicios públicos, proveedores, fabricantes y proveedores de servicios eléctricos), diversas organizaciones de estandarización, instituciones académicas, organismos reguladores y agencias federales. Está destinado principalmente a los individuos y organizaciones responsables de abordar la seguridad cibernética de los sistemas de redes inteligentes y los subsistemas constitutivos de hardware y componentes de software.

El documento de tres volúmenes, NISTIR 7628 [102], Directrices para la Seguridad Cibernética en el Smart-Grid, presenta un marco analítico que las organizaciones pueden utilizar para desarrollar estrategias efectivas de seguridad cibernética específicas para las características del smart grid, para mitigar los riesgos y vulnerabilidades. Las diversas organizaciones interesadas en el smart grid, pueden utilizar los métodos y la información complementaria que se presenta en el informe, como una guía para la evaluación de riesgos y, a continuación, la identificación y aplicación adecuada de requisitos de seguridad para mitigar dichos riesgos. El enfoque reconoce que la red eléctrica está cambiando de un sistema relativamente cerrado a un entorno complejo, altamente interconectado. Los requisitos de seguridad cibernética de cada organización, deben evolucionar a medida que avanza la tecnología, ya que las amenazas a la seguridad de la red inevitablemente se multiplican y diversifican. Debido a su creciente importancia, se está empezando a estudiar y aplicar en redes inteligentes [103] [104].

El principal objetivo, es la elaboración de estrategias eficaces para proteger las redes informáticas y de comunicaciones que serán fundamentales para el rendimiento y la disponibilidad de la infraestructura de energía eléctrica prevista, y para proteger la

privacidad de los datos personales de las redes inteligentes. Si bien la integración de tecnologías de la información es esencial para la construcción del smart grid y aprovechar sus beneficios, las mismas tecnologías de red añaden complejidad y también introducen nuevas interdependencias y vulnerabilidades. Los enfoques para asegurar estas tecnologías y para proteger la privacidad deben ser diseñados e implementados en los primeros instantes de la transición a las redes inteligentes.

Volumen 1

El primer volumen del informe describe el enfoque analítico, incluyendo el proceso de evaluación de riesgos, que utiliza el CSWG para identificar los requisitos de seguridad de alto nivel. También presenta una arquitectura de alto nivel, seguido de un modelo de referencia de interfaz lógica, utilizada para identificar y definir las categorías de interfaces dentro y fuera de los siete dominios del smart grig (ver Figura 7). El primer volumen concluye con un análisis sobre técnicas criptográficas y de gestión de claves en todo el ámbito de los sistemas de redes inteligentes y dispositivos.

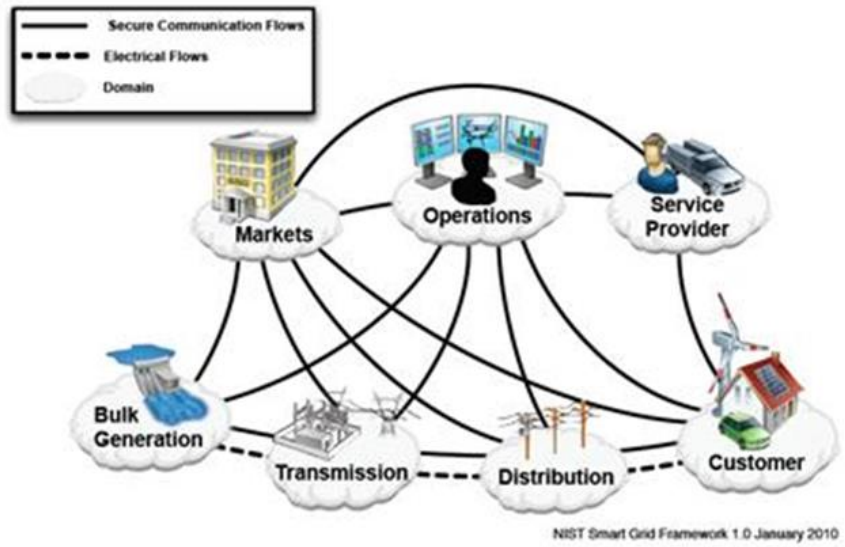

Figura 7. Dominios del Smart-Grid [102]

Volumen 2

El segundo volumen se centra en aspectos de privacidad en las viviendas de los usuarios. Discute y aporta datos sobre temas tales como la evolución de las tecnologías de redes inteligentes y nuevos tipos de información relacionados con las personas, grupos de personas, y su comportamiento dentro de sus casas y vehículos eléctricos. También, si estos nuevos tipos de información pueden contener riesgos y desafíos de privacidad que no han sido legalmente aprobados todavía.

Además, el segundo volumen ofrece recomendaciones basadas en los principios de privacidad ampliamente aceptados, para las entidades que participan en el smart grid. También propone como educar a los consumidores y otras personas acerca de los

riesgos de la privacidad en las redes inteligentes y lo que pueden hacer para mitigar estos riesgos.

Volumen 3

El tercer volumen es una recopilación de análisis de apoyo y referencias utilizadas para desarrollar los requisitos de seguridad de alto nivel y otras herramientas y recursos presentados en los dos primeros volúmenes.

En otro capítulo, se condensan temas de investigación y desarrollo que pretenden presentar los grandes cambios que han tenido lugar en la seguridad informática que permiten mayores niveles de fiabilidad y seguridad de la red inteligente, ya que cada vez son más avanzados tecnológicamente. Además, el tercer volumen ofrece una visión general del proceso que el CSWG ha desarrollado para evaluar si las normas, identificadas a través del proceso del NIST en apoyo de la interoperabilidad de redes inteligentes, cumplen los requisitos de seguridad de alto nivel incluidos en el informe.

2.4.2. ISO 27000

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

El origen fue en 1995, cuando surgió la norma BS 7799 de BSI (British Standards Institution) [105] con el fin de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de la información. Desde entonces ha sufrido algunas revisiones para adecuarse a las normas ISO.

El ISO/IEC 27000 es un conjunto de estándares [106] desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044, con 27799 finalizando la serie formalmente en estos momentos.

Partiendo del fundamento de que el estándar ISO/IEC 27001 indica qué requisitos deben conformar un SGSI, pero no cómo cumplirlos, algunas de las normas que conforman la serie 27000 van orientadas precisamente a documentar mejores prácticas en aspectos o incluso cláusulas concretas de la norma ISO/IEC 27001, de modo que se evite repetir estándares con el sustancial ahorro de tiempo en la implantación.

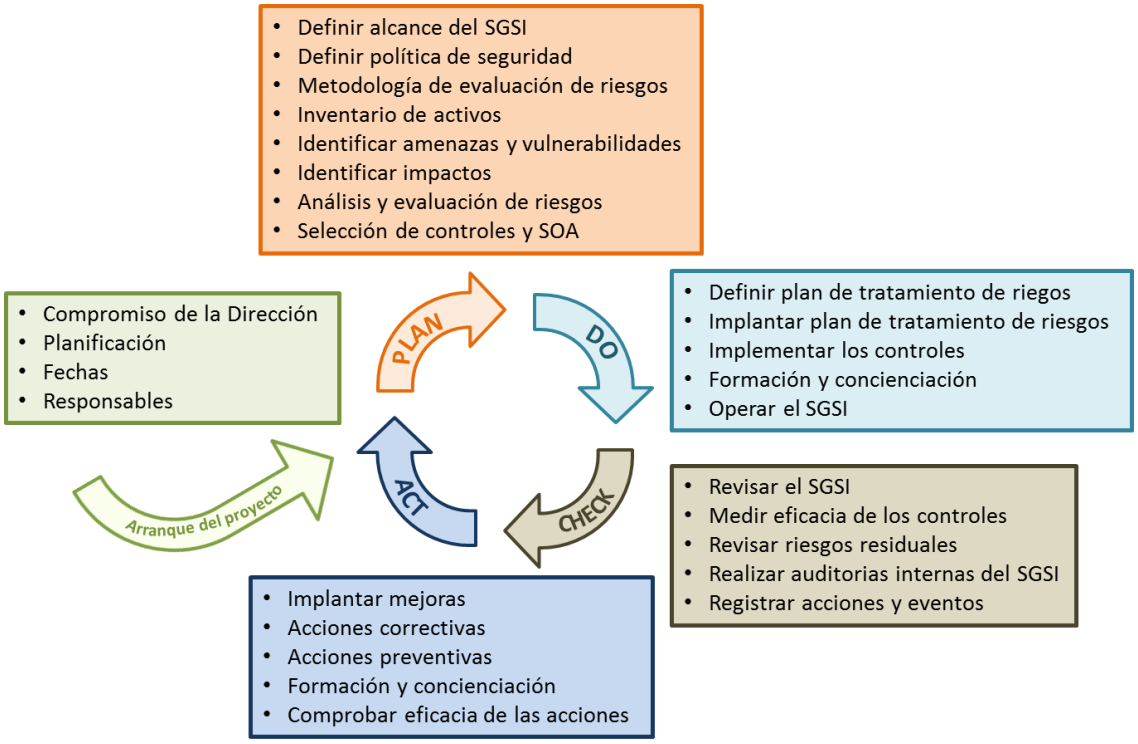

Figura 8. Estructura de la norma ISO 27000

Las principales aportaciones del uso del estándar ISO/IEC 27000 son:

- Establecimiento de una metodología de gestión de la seguridad, clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001…).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.

- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos, en vez de en la compra sistemática de productos y tecnologías.

Algunas de las principales normas que contiene la serie 27000 son las siguientes:

La norma ISO/IEC 27000 proporciona una visión general de las normas que componen la serie 27000, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción del ciclo Plan-Do-Check-Act y términos y definiciones que se emplean en toda la serie 27000.

ISO/IEC 27001 es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó obsoleta) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

ISO/IEC 27002 es una guía de buenas prácticas, que describe los objetivos de control y mecanismos de control recomendables en cuanto a seguridad de la información. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. El estándar establece las directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información.

ISO/IEC 27003 es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo a la ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

ISO/IEC 27004 es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001. Su objetivo es ayudar a una organización a establecer la efectividad de su implementación SGSI.

2.4.3. Common Criteria

El Common Criteria for Information Technology Security Evaluation (abreviado como Common Criteria o CC) es un estándar internacional (ISO/IEC 15408) para la certificación de la seguridad informática. [107]

El CC es un marco en el que los usuarios de sistemas informáticos pueden especificar sus requisitos funcionales de seguridad (SFR) y sus requisitos de garantía de seguridad (SAR) mediante el uso de perfiles de protección (PP), los proveedores pueden implementar y hacer afirmaciones acerca de los atributos de seguridad de sus productos y los laboratorios de ensayo pueden evaluar los productos para determinar si, efectivamente, cumplen las especificaciones. Es decir, Common Criteria ofrece la garantía de que el proceso de especificación, implementación y evaluación de un producto de seguridad informática se ha realizado de una manera rigurosa, estándar y repetible en un nivel que sea compatible con el entorno de destino para su uso.

Los principales objetivos que se quieren lograr mediante la certificación son:

- Garantizar que las evaluaciones de productos de Tecnología de la Información (TI) y los perfiles de protección se realicen con un alto nivel de rigor, lo que contribuirá de manera significativa a la confianza en la seguridad de los productos y perfiles.
- Mejorar la disponibilidad de los productos de TI de seguridad y perfiles de protección evaluados, facilitando a los usuarios la información.
- Eliminar la duplicación de las evaluaciones de productos de TI y perfiles de protección.
- Mejorar continuamente la eficiencia y el coste-efectividad del proceso de evaluación y certificación/validación para productos de TI y perfiles de protección.

El estándar está dividido en tres partes. La primera parte define una estructura y un lenguaje para describir los requisitos de seguridad de un producto TI. La segunda parte es un catálogo de SFRs, los cuales definen que hace el producto, es decir, sus funciones de seguridad (identificación, autenticación, etc.). La tercera parte es un catálogo de SARs que permite otorgar confianza en que el producto cumple las funciones de seguridad que declara de una manera correcta (manuales, soporte al ciclo de vida, etc.) Por último, existe una cuarta parte o CEM que especifica la metodología de evaluación a seguir por los evaluadores.

Los niveles de garantía que se pueden certificar son los siguientes:

- Funcionalmente probado.
- Estructuralmente probado.
- Metódicamente probado y comprobado.
- Metódicamente diseñado, probado y comprobado
- Semiformalmente diseñado y probado.
- Diseño verificado semiformalmente y probado.

Desde hace tiempo se aplica el CC en muchos proyectos [108] [109], para poder definir un gran número de requisitos de seguridad en el sistema y en el desarrollo. La aplicación de CC a los contadores inteligentes aporta numerosos beneficios, como se

muestra en [110], por ese motivo se debería aplicar en todo el smart grid. Por lo tanto, el sistema desarrollado debe cumplir con las normas de la CC con el fin de proporcionar un nivel de confianza de la red inteligente. Esto puede mejorar la calidad, la seguridad y la privacidad y reducir el costo del sistema.

2.4.4. Security Assurance

Se considera Security Assurance (SA) un proceso para mantener la confidencialidad, la integridad y la disponibilidad de la información y los servicios que ofrecen los sistemas de información basados en TIC, siguiendo la definición del CC.

La investigación sobre SA se centra principalmente en tres objetivos: (i) las iniciativas en desarrollo de software, (ii) el desarrollo de métricas y (iii) la evaluación de los sistemas o productos.

El primer objetivo busca lograr sistemas más seguros mediante el establecimiento de requisitos de seguridad donde los riesgos se evalúan en el desarrollo de software. En este caso, se requiere una forma rigurosa y eficaz para hacer frente a la seguridad en todo el proceso de desarrollo del sistema, de modo que el producto final pueda ser considerado seguro. [111] [112]

El segundo objetivo está relacionado con las métricas. De forma similar al NISTIR 7628, hay algunos estudios que proporcionan una guía que explica cómo desarrollar métricas que puedan mejorar los mecanismos de seguridad, las políticas y las implementaciones [113] [114]. En [115], los autores definen una taxonomía de los sistemas de red y sugieren un marco lineal para obtener un único valor que representa el nivel de seguridad del sistema de información. El uso de un valor único simple y agregado de security assurance permite ver rápidamente el estado de seguridad del sistema, similar a un semáforo. El sistema propuesto en este trabajo seguirá este esquema, aunque mejorado, proporcionando también un medio para analizar rápidamente el proceso mediante el cual el sistema ha llegado al valor de SA actual.

Una vez que se han definido las métricas, el tercer objetivo es determinar el nivel de garantía de los productos y sistemas basados en estándares como Common Criteria. Para esto se pueden realizar pruebas de penetración para evaluar la seguridad con ataques simulados [116]. Otro ejemplo es el proyecto BUGYO Beyond [117] [118], que emplea una metodología pionera y una herramienta para la evaluación continua del SA. Desafortunadamente BUGYO Beyond sólo considera la corrección sin tener en cuenta la eficacia, que es otro parámetro clave en el SA.

Existen algunas aplicaciones que utilizan el SA como parámetro para evaluar la seguridad del sistema, aunque ninguno en el campo de las infraestructuras críticas. Por ejemplo, un marco para la defensa activa del SA basado en una plataforma fiable para el comercio electrónico [119] o de un sistema de reconocimiento facial utilizando la información de las personas [120].

El concepto de SA se puede enlazar directamente con SWE, desde el mismo momento que en entornos de cyberseguridad existen sensores físicos y lógicos que monitorizan el estado de la seguridad de un entorno. SWE nos permite integrar todos los sensores en un mismo marco, y al mismo tiempo acceder a ellos de forma transparente. Al basarse el SA en la toma de medidas por parte de los sensores desplegados en el entorno lógico a analizar. El almacenamiento y gestión de las medidas en los servicios de SWE es más que adecuado [121].

2.4.5. Sistemas de detección de vulnerabilidades

La principal prioridad en un sistema de monitorización y control, debe ser la detección de las vulnerabilidades y eventos relativos a la seguridad. Para que sea lo más efectivo posible, se considera como primordial requerimientos de tiempo real y alta velocidad de detección. Una vez detectados los problemas de seguridad habrá que establecer de forma inmediata mecanismos de actuación, para evitar que se produzcan ataques sobre el sistema así como también posibilitar adaptarse al dinamismo del entorno. Se habla entonces de sistemas de prevención, en referencia a la combinación de técnicas de detección y actuación.

Los sistemas de detección de vulnerabilidades, están pensados para encontrar las debilidades de los activos de una organización que puedan ser explotadas por un atacante o una amenaza. El sistema debe ser capaz de detectar estas debilidades en el momento en que se producen y actuar en consecuencia, para solventar el problema y eliminar el riesgo.

Dentro de los sistemas de detección de vulnerabilidades será posible distinguir varios tipos o categorías, dependiendo de su funcionalidad. Por un lado, tendremos detectores pasivos de vulnerabilidades (IDS, Intrusion Detection System [122]), que analizarán el tráfico de red en busca de comportamientos sospechosos y, ante una incidencia, reportarán avisos o alertas al administrador de la red para que sea éste quien decida cómo actuar y proceda a bloquear el posible ataque. Por otro lado, estarán los detectores activos de intrusión (IPS, Intrusion Prevention System [123]), los cuales serán capaces de tomar decisiones y emprender acciones de forma autónoma al detectar las vulnerabilidades en la red, bloqueando los ataques ellos mismos.

Desde el punto de vista de una detección de alta velocidad y en tiempo real, las herramientas que resultarán más interesantes son las de detección activa, y más concretamente los sistemas de prevención de intrusión y los firewalls.

Tanto los firewalls, como los sistemas de prevención de intrusión, son herramientas destinadas a crear un perímetro de seguridad en la red de cualquier organización. Además de proteger de las amenazas externas provenientes de la red a la que estamos conectados, también protegen de las amenazas internas, por ejemplo, evitando el envío de información confidencial o la saturación de los recursos de comunicaciones.

Sistemas de prevención de intrusión (IPS)

Los sistemas IPS son herramientas que llevan a cabo un análisis en tiempo real de las conexiones y los protocolos para determinar si se está produciendo o se va a producir un incidente relativo a la seguridad. Los IPS se utilizan para detectar y prevenir accesos no autorizados a un equipo o a una red, ya que existen IPS de equipo y de red. Ambos monitorizan el tráfico para determinar y prevenir comportamientos sospechosos. Con frecuencia suelen ir integrados con firewalls.

A diferencia de los sistemas de detección de intrusiones o IDS que monitorizan el tráfico de red y envían alertas sobre actividades sospechosas, los IPS están diseñados para bloquear los ataques, examinando detenidamente todos los paquetes entrantes y tomando en consecuencia decisiones instantáneas para permitir o impedir el acceso.

El objetivo de los IPS es proteger de los ataques de red examinando los paquetes y bloqueando el tráfico malicioso. Para ello siguen los siguientes pasos:

- Cada paquete es clasificado en función de la cabecera y de la información de flujo asociada.
- En función de la clasificación del paquete, se aplican las políticas asociadas a su información de flujo.
- Todas las políticas relevantes se aplican en paralelo y, si un paquete se identifica como sospechoso, es etiquetado como tal.
- Entonces se descarta y se actualiza su información de estado de flujo con el fin de descartar el resto de dicho flujo.

El problema es que un IPS por sí solo no posee las funcionalidades necesarias para gestionar el control, la protección y el rendimiento requerido por las organizaciones en la actualidad. Esto es debido a que el panorama de las aplicaciones y las amenazas está cambiando, y así lo deben hacer los IPS para adaptarse a la nueva situación. Por ejemplo, las aplicaciones actuales, tanto las personales como las de negocio, utilizan técnicas evasivas de las medidas de seguridad tradicionales (como utilización aleatoria de puertos, uso de puertos no estándar, tunelizado por medio de otros servicios más comunes, ocultación dentro de tráfico cifrado, etc.) con el fin de que cualquier usuario sea capaz de usarlas independientemente del tipo de red en la que se encuentre, y por tanto de la seguridad de esa red. Otra tendencia cada vez más popular, es el traslado de los servicios a hosting externo y servicios en la nube, por lo que se estima que gran parte del tráfico de una organización son de tipo HTTP y HTTPS. Con lo cual el filtrado por número de puerto está perdiendo cada vez más efectividad.

Firewall tradicional

Los firewall o cortafuegos, en su concepto inicial o tradicional, son productos destinados a proteger los sistemas y dispositivos conectados a una red. Estas herramientas permiten establecer un perímetro de seguridad y garantizar comunicaciones seguras, evitando accesos no autorizados y ataques provenientes de redes externas y de Internet.

Para ello, estos productos imponen una política de seguridad sobre las comunicaciones hacia y desde la red privada e Internet, rastreando y controlando las comunicaciones y bloqueando el tráfico sospechoso. El firewall determina cuál de los servicios de red pueden ser accedidos por los que están fuera, es decir, quién puede entrar para utilizar los recursos de red pertenecientes a la organización.

Para que un firewall sea efectivo, todo tráfico de información proveniente del exterior deberá pasar a través del mismo, donde podrá ser inspeccionado. El firewall será el único que pueda autorizar el paso del tráfico. Desafortunadamente, este sistema no puede ofrecer protección una vez que el atacante lo traspasa y accede a la red interna.

Pero los firewall tradicionales suponen algunos problemas, como son: el filtrado de protocolos dinámicos y la escasa consciencia o visibilidad a nivel de aplicación no son efectivas en la gestión de las amenazas emergentes; el uso separado e independiente de los cortafuegos y la tecnología de prevención de intrusión resulta en un mayor coste operacional y no introduce un aumento en la seguridad; ataques de tipo botnets resultan invisibles para este tipo de firewalls; cada vez más tráfico utiliza un número menor de puertos (típicamente HTTP y HTTPS) y a través de menos protocolos, por lo que el filtrado en base a información de protocolo/puerto se ha vuelto menos relevante y eficiente.

Como se deduce de la problemática expuesta, tanto los IPS como los firewall tradicionales requieren un avance tecnológico para ser capaces de adaptarse a los nuevos requerimientos de seguridad. El futuro parece orientarse hacia los Firewalls de Nueva Generación, que se basan en las bondades que las tecnologías previamente expuestas ya ofrecen (detectar y bloquear el tráfico sospechoso) y las extenderá para hacer frente a las nuevas amenazas que están surgiendo, proveyendo control sobre las aplicaciones y su contenido, descifrando el tráfico SSL y descomprimiendo el contenido de los archivos.

Los firewall de nueva generación permiten que las empresas puedan ver y controlar las aplicaciones, los usuarios, y el contenido, no sólo los puertos, direcciones IP, y los paquetes. Para ello, utilizan tecnologías de identificación a nivel de aplicación, identificación a nivel de usuario e identificación a nivel de contenido. Estas tecnologías de identificación permiten que las empresas puedan crear políticas de seguridad relevantes a su negocio, permitiendo de manera segura a las organizaciones adoptar nuevas aplicaciones, en lugar del tradicional "todo o nada" que ofrece el bloqueo de puertos del firewall tradicional.

2.4.6. Modelo de Seguridad para Redes de Sensores

Las redes de sensores están compuestas por un conjunto grande de dispositivos electrónicos pequeños y de bajo coste. Estos dispositivos tienen por misión la obtención de datos del entorno para ser transmitidos hasta una estación base que los hará accesibles desde el exterior de la red.

El bajo coste de un sensor provoca que éste tenga una capacidad de cómputo y de comunicación muy restringida y una cantidad de energía limitada que no debe ser malgastada. Por este motivo, si se desea añadir algún tipo de mecanismo de seguridad a la red no puede basarse en las técnicas clásicas (pensadas para máquinas más potentes). Además, la naturaleza "móvil" de los sensores junto a las capacidades de un fácil y rápido despliegue de los mismos hace que las redes de sensores sean más vulnerables a diversos ataques.

La mejora tanto en el hardware como en el software de los sensores, puede solucionar parte de los problemas de seguridad a los que estos sensores (y en consecuencia la red subyacente) tienen que hacer frente. Pero hay que tener en cuenta que para que exista una completa solución de seguridad en las redes de sensores, es necesario el despliegue de las contramedidas pertinentes así como un correcto uso de claves de sesión unido a unos mecanismos de "routing" seguros junto con técnicas de cifrado no excesivamente complejas (para no introducir tráfico en exceso).

Las redes de sensores son susceptibles de diferentes tipos de ataque, a modo de resumen:

- Nodo comprometido.
- Destrucción de un nodo.
- Escucha o modificación de los datos.
- Acceso o alteración de la red.
- Denegación de servicio (DoS).

Para protegerse de estos y de más ataques, se han desarrollado diferentes técnicas y estrategias que se pueden aplicar a las redes de sensores.

INSENS (Intrusion-Tolerant Routing in Wireless Sensor Networks)

INSENS [124] es una propuesta que pretende solucionar el problema de routing seguro en redes de sensores. El problema a evitar consiste en la alteración por parte de un atacante de las tablas de enrutado de los datos. De esta forma, un atacante que haya capturado un sensor puede obligar a que todos los datos atraviesen este sensor. La aproximación presentada no pretende detectar intrusiones sino tolerarlas mediante unos mecanismos que permitan evitar el efecto de los nodos comprometidos.

El resultado de aplicar este protocolo es que un nodo bajo el control de un atacante en la red solo podrá capturar un conjunto reducido de nodos, mientras que los nodos restantes podrán seguir con su funcionamiento normal.

La primera medida consiste en no permitir un broadcast iniciado por un sensor. Con esta medida se pretende evitar un posible ataque de denegación de servicio por parte de los nodos comprometidos. Para autenticar la estación base (elemento que sí está autorizado a hacer un broadcast) se utiliza una cadena de hash generada por la misma, INSENS especifica la función hash a emplear, para adecuarse al pequeño tamaño de los paquetes transmitidos por los sensores.

Las tablas de routing son calculadas por la estación base a partir de la información proporcionada por los nodos. Esta información debe estar correctamente autenticada. Para ello, cada nodo comparte con la estación base una clave secreta simétrica con la que genera un MAC que autentica el mensaje. De esta forma, se evita que un nodo malicioso pueda proporcionar información falsa sobre la topología de red. Únicamente puede esconder a la estación base la existencia de sus nodos hijos eliminando todos los paquetes que deban circular a través suyo.

Finalmente, la estación base repartirá las tablas de routing calculadas para cada nodo. Cada uno de ellos recibirá dos rutas independientes (si existen). Dada la mayor capacidad de cómputo de la estación base y el conocimiento de la información correcta de cómo mínimo una parte de la red, ésta podrá calcular las rutas que se adapten mejor al entorno. Una de las rutas es calculada usando el algoritmo de Dijkstra (siendo por lo tanto la ruta más corta posible). La segunda se calcula tratando que no pase ni por los nodos de la primera ruta ni por sus vecinos a uno o a dos saltos. Con esta medida, se pretende proporcionar a cada nodo dos caminos lo más independientes posibles para que la información pueda esquivar nodos que hayan sido capturados y así pueda llegar a su destinatario.

SPINS – Protocolos de Seguridad en Redes de Sensores

Los datos que produce un sensor pueden ser sensibles y necesitar de un mecanismo que los proteja. Existen técnicas ampliamente conocidas y usadas para la protección de los datos que circulan por una red abierta. No obstante, estas técnicas se deben adaptar a las peculiares características de las redes de sensores, en las que en primer lugar no suele emplearse el protocolo IP.

SPINS (Security Protocols for Sensor Networks) [125] es una solución propuesta por la UC Berkeley, desarrolladora de los nodos sensores que actualmente comercializa la empresa Crossbow. SPINS es una filosofía de seguridad compuesta por bloques, concretamente dos bloques o protocolos de seguridad que protegen los datos que se comunican. En primer lugar, μTESLA [126] (la version reducida para su ejecución en sensores del Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol) es un protocolo que proporciona un broadcast autenticado. En segundo lugar, SNEP [127]

(Sensor Network Encryption Protocol) proporciona confidencialidad, autenticación de las dos partes y garantiza la validez de los datos.

Para el funcionamiento de los protocolos es necesario que haya una previa relación de confianza. Para empezar, cada nodo compartirá una clave con la estación base, así que todos los nodos deben confiar en ella. Asimismo, es necesario que cada nodo confíe en sí mismo y en particular en su reloj local. Por contrario, nadie confía en ningún sensor ya que cualquiera de ellos puede ser comprometido por un atacante.

La falta de memoria de los sensores se traduce en la necesidad de usar criptografía simétrica debido a su mayor nivel de seguridad a igual tamaño de clave. Asimismo, la poca memoria destinada al programa exige también el uso de primitivas criptográficas simples (autenticación con hash, etc...).

SNEP es el primero de los bloques que componen la arquitectura SPINS, es un protocolo que pretende proporcionar un nivel de seguridad a los datos que viajan por la red. El objetivo debe ser conseguido sin un incremento sustancial en el tamaño de los mensajes. SNEP parte de la base que las dos partes que se quieren comunicar comparten una clave principal y dos contadores (uno para cada sentido de la comunicación). De la clave compartida, se derivan mediante una función pseudoaleatoria, dos claves para proporcionar confidencialidad en cada sentido de la comunicación y dos claves más para proporcionar autenticación de cada una de las partes. Cada uno de los contadores se incrementará cada vez que se transmita un paquete.

El servicio de confidencialidad se consigue mediante el uso de criptografía simétrica. Para dificultar el criptoanálisis, el cifrado es función, además de la clave, del contador compartido para este sentido de la comunicación. De esta forma se consigue que aunque el mensaje enviado sea el mismo, el criptograma sea distinto. La autenticación del mensaje se consigue mediante el uso de MAC. El MAC es función, además de la clave de autenticación, del contador. El receptor no es autenticado explícitamente por el emisor, no obstante, solo podrá leer el mensaje quien disponga de la clave compartida.

Finalmente, SNEP ofrece un mecanismo mediante el cual se pretende asegurar la validez de los datos. Para ello, junto con la petición de información, la estación base debe incluir un número aleatorio. En el MAC de la respuesta el sensor interrogado incorporará este número aleatorio. De esta forma, la estación base sabe que el mensaje de respuesta ha sido generado posteriormente a su pregunta.

Por otro lado, μTESLA es un protocolo que surge inspirado en el protocolo de broadcast autenticado TESLA. Con él, se pretende que la estación base pueda mandar mensajes autenticados a todos los nodos.

TESLA ofrece la funcionalidad deseada pero necesita unos recursos que no se pueden garantizar en una red de sensores: la autenticación se lleva a cabo mediante firmas digitales, añade un overhead de 24 bytes por paquete y requiere del almacenaje por parte de los nodos de una cadena de claves unidireccional de tamaño demasiado grande.

Para evitar el coste derivado del uso de criptografía asimétrica, μTESLA autentica sus paquetes mediante un MAC generado a partir de una cadena de claves. Cada intervalo de tiempo, la estación base usará un elemento distinto de la cadena de claves.

En la creación de la red, se genera la cadena de claves y se reparte a todos los sensores el último valor. Si más adelante se añaden nuevos nodos o se desea generar una nueva cadena de claves, la estación base emitirá en claro la última clave de la nueva cadena debidamente autenticada (mediante, por ejemplo, una clave compartida en el caso de un nuevo nodo o usando las claves de la cadena antigua en el caso de renovación de cadenas).

Cuando la estación base desea enviar un paquete, mira en qué intervalo de tiempo está y usa la clave correspondiente a ese intervalo de tiempo. Dicha clave se mandará a los nodos en claro unos intervalos de tiempo más adelante. El nodo recibe el paquete pero no dispone de la clave para verificar su autenticidad. Esta clave le llegará a posteriori. Una vez recibida la clave, el nodo puede verificar su autenticidad a partir de la clave inicial (o de claves anteriores) de que dispone.

Un atacante puede escuchar la transmisión de las claves de autenticación. Con ellas, podría generar paquetes broadcast que fueran interpretados como auténticos por los nodos. Para evitar este suceso la clave se manda unos intervalos de tiempo después de mandar el paquete, con la intención que cuando se descubra la clave ya haya pasado su tiempo de validez para generar MACs.

SPINS es una de las primeras propuestas en cuanto a la gestión de seguridad en redes de sensores, principalmente para la implementación de enrutamiento seguro, pero sigue teniendo validez en la actualidad.

2.5. Sistemas de transporte inteligente

Un Sistema de Transporte Inteligente es una tecnología en la que se aplica Internet of Things en ámbito del tráfico de vehículos. Tiene como objetivo, proporcionar servicios innovadores relacionados con los diferentes modos de transporte y gestión del tráfico, y permite que los usuarios estén mejor informados, de modo que sea más seguro y coordinado el uso de las redes de transporte. En comparación con el sistema de transporte tradicional, la característica más significativa del ITS es la combinación de la inteligencia artificial y el sistema de transporte. Un ITS abarca una amplia gama de información de comunicaciones inalámbricas y fijas, el procesado de dicha información, algoritmos de control, electrónica y otras tecnologías. Cuando está operativa la infraestructura del sistema de transporte, incluidos los vehículos, esta tecnología es capaz de reducir la congestión, mejorar la seguridad y aumentar la productividad.

El desarrollo de un ITS se puede dividir en dos etapas. La característica principal de la primera etapa, es la adquisición de información sobre el estado del tráfico y el procesado inteligente. En la segunda etapa, se desarrollan tecnologías para mejorar la seguridad activa del vehículo como prevención de colisiones o vehículos inteligentes.

2.5.1. Monitorización del estado del tráfico mediante técnicas de visión por computador

La visión por computador es una disciplina que estudia el procesamiento y análisis de datos obtenidos a través de imágenes digitales. Actualmente, su aplicación al análisis de la monitorización del tráfico, se encuentra en pleno auge. Esto es debido a la posibilidad de acceso a datos procedentes de cámaras o de sensores de vigilancia.

La calidad de la información obtenida procedente de estos sistemas de vigilancia, depende en gran medida del entorno analizado. Para su análisis se consideran dos tipos de entornos: entornos urbanos y carreteras.

Los entornos urbanos, presentan dificultades asociadas a la alta variabilidad de las condiciones a las que se opera. El número de incidentes o infracciones suele ser elevado, el tráfico no es homogéneo, hay gran número de congestiones y de oclusiones entre vehículos y la presencia de peatones o bicicletas. En el estudio propuesto por Enzweiler y Gavrila se emplea la visión por computación y el reconocimiento de patrones en la detección de peatones [128]. En Londres, se ha lanzado un sistema de detección de congestión del tráfico urbano, con el fin de aliviar el número de usuarios en las carreteras, disminuir niveles de contaminación y gastos de combustible [129].

Las condiciones de operación en carreteras presentan menor variabilidad. Su principal característica es la ausencia de peatones y de bicicletas que puedan dificultar la detección. Además, el tráfico es homogéneo, y cuenta con la ventaja del ángulo de la cámara. Algunas de las aplicaciones desarrolladas en este entorno se emplean para contar y clasificar vehículos [130], otras para la detección de accidentes o infracciones en carreteras [131], así como la vigilancia de vehículos en túneles [130].

Como consecuencia de esta diversidad, la detección y clasificación de elementos en entornos urbanos, alcanza menores rendimientos que los obtenidos en carretera [132] [133]. Un ejemplo es el estudio de Messelodi [134] desarrollado en entorno urbano y el de Huang y Liao [135] desarrollado en carretera. En el primero, el sistema realiza la cuenta y clasificación de 7 tipos de vehículos en entorno urbano. Este sistema no se ve afectado por la lluvia. Sin embargo, la identificación de vehículos es imposible en situaciones de iluminación nocturna. El rendimiento logrado fue del 82.8%. Por otro lado, el sistema desarrollado por Huang y Liao, que clasifica también los vehículos en 7 tipos, presenta errores cuando se dan dos condiciones: que hay oclusiones entre vehículos y que la velocidad de ambos es similar. El rendimiento alcanzado, en este caso, fue del 91%.

En los sistemas de análisis de tráfico se consideran 3 etapas. Una etapa de segmentación donde se estiman los píxeles del primer plano y se agrupan en regiones. A continuación, la etapa de clasificación recoge la información de la estimación de las diferentes regiones y le asigna una de ellas. La última etapa es la de tracking o seguimiento, cuya finalidad es el seguimiento del objeto a lo largo de las secuencias de video.

La etapa de segmentación consiste en la división de una imagen en regiones para facilitar su posterior procesamiento. En primer lugar, se toma como modelo de referencia las escenas del primer plano de una secuencia de video. Posteriormente, este modelo de referencia se compara con los cuadros de imagen consecutivos y se identifican las diferencias.

La etapa de clasificación (que se desarrollará con más detalle en la siguiente sección) consiste en asignar un elemento de la imagen a una clase de vehículo (p.ej. coche, camión, motocicleta) que ha sido previamente definida en el sistema. Para que el clasificador asigne un elemento a una clase concreta, es necesario extraer características de ésta. En la clasificación de vehículos se emplean principalmente dos métodos: top-down y bottom-up. La clasificación top-down analiza los objetos como un todo, mientras que la clasificación bottom-up detecta las partes del objeto y las clasifica previamente a su agrupación en objetos.

La última etapa es el tracking o rastreo. Consiste en la localización de un elemento en los cuadros consecutivos de una secuencia de video. Esta asociación se complica si los elementos están en movimiento. El proceso se divide en dos partes. Primero, se generan características del objeto o del fondo del objeto para cada cuadro del video. Posteriormente, se asocian las correspondientes regiones con cuadros consecutivos basados en las características previamente extraídas.

2.5.2. Sistemas de detección de clases de vehículos

Los sistemas de clasificación y detección de vehículos asignan un elemento detectado en una imagen (o secuencia de vídeo) a una clase en base a información previamente definida. Se pueden distinguir dos métodos de clasificación: top-down y bottom-up. Tradicionalmente el método más empleado ha sido el top-down, aunque conlleva limitaciones, debido a la amplia variedad de condiciones de análisis que se presentan. Actualmente, los métodos de reconocimiento de patrones o bottom-up están ofreciendo resultados prometedores [136].

Un sistema de clasificación de vehículos bottom-up extrae partes de una imagen. Estas partes se identifican con una clase de un objeto previamente entrenado. Las partes identificadas se combinan para dar como resultado un objeto mediante un proceso de votación. Por ejemplo, un área de una imagen se clasifica como una rueda. Esta clasificación se basa en información aprendida previamente sobre imágenes de ruedas. A continuación, las ruedas se combinan para dar un objeto que podría ser una moto. La extracción de características de la imagen más simple, se basa en información de los píxeles. Con esta información, se crea un vocabulario visual de las distintas partes del objeto a partir de un conjunto de imágenes de muestra. Las imágenes se representan combinando el vocabulario junto con las relaciones espaciales entre las distintas partes de la imagen. El algoritmo de aprendizaje aprende a detectar partes pertenecientes a un objeto en nuevas imágenes [137]. Se emplea como medida de similitud la correlación cruzada para determinar qué partes del vocabulario están presentes en la imagen. Una de

las limitaciones que conlleva el empleo de la función de correlación cruzada, es que se ve afectada por cambios de iluminación o del tamaño de la imagen.

Existen otros descriptores de extracción de características. Los más relevantes son: SIFT (Scale Invariant Feature Transform), U-SURF (Upright-Speeded- Up Robust Features), HOG (Histograms Oriented Gradients) o BFM (Boundary Fragment Model).

SIFT se basa en la transformación de una imagen en una representación compuesta de puntos de interés, una colección de vectores de características locales [138]. Normalmente, si la imagen sufre cambios de escala o de iluminación, las características del vector varían. Esta variación se evita con la aproximación del filtrado por etapas. En la primera etapa, se identifican los puntos de interés mediante el uso de la función de diferencia gaussiana. Cada punto permite generar un vector de características que describe la región local de la imagen y que se relaciona con las coordenadas en el dominio espacio-escala. Estas características son invariantes ante posibles cambios locales y permiten encontrar correspondencias en dos imágenes que contienen el mismo objeto.

El descriptor U-SURF es similar al visto anteriormente, con la diferencia que la velocidad de computación es mayor. Su empleo es apropiado para aplicaciones donde la cámara se encuentra en posición horizontal [139].

El descriptor HOG está basado en una técnica de reconocimiento de patrones desarrollada por NcConell que emplea histogramas de orientación local [140]. Consiste en la división de la imagen en regiones más pequeñas denominadas celdas. Para cada celda se obtiene el histograma de las distintas orientaciones y se almacenan en cada una de ellas la suma de las magnitudes de gradiente de los píxeles [141]. Con el fin de que no se produzcan variaciones con la iluminación o las sombras, se almacena la energía del histograma de cada celda, en grupos de celdas denominados bloques. Posteriormente, se normalizan todas las celdas del bloque. Su aplicación se extiende tanto al reconocimiento de peatones como de coches. En el estudio de Bunch [142] se aplica a la detección de coches con modelos de superficies en 3 dimensiones, en vez de trabajar con celdas de la imagen en 2 dimensiones.

Por último, el descriptor BFM introduce segmentos de contorno para el reconocimiento general de objetos [143].

La siguiente fase de la clasificación bottom-up es el boosting. Este método, pretende mejorar la precisión del algoritmo de entrenamiento [144]. Éste tiene en cuenta los errores del modelo anterior y lleva asociado un peso en función de los índices de acierto. Suele combinarse con el vector de características locales obtenidas de la etapa anterior, mejorando así la velocidad de computación [145]. Uno de los métodos de aprendizaje de boosting más conocido es Adaboost, consiste en la selección de un número pequeño de características del vector previamente calculado, que serán las que más información aporten al modelo [146].

Para finalizar, se realiza el modelado de las partes de los objetos detectados, y se obtiene la forma del objeto en cuestión. A esta etapa se le conoce como Explicit Shape.

2.5.3. Sistemas de monitorización del estado del tráfico

En los sistemas de monitorización del tráfico se consideran dos tipos de entornos: entornos urbanos y carreteras. Las diferencias entre ambos entornos son significativas, como se ha comentado en secciones anteriores.

En el estudio de Beimer [147], se desarrolla una aplicación para la realización de tracking en carreteras en situaciones de congestión de tráfico en tiempo real. Este sistema fue modificado por Saunier y Sayed [148] aplicado a entornos urbanos. Las secuencias de video fueron grabadas en 4 intersecciones distintas, en escenas complejas, con múltiples opciones de entradas y salidas. En rendimiento del tracking alcanzado fue entre el 85% y el 94%.

Messelodi realiza un análisis del tracking y clasificación de vehículos en intersecciones urbanas en tiempo real [134]. La clasificación de vehículos emplea un modelo de 3 dimensiones que ofrece una descripción general de las formas de los diferentes grupos de vehículos. El principal problema es la generalización de la apariencia de los objetos pertenecientes a la misma clase.

En el gran Canal de Venecia se ha elaborado un modelo de tracking para el seguimiento y la cuenta de botes [149]. Este sistema construye un modelo de fondo del agua del canal y realiza el seguimiento de los botes en tiempo real. En cuanto al seguimiento, emplea el modelo mixto de gaussiana para cada píxel, combinado con flujo óptico y el filtro de Kalman. La precisión obtenida fue del 94% en la cuenta del número de botes.

Kim y Malik se fundamentan en las características de línea de los vehículos para llevar a cabo la detección y el tracking [150]. Las líneas horizontales y verticales del vehículo son capturados por un detector de bordes. Estas líneas se agrupan mediante un método de densidad de probabilidad que forma un modelo de línea del vehículo tridimensional. El tracking se realiza empleando correlación cruzada entre cuadros. El rendimiento en la detección de vehículos fue del 85% y la tasa de alarmas erróneas se mantuvo inferior al 1%.

La detección y clasificación de vehículos en el estudio de Gupte [151] se basa en la correspondencia entre regiones y vehículos a medida que éstos se mueven en la secuencia de la imagen. Para la segmentación, la eliminación del fondo se realiza de manera adaptativa. La tasa de vehículos correctamente detectados fue del 90%, en una secuencia de 20 minutos de video en autopista. De este 90% de vehículos, el 70% fueron correctamente clasificados.

Para concluir, destacar el trabajo de Rad y Jamzad cuyo sistema de clasificación y tracking determina parámetros del tráfico como el cambio de carril o la cuenta de vehículos en carreteras [152]. Se emplea el filtro de Kalman junto con técnicas de diferenciación del fondo para el tracking de vehículos. Además, el algoritmo aprovecha modelos basados en regiones y contornos con el fin de detectar el cuadro que delimita el vehículo. Se examina la forma del objeto y atendiendo el cuadro delimitador del vehículo y las regiones, se determina si fue el resultado de la fusión de varios vehículos

o no. Si es así, se decide el punto más adecuado de división de ambos vehículos. El error de tracking obtenido es del 5.4%.

2.5.4. Técnicas de inteligencia artificial para la gestión del tráfico rodado

Existen varias aproximaciones en la literatura sobre el uso de técnicas de inteligencia artificial basadas en la cooperación para la optimización del tráfico de vehículos. [153] y [154] proponen sistemas cooperativos para el encaminamiento de vehículos basados en sistemas multiagente y algoritmos de inteligencia artificial inspirados en la biología. El sistema de navegación cooperativo propuesto en [155] se basa en la compartición de información de rutas. Aquí, cada vehículo transmite su información de ruta a un servidor, que estima la congestión de tráfico futura y retroalimenta esta información a los vehículos. Sin embargo, el hecho de que se proporcione la misma información a todos los vehículos (en lugar de información individualizada) y que estos replanifiquen sus rutas de forma individual (en lugar de tener en cuenta los intereses colectivos) hace que se manifieste el problema del "juego en minoría", que produce oscilaciones en las rutas.

Otros autores, proponen la propagación de información de tráfico empleando mecanismos inspirados en la biología. Por ejemplo, el uso de feromonas en gestión de tráfico ha ganado popularidad en los últimos años [156] [157]. Del mismo modo, se han empleado técnicas de enjambre inteligente para la propagación de información en [158] y [153]. Estas técnicas guardan cierta similitud con los mecanismos basados en reserva de [159] y con la aproximación basada en mercados de [160]. El uso de sistemas multiagente en estos enfoques se asemeja a los poliagentes de [161].

Desde la perspectiva de la teoría de control, la gestión de un sistema a gran escala como el tráfico rodado en una ciudad es una tarea compleja, dado el alto grado de incertidumbre e impredecibilidad que conlleva [160]. El control óptimo de flujos en cualquier red de tráfico (incluyendo el tráfico rodado) es un problema tradicionalmente reconocido como NP (no resoluble en tiempo polinomial). Por ello, las estrategias tradicionales de control a menudo consisten en buscar semejanzas con situaciones pasadas y aplicar las estrategias de control que mejor funcionaron en esas situaciones. Desafortunadamente, las fluctuaciones en sistemas dinámicos son muy grandes, por lo que la estrategia de control resultante a menudo es óptima para una situación media que apenas se da en la práctica. Una forma diferente de abordar este problema puede ser una estrategia distribuida en tiempo real. Algunos autores proponen el uso de mercados como solución, ya que se han demostrado útiles para otros problemas de asignación de recursos. En el contexto de la gestión de tráfico, el problema puede resumirse como alcanzar un acuerdo sobre el reparto de los elementos de la red de carreteras a los conductores. En [160], los autores diseñan un mercado computacional competitivo, donde los agentes que representan a los conductores "compran" el uso de la capacidad de las intersecciones a unos "agentes de intersección". Los autores muestran cómo la dinámica de mercado influye en el comportamiento de los conductores, resultando en un

uso más eficiente de la infraestructura de transporte, en términos de unos tiempos de tránsito menores y una congestión menos acusada.

En los últimos años, está habiendo un creciente interés sobre la aplicación de técnicas basadas en agentes al control del tráfico, debido a su demostrada flexibilidad y escalabilidad. En [162], agentes en los semáforos crean "oleadas verdes" en direcciones específicas como respuesta a problemas de satisfacción de restricciones distribuidas. En [163] los agentes de los semáforos aprenden de forma coordinada las mejores planificaciones para su secuencia de señalización. En [164], se presenta un enfoque auto organizativo que conduce a patrones de coordinación emergentes y logra un control descentralizado eficiente. Otras aproximaciones se centran en el modelado del comportamiento de los conductores [165] [166]. Las tasas por congestión son otro mecanismo para influir en el comportamiento de los conductores, en el que se penaliza a éstos por las externalidades negativas que causan al resto de conductores (congestión) y al medio ambiente (polución). Estos mecanismos se han desplegado con éxito en muchas grandes ciudades como Londres [167], Estocolmo [168] y Singapur [169]. Aunque las tasas fijas de congestión pueden, en principio, reducir la congestión del tráfico, el hecho de que se establezcan a priori hace que no se adapten a las diferentes condiciones del tráfico. En los mercados computacionales, por el contrario, los agentes que representan a la infraestructura pueden calcular el esquema de precios más adecuado en cada momento para lograr una distribución de la carga de tráfico cercana al óptimo.

En [170], los autores proponen una infraestructura para el control de sistemas dinámicos por medio de tecnologías multiagente, que descompone un modelo centralizado del problema en una red de sub problemas más pequeños interconectados que pueden ser resueltos por agentes distribuidos. Esta infraestructura se aplica al control de la señalización en redes de tráfico. En [171], se propone la coordinación óptima de los límites de velocidad en una red de carreteras con el objetivo de minimizar el tiempo que los vehículos pasan en la red. El problema se resuelve por medio de un modelo de control predictivo, donde se usa el modelo de tráfico macroscópico METANET [172] como modelo de predicción. En [173], se propone un sistema de control para señales de tráfico, de nuevo basado en la compartición de rutas y el procesamiento de dicha información para predecir la congestión al estilo de [155]. Los diferentes parámetros de las señales de tráfico (ej. ciclo, split y offset) se optimizan en función de la congestión esperada.

2.6. Internet of Things

IoT es un concepto que hace referencia a la interconexión digital de objetos cotidianos a Internet, de modo que puedan ofrecer información o interactuar entre ellos. La idea de tener dispositivos interconectados de forma continua a nivel global, surgió con la tecnología RFID (Radio Frequency IDentification), y este concepto se ha ampliado considerablemente con la visión actual que contempla una gran cantidad de objetos heterogéneos que interactúan con el entorno físico. Cada objeto está identificado de

forma única y es accesible a la red, de modo que es posible conocer su posición y su estado, lo que le añade inteligencia. Esto da lugar a la generación de enormes cantidades de datos que tienen que ser almacenados, procesados y presentados de una forma transparente, eficiente y fácilmente interpretable.

Las WSN son uno de los elementos más importantes del paradigma Internet of Things, ya que proporcionan una capa virtual donde cualquier pieza de información capaz de monitorizar el mundo físico, puede ser potencialmente accesible por cualquier sistema informático.

Mientras que *sensor web* describe una infraestructura para sensores heterogéneos, que pueden estar conectados en red o de forma individual, fijos o móviles, y pueden incorporar dispositivos de detección in situ o remotos, la visión de los dos campos de investigación relacionados Internet of Things y Web of Things, es la integración, en general, de las "cosas" del mundo real con Internet o Web, respectivamente. Algunos ejemplos de este tipo de cosas son los electrodomésticos, dispositivos embebidos y móviles, pero también dispositivos de detección inteligentes (sensores). A menudo, la interacción con el usuario se realiza a través de un teléfono móvil que actúa como mediador en el triángulo de personas, cosas, e Internet/Web.

Sin embargo, en los casos de uso más complejos que necesitan modelos de información de sensores detallados y normalizados y mayor funcionalidad en el acceso, descubrimiento, gestión de tareas y eventos, tales como la gestión de desastres o de sistemas de alerta temprana, pueden no ser realizables con Internet of Things.

En cuanto la arquitectura de red de IoT, los principales elementos de red que la componen son generalmente Internet y redes de smart objects. Técnicamente, el éxito de Internet se debe en parte a la adopción de la arquitectura TCP/IP. También, como se muestra en [174], la arquitectura IP es interoperable con dispositivos y tecnologías de comunicación, está en constante evolución y es versátil sin dejar de ser estable, es escalable y fácil de administrar, y es lo suficientemente simple para que un smart object con recursos limitados pueda ejecutarlo fácilmente. Todos estos hechos hacen razonable que IoT se base en una arquitectura IP.

Actualmente, IoT se centra en la visibilidad de la información, y la idea principal es el uso de métodos de planificación y control descentralizados y jerárquicos. La combinación de control autónomo e IoT proporciona un mayor nivel de robustez en la infraestructura, escalabilidad y agilidad. En la actualidad, ya existen diversos gestores de datos y servicios en la nube para la interoperabilidad de las aplicaciones de la IO, como por ejemplo, ThingWorx [175], EVRYTHNG [176], Sense [177] o SNSoT [178].

Dominios de aplicación

Existen varios dominios de aplicación que se ven afectados por el crecimiento de Internet of Things. Las aplicaciones se pueden clasificar en función del tipo de red disponible, la cobertura, la escala, la heterogeneidad, la repetitividad, la participación de

los usuarios y el impacto [179]. Las aplicaciones se pueden clasificar en cuatro dominios de aplicación: personal y del hogar, empresa, servicios públicos, y móvil.

En el hogar, la información recogida por los sensores es utilizada únicamente por los propietarios de la red. Por lo general, se utiliza Wi-Fi como protocolo de comunicaciones, ya que permite mayor ancho de banda en la transferencia de datos (vídeo), así como frecuencias de muestreo más altas (audio). En el ámbito del hogar, IoT ofrece una plataforma perfecta para la monitorización continua de la salud [180], utilizando un teléfono inteligente junto con varios sensores que miden parámetros fisiológicos. Esto se puede extender para crear un sistema de monitorización en el hogar para el cuidado de personas de edad avanzada, permitiendo al médico vigilar los pacientes en sus hogares y actuar de forma inmediata ante una emergencia [181] [182]. Otra de las utilidades es el control de los equipos de casa, tales como aire acondicionado, neveras, lavadoras, etc., lo que permite un mayor control y el ahorro de energía [183] [184].

A nivel empresarial, la información recogida en este tipo de redes también es utilizada solamente por los propietarios. La aplicación más común es la monitorización ambiental, que se lleva a cabo para gestionar los recursos de la empresa (por ejemplo, sistemas de climatización, iluminación). Una de las principales áreas de aplicación de IoT es para la conservación del medio ambiente [179] [185].

La información de las redes en servicios públicos, es por lo general, para la optimización de un servicio en lugar de consumo incontrolado. Ya está siendo utilizado por empresas de servicios públicos para la gestión de recursos en redes muy extensas (a escala regional y nacional), con el fin de optimizar el costo. Una de estas aplicaciones es el smart grid y los contadores inteligentes [186], que se usa para lograr un consumo eficiente de energía mediante un seguimiento continuo de todos los puntos de electricidad dentro de una casa y el uso de esta información para modificar la forma en que se consume la electricidad. La supervisión de la red de agua y la garantía de calidad del agua potable es otra aplicación crítica que se aborda con el uso de IoT. Los sensores que miden parámetros críticos del agua se instalan en lugares estratégicos con el fin de garantizar una alta calidad de suministro. Esto evita la contaminación accidental de los drenajes de aguas pluviales, agua potable y eliminación de aguas residuales [187]. La misma red se puede ampliar para controlar riego en tierras agrícolas. La red se extiende también para el seguimiento de los parámetros del suelo que permite la toma de decisiones informadas en relación con la agricultura [188].

El transporte inteligente y la logística inteligente se colocan en un dominio independiente (dominio móvil) debido a la naturaleza del intercambio de datos. Por ejemplo, el tráfico urbano es el principal contribuyente a la contaminación sonora y más importante aún, produce emisiones contaminantes y de gases de efecto invernadero. Además, la congestión del tráfico influye directamente los costos de actividades económicas y sociales en la mayoría de las ciudades. La aplicación de IoT en el transporte, permite el uso de WSNs a gran escala para obtener información dinámica del tráfico, seguimiento online de los tiempos de viaje, contaminación del aire o las

emisiones de ruido. Con toda esta información recopilada, es posible mejorar el sistema de control de tráfico urbano, mejorar la planificación de servicios públicos, y ofrecer información actualizada a los ciudadanos [189]. Otra aplicación importante en el dominio móvil de IoT es la gestión logística eficiente [190], que incluye el seguimiento de los artículos que se transportan, así como la planificación de transporte eficiente.

3. Especificación de arquitectura

3.1. Introducción

El objetivo principal de este capítulo, es la descripción general de la arquitectura de IoT propuesta que va a ser utilizada en los casos de uso planteados (FASyS, UniverSEC y STIMULO). La arquitectura será compatible con los objetivos planteados en el inicio de la tesis, sin perder la aplicabilidad a los diferentes casos de uso. La arquitectura tendrá como finalidad garantizar la interoperabilidad de los sistemas, y garantizar las prestaciones y la integración de los diferentes sensores en las aplicaciones de los casos de uso, siguiendo las especificaciones de los estándares propuestos en el estado del arte.

La arquitectura es la base estructural que unifica los requerimientos actuales y permite la incorporación de su evolución, así como nuevos requerimientos de forma satisfactoria. Para esta tesis se ha desarrollado la arquitectura **I3WSN** (Intelligent Wireless Sensor Networks in Indoor Industrial applications) [191], ya que cumple todos los requisitos ya sean funcionales o no funcionales: calidad, seguridad, disponibilidad, eficiencia, rendimiento, etc. Aunque en un principio estaba pensado para entornos indoor, se puede adaptar fácilmente para entornos exteriores sin alterar su esencia. Para el diseño de la arquitectura se consideran los usuarios finales del sistema, los objetivos y requisitos funcionales, y la metodología que se va a aplicar, aunque la arquitectura se ha diseñado con el objetivo de poder ser extendida a diversos entornos de funcionamiento.

La arquitectura I3WSN, da una visión global de los diferentes componentes que la forman, así como su distribución en los distintos escenarios y casos de uso. La arquitectura tiene carácter distribuido, por lo que las comunicaciones, la gestión y el control son una parte relevante del diseño de la misma.

La definición de una arquitectura genérica, aporta una serie de ventajas al aplicarla a los casos de uso definidos y aquellos a los que potencialmente se podría aplicar en un futuro:

- Permite definir la estructura en la que todas las partes interesadas definan sus necesidades.
- Separar distintas tareas y objetivos de manera que se reduzca la complejidad y se pueda abordar cada parte por separado.
- Mejorar la calidad del sistema gracias a la tolerancia a fallos, compatibilidad, escalabilidad, disponibilidad o seguridad.
- Facilitar la reutilización de arquitecturas estándar debido a problemas recurrentes.
- Proporcionar un modelo de referencia de arquitectura para la interoperabilidad de los sistemas de IoT.

En la primera sección del capítulo se presenta la arquitectura I3WSN para los sistemas de monitorización y gestión. En la segunda sección, se describe como se aplica el estándar SWE a dicha arquitectura propuesta, centrándose en el funcionamiento del servicio SOS. Por último, se incluye una descripción de las diferentes variantes de la arquitectura en función de la topología para su posterior aplicación a los casos de uso definidos.

3.2. Visión general de la arquitectura

La arquitectura I3WSN está diseñada de forma general para que sea compatible con las necesidades específicas de los sistemas IoT [192]. Además, la arquitectura está organizada jerárquicamente de manera que sea flexible para adaptarse a los distintos casos de uso. Por tanto, el principal objetivo es garantizar la interoperabilidad entre las distintas redes de sensores y con la plataforma de monitorización y control, de forma que se facilite la recopilación, almacenaje y procesado de los datos.

En la Figura 9, se puede ver una visión de alto nivel de la arquitectura del sistema propuesto para el sistema de monitorización y control de los casos de uso. Además del propio sistema que se debe supervisar y gestionar, existen dos bloques independientes y que funcionan en paralelo al sistema evaluado: el **bloque de obtención de datos** y el **centro de control**.

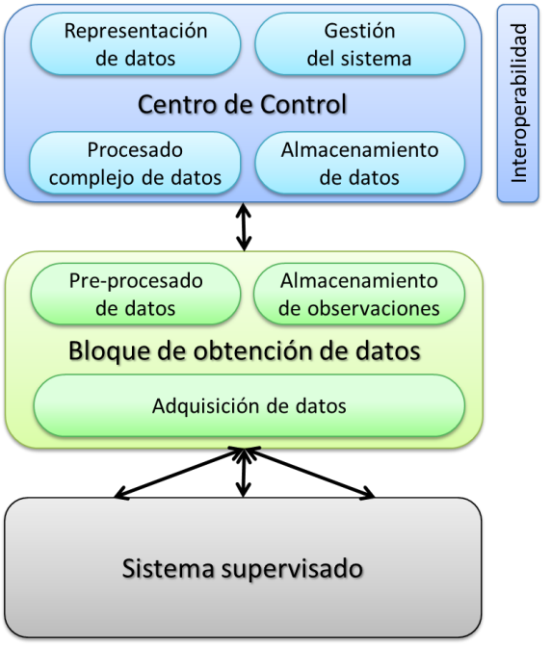

Figura 9. Visión de alto nivel de la arquitectura I3WSN

Ya que el sistema debe ser escalable para adaptarse al tamaño del sistema supervisado, es posible que exista más de un centro de control o bloque de obtención de datos. Por tanto, ambos bloques permiten la interoperabilidad a través de un protocolo de comunicaciones.

Esta arquitectura permite separar las dos funcionalidades principales, de modo que es más sencillo de implementar y más fácil de modificar o cambiar en caso de que fuera necesario.

3.2.1. Bloque de obtención de datos

El primero de estos dos bloques es el de obtención de datos, el cual es el responsable de reunir, almacenar y proporcionar todos los datos relevantes del sistema supervisado.

Proporciona las diferentes medidas y eventos relacionados tanto con datos como con la infraestructura del sistema supervisado, que se soliciten desde el centro de control. Los eventos relacionados con la infraestructura pueden ser la pérdida o la adición de objetos al sistema (sensores o sondas).

Por tanto el bloque de obtención de datos debe conocer:

- La topología de sensores desplegados (su tipo, la ubicación, sus medidas y la fiabilidad/calidad).
- La topología de servicios (dónde acceder a las mediciones, o desplegar un sensor específico para un dispositivo). Básicamente, es responsable de establecer el vínculo entre las solicitudes centro de control y los sensores.

La situación actual de las redes de sensores es que cada una de ellas son sistemas adquiridos y desarrollados para resolver un problema específico, caracterizados por un enfoque y funcionalidad limitados y conteniendo datos que no son fácilmente compartibles con otros sistemas; esto se traduce en sistemas propietarios en el descubrimiento, el acceso a las observaciones, la recepción de alertas y la asignación de tareas. La integración de un sensor nuevo en estos sistemas es típicamente una tarea altamente costosa, debido a servicios y codificaciones incompatibles. Para poder acometer la visión 'plug-and-play' se requieren las siguientes funcionalidades:

- Descubrimiento de sensores y datos de sensores
- Determinación de las capacidades de los sensores y la calidad de las medidas
- Acceso a los parámetros de los sensores que permiten al software procesar las observaciones automáticamente
- Acceso a medidas en tiempo real, así como a medidas de ventanas temporales en codificaciones estandarizadas
- Configuración de sensores y simulaciones para adquirir observaciones de interés
- Suscripción y publicación de alertas llevadas a cabo por los sensores y basadas en algún tipo de criterio (notificación basada en eventos)

Es por ello, que es imprescindible que el bloque de obtención de datos se base en estándares con el fin que sensores de cualquier fabricante y tipo puedan insertar datos, y cualquier aplicación pueda acceder a los datos. Por ese motivo, SWE implementa el SOS (Sensor Observation Service), un repositorio estándar en el que almacenar todas las medidas y especificaciones para el envío de datos.

En caso de ser necesario, en el bloque de datos, es posible realizar un procesado previo a insertar los datos en el SOS. Este procesado puede consistir en transformar los datos a medidas adecuadas o la obtención de nuevos parámetros a partir de un subconjunto de los datos obtenidos. De este modo, se almacenan en el SOS datos más útiles que pueden ser usados directamente para procesos más complejos.

3.2.2. Centro de control

El segundo bloque es el centro de control, cuya función principal es proporcionar al usuario una visión global centralizada del estado de los parámetros de seguridad configurados para el sistema monitorizado. Para ello, se debe procesar la información, extraer conclusiones y mostrar los resultados a los usuarios.

Los principales elementos que interactúan con el centro de control son el usuario final, ya sea el administrador o el supervisor del sistema evaluado y el bloque de obtención de datos que proporciona una capa de abstracción para la recogida de los datos proporcionados por los sensores. El centro de control tiene como objetivo ser una herramienta integrada en el sistema supervisado, lo que significa que tiene que ser capaz de interoperar con diversos agentes.

El centro de control es responsable de la gestión (especificación, modificación, evaluación) del modelo de seguridad de los servicios supervisados (objetivos, requisitos, evaluación). Sin embargo, el centro de control no tiene conocimiento de la infraestructura de medición: el tipo de sensores, su ubicación y características. El centro de control define un conjunto de indicadores y proporciona un conjunto de definiciones de medición necesarios, para la evaluación global de la seguridad.

El centro de control se compone de dos elementos principalmente:

- Un interfaz gráfico o HMI, a través del cual, se puede gestionar el sistema y visualizar toda la información pertinente.
- Un motor de procesado de eventos complejos o CEP, que incluye funciones relacionadas con la obtención de datos inteligente, combinación, agregación, etc.

Además el centro de control dispone un modelo de datos en el cual se almacena información referente al control de usuarios, parámetros de configuración y de medida, datos del sistema supervisado, etc.

3.2.3. Comunicación entre el centro de control y el bloque de obtención de datos

La comunicación entre los diferentes bloques del sistema es un elemento crítico y por tanto se debe tener especial interés en su seguridad. En la arquitectura diseñada, el bloque de obtención de datos se encarga de la recogida continua de la información requerida en la evaluación de la seguridad del sistema supervisado, pero la comunicación entre ambos no consiste únicamente en enviar las medidas obtenidas, sino que se intercambian otros datos en ambas direcciones. La Figura 10 muestra el flujo de datos entre el centro de control y el bloque de obtención de datos.

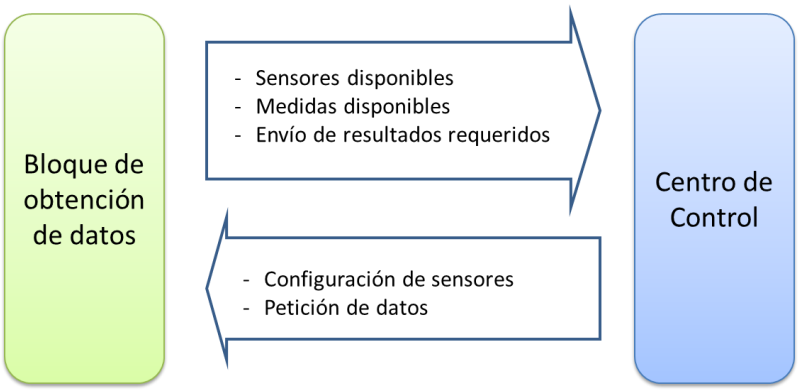

Figura 10. Comunicación entre ambos bloques

Como se distingue en la figura, en la comunicación entre los bloques se observan los siguientes casos:

- Notificación de información: el bloque de obtención de datos comunica del tipo de información que puede obtener del sistema supervisado.
- Notificación de la disponibilidad de sensores: el bloque de obtención de datos informa al centro de control de todos los sensores o sondas desplegados y la posición de cada uno de ellos.
- Configuración de sensores: El centro de control envía al el bloque de obtención de datos la configuración que deben tener cada uno de los sensores.
- Petición de datos: El centro de control pide al bloque de obtención de datos todos los datos necesarios para la evaluación de los parámetros de seguridad.
- Envío de resultados: El bloque de obtención de datos devuelve todos los datos requeridos por el centro de control que tiene almacenados en el SOS.

3.3. SWE en la arquitectura I3WSN

Además de ver la arquitectura general del sistema es importante también comprender como se aplica SWE dentro de dicha arquitectura.

En primer lugar, de entre todos los servicios que ofrece SWE, se va a utilizar el SOS para el almacenamiento de medidas y las especificaciones O&M y SensorML para modelar las medidas de los sensores y los propios sensores.

Cada uno de los dispositivos desplegados en los casos de uso, ya sean sensores, trabajadores, routers, cámaras, etc., son tratados como sensores, y por tanto insertan sus medidas en el SOS. De esta forma, el sistema supervisado y el bloque de obtención de datos quedarían como se muestra en la Figura 11.

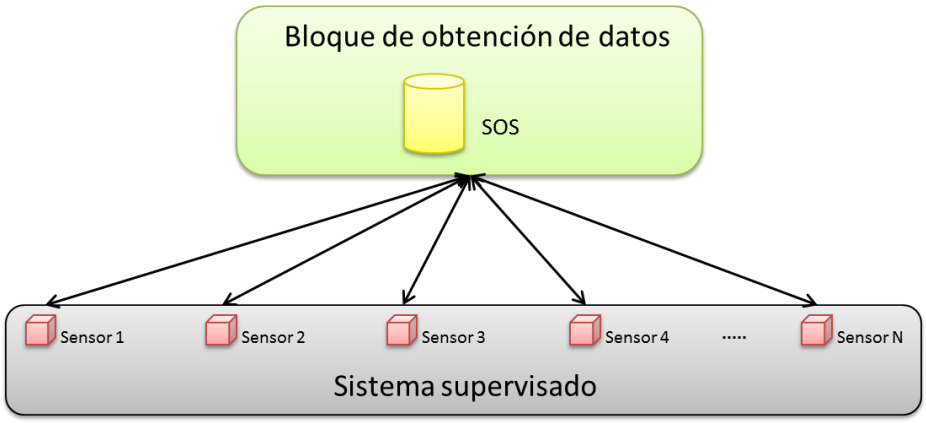

Figura 11. Aplicación de SWE a la arquitectura

Se ha utilizado la implementación libre más extendida y potente del SOS, la desarrollada por el 52north [53]. La primera versión de la especificación se desarrolló en 2008 (SOS 1.0.0) y ha sido utilizado para múltiples trabajos y proyectos. Gracias al esfuerzo y colaboración de toda la comunidad, en 2012, se terminó la especificación SOS 2.0, en la que se mejoran algunos aspectos y bugs.

Las principales diferencias entre ambas versiones, es que en la versión SOS 1.0 se define una operación (RegisterSensor) para dar soporte a la inserción de nuevos sensores. Sin embargo, el modelo de esa operación, y en particular la asociación del nuevo sensor con los metadatos específicos del offering, era insuficiente. Por tanto, en la versión SOS 2.0, el modelo de servicio SWE define el modelo conceptual de la operación InsertSensor que sustituye a la operación RegisterSensor. La operación InsertSensor ahora incluye todos los elementos de información requeridos para rellenar una oferta de servicios SWE (por ejemplo, las propiedades observadas por el nuevo sensor o características relacionadas con ese sensor). Además, se pueden añadir metadatos específicos para un determinado tipo de servicio de SWE (por ejemplo, SOS o SPS), permitiendo introducir propiedades específicas necesarias.

Además, esta nueva versión reestructura la especificación mediante la separación en principales y extensiones, introduce KVP o mejora la interoperabilidad gracias a la definición de un conjunto obligatorio de operadores y operandos para los filtros temporales y espaciales

3.3.1. Funcionamiento del SOS

El SOS de OGC especifica un interfaz estándar y un protocolo para descubrir y acceder a las observaciones. Al igual que otras especificaciones de servicio de OGC, el SOS utiliza el protocolo HTTP, en particular las operaciones GET y POST, para el envío de solicitudes y mensajes de respuesta basados en XML.

El proceso que debe seguir un sensor o productor para insertar datos en el SOS, así como el que debe seguir un cliente o consumidor para leer datos, es el que se encuentra en la Figura 12. La interacción es la siguiente:

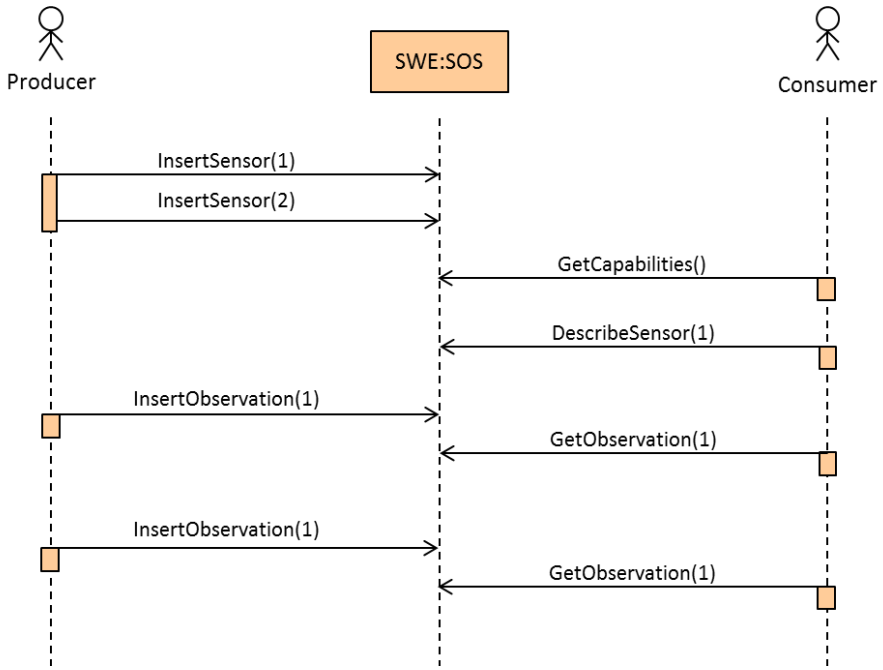

Figura 12. Esquema del funcionamiento del SOS

1. En primer lugar, el productor datos (típicamente un sensor, una red de sensores, o incluso un simulador) se registra en el servidor SOS mediante la operación *InsertSensor*. Nótese que el productor registra dos sensores, lo cual es posible y lógico para una red de sensores o una estación que cuente con múltiples sensores. Aunque no se indica en la figura, el servidor SOS, responde típicamente en caso de éxito con un ID único que identifica al sensor para posteriores búsquedas.
2. En un primer momento, el consumidor (o un servicio de monitorización, como es el caso del dentro de control) contacta con el servidor SOS para obtener datos de medidas de un sensor registrado. Como inicialmente desconoce los sensores que están registrados en dicho servidor, el consumidor procede con una operación *GetCapabilities* para obtener una lista de ellos y las operaciones permitidas.
3. A continuación, el consumidor desea conocer más datos acerca de un sensor en concreto. Es por ello, por lo que envía una petición del tipo *DescribeSensor* para conocer todos los detalles de este sensor.
4. En un momento determinado, el productor inserta medidas en el servidor SOS mediante la operación InsertObservation. Aunque esta operación es asíncrona, típicamente las redes de sensores se configuran para obtener resultados de los sensores de forma periódica. En caso de almacenarse correctamente la respuesta es el identificador de la observación.

5. En un momento posterior, el consumidor solicita la(s) medida(s) relativa al sensor previamente descrito por el SOS mediante la operación *GetObservation*. Debido a la posible gran cantidad de datos es necesario utilizar filtros espaciales y temporales.
6. El productor sigue enviando datos (medidas) al servidor SOS.
7. Del mismo modo, el consumidor solicita al servidor SOS nuevos resultados de medidas. En este momento, se dispone de nuevos datos que pueden ser enviados al consumidor.

3.3.2. Mensajes del SOS

Seguidamente, se va a describir la estructura que debería tener los mensajes previamente comentados para poder ser enviados al SOS correctamente y algunas de las respuestas más importantes.

GetCapabilities

La operación *GetCapabilities* permite a un cliente solicitar y recibir un documento sobre las prestaciones del servicio, que describe las operaciones y los sensores registrados en una instancia de SOS.

A continuación, se muestra un ejemplo de petición *GetCapabilities*. En el mensaje se debe indicar la versión del SOS y que información se desea recibir.

```
<ows:AcceptVersions>
   <ows:Version>2.0.0</ows:Version>
</ows:AcceptVersions>
<ows:Sections>
   <ows:Section>OperationsMetadata</ows:Section>
   <ows:Section>ServiceIdentification</ows:Section>
   <ows:Section>FilterCapabilities</ows:Section>
   <ows:Section>Contents</ows:Section>
</ows:Sections>
```

El mensaje de respuesta sería de la siguiente forma. Este mensaje es bastante extenso y se omiten varios elementos y atributos por simplicidad, centrándose únicamente en el listado de sensores.

```
<ows:Parameter name="procedure">
<ows:AllowedValues>
<ows:Value>Sensor1</ows:Value>
<ows:Value> Sensor 2</ows:Value>
<ows:Value> Sensor 3</ows:Value>
</ows:AllowedValues>
</ows:Parameter>
```

InsertSensor

La operación *InsertSensor* permite registrar nuevos sensores en el SOS, estructurados con la especificación SensorML.

A continuación se muestra un ejemplo de petición *InsertSensor*, en el que se detallan todas las propiedades de un sensor, como su identificador, nombre, tipo, posición o propiedades medidas.

```
            <sml:IdentifierList>
              <sml:identifier name="uniqueID">
                <sml:Term definition="urn:ogc:def:identifier:OGC:1.0:uniqueID">
                  <sml:value>id</sml:value>
                </sml:Term>
              </sml:identifier>
              <sml:identifier name="shortName">
                <sml:Term definition="urn:ogc:def:identifier:OGC:1.0:shortName">
                  <sml:value>name</sml:value>
                </sml:Term>
              </sml:identifier>
              <ns:identifier name="type">
                <ns:Term definition="urn:ogc:def:identifier:UniverSEC:1.0:type">
                  <ns:value>BM</ns:value>
                </ns:Term>
              </ns:identifier>
            </sml:IdentifierList>

                <swe:coordinate name="easting">
                  <swe:Quantity axisID="x">
                    <swe:uom code="degree"/>
                    <swe:value>latitude</swe:value>
                  </swe:Quantity>
                </swe:coordinate>
                <swe:coordinate name="northing">
                  <swe:Quantity axisID="y">
                    <swe:uom code="degree"/>
                    <swe:value>longitude</swe:value>
                  </swe:Quantity>
                </swe:coordinate>
                <swe:coordinate name="altitude">
                  <swe:Quantity axisID="z">
                    <swe:uom code="m"/>
                    <swe:value>altitude</swe:value>
                  </swe:Quantity>
                </swe:coordinate>

            <sml:InputList>
              <sml:input name="property">
                <swe:ObservableProperty definition="
urn:ogc:def:phenomenon:OGC:1.0.30:property"/>
              </sml:input>
            </sml:InputList>
          </sml:inputs>
          <sml:outputs>
            <sml:OutputList>
              <sml:output name="Vulnerability">
                < swe:Quantity definition="urn:ogc:def:phenomenon:OGC:1.0.30:property">
                </swe:Quantity>
              </sml:output>
            </sml:OutputList>
          </sml:outputs>
```

InsertObservation

La operación *InsertObservation* permite enviar al SOS las nuevas medidas que se van produciendo estructuradas de acuerdo con la especificación O&M.

A continuación se muestra un ejemplo de petición *InsertObservation*, en el que se detallan todas las propiedades de una medida, como su fecha, sensor, propiedad medida, valor y unidades.

```
<om:phenomenonTime>
   <gml:TimeInstant gml:id="phenomenonTime">
      <gml:timePosition>date</gml:timePosition>
   </gml:TimeInstant>
</om:phenomenonTime>
<om:resultTime xlink:href="#phenomenonTime"/>
<om:procedure xlink:href="id"/>
<om:observedProperty xlink:href=" urn:ogc:def:phenomenon:OGC:1.0.30:property"/>

<om:result xsi:type="gml:MeasureType" uom="utit">1.2</om:result>
```

DescribeSensor

La operación *DescribeSensor* permite a un cliente obtener información detallada de las características de un sensor, estructurada con la especificación SensorML.

A continuación se muestra un ejemplo de petición *DescribeSensor*, en la que se solicita información un sensor.

```
<swes:procedure>id</swes:procedure>
<swes:procedureDescriptionFormat>http://www.opengis.net/sensorML/1.0.1</swes:procedureDescriptio
nFormat>
```

El mensaje de respuesta es el mismo que se envía al registrar el sensor con todos sus datos actualizados. Se mostrará su id, nombre, posición, las medidas que ofrece, etc.

GetObservation

La operación *GetObservation* permite recuperar los datos de observaciones de sensores, estructuradas de acuerdo con la especificación O&M. Permite realizar de forma sencilla filtrados temporales y espaciales con el fin de mejorar la obtención de datos.

A continuación se muestra un ejemplo de petición *GetObservation*, en el que únicamente se solicita la última medida (filtro temporal) de una de las propiedades de un sensor.

```
   <sos:procedure>id</sos:procedure>
<sos:observedProperty>urn:ogc:def:phenomenon:OGC:1.0.30:property</sos:observedProperty>

   <sos:temporalFilter>
      <fes:TEquals>
         <fes:ValueReference>phenomenonTime</fes:ValueReference>
         <gml:TimeInstant gml:id='ti_1'>
            <gml:timePosition>latest</gml:timePosition>
         </gml:TimeInstant>
```

```
      </fes:TEquals>
   </sos:temporalFilter>
```

El mensaje de respuesta sería de la siguiente forma. Los principales parámetros serían la fecha de la medida, la propiedad medida y la propia medida junto con sus unidades.

```
         <om:phenomenonTime>
            <gml:TimeInstant gml:id="phenomenonTime_28345">
               <gml:timePosition>date</gml:timePosition>
            </gml:TimeInstant>
         </om:phenomenonTime>
         <om:procedure xlink:href="id"/>
         <om:observedProperty xlink:href="urn:ogc:def:phenomenon:OGC:1.0.30:property"/>
         <om:result xmlns:ns="http://www.opengis.net/gml/3.2" uom="units"
xsi:type="ns:MeasureType">value</om:result>
```

3.4. Topologías colaborativas

La arquitectura de la Figura 9 es el caso más sencillo posible, pero para poder adaptar la arquitectura a la distribución de una fábrica o la topología de una infraestructura crítica, es necesario que la arquitectura sea adaptable y versátil.

Si el tamaño de la infraestructura a monitorizar es demasiado grande para ser cubierto completamente por un solo centro de control, o si la infraestructura es demasiado heterogénea para que un solo centro de control pueda reflejar sus características, un enfoque centralizado no sería la mejor implementación. En este caso, la solución más adecuada es una arquitectura jerárquica en la que los bloques interoperan entre ellos.

Es por ello, que a partir de los dos bloques principales comentados anteriormente, el centro de control y el bloque de obtención de datos, se puede llevar a cabo un enfoque jerárquico de la arquitectura.

3.4.1. Arquitectura centralizada

Una arquitectura centralizada es aquella en la que existe un elemento central al que llega toda la información y toma las decisiones que afectan al conjunto del sistema. En este caso, toda la información relevante se encuentra almacenada en un único sitio y por tanto es fácilmente accesible. Además, al estar centralizado, la gestión y la securización del sistema es más sencilla

En la arquitectura centralizada existe un centro de control central que agrupa la información de todo el sistema y por tanto tiene una visión global de la seguridad. Por debajo, puede tener varios centros de control locales distribuidos por áreas o zonas que proporcionan una visión local y detallada de la seguridad. Por último, cada uno de los centros de control locales, puede tener uno o más bloques de obtención de datos en función de la topología del sistema o la distribución de las instalaciones.

Los centros de control locales informan sólo de la información más relevante para el central, tales como los valores de seguridad y las alarmas, evitando de esta manera la sobrecarga del centro de control central.

El centro de control central proporcionar una visión global del valor de la seguridad de la infraestructura. Para tener información más completa y detallada se necesita solicitarla a los centro de control locales correspondientes.

Tanto en el proyecto STIMULO, como en UniverSEC, es interesante utilizar una arquitectura centralizada. En el primero, porque necesitas equipos específicos para realizar el procesado de imágenes y las simulaciones. En el caso de UniverSEC, porque necesitas tener una visión centralizada de todo el smart grid.

En la Figura 13 se muestra un ejemplo de enfoque jerárquico centralizado, donde hay dos centros de control locales que informan a uno central.

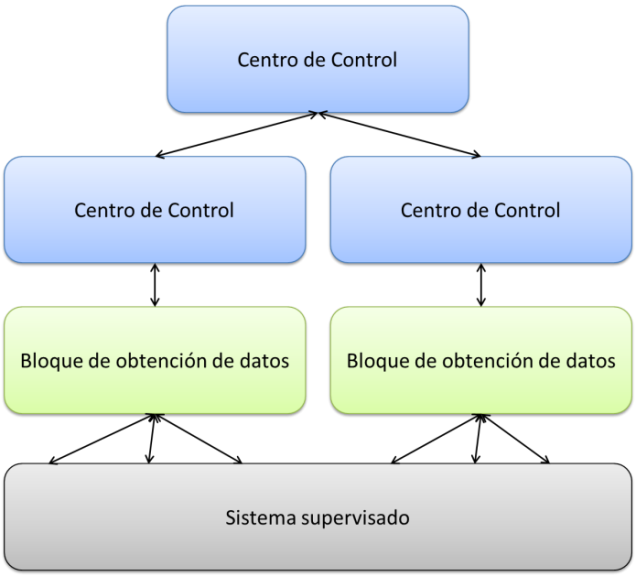

Figura 13. Visión de alto nivel de una arquitectura centralizada

3.4.2. Arquitectura distribuida

Una arquitectura distribuida es aquella en la que varios elementos que tienen un ámbito local, colaboran para cumplir los objetivos globales del sistema. En este caso se consigue que el sistema sea más fiable y resistente, ya que la caída de uno de los elementos no supone el fallo total del sistema. Además, cada uno de ellos tiene una carga computacional menor, y por tanto la velocidad de computación es mayor y se necesitan equipos menos potentes. El sistema permite más fácilmente la escalabilidad, permitiendo ampliar el sistema en caso de necesidad.

En la arquitectura distribuida propuesta no existe un centro de control central donde llega toda la información, sino todos los centros de control locales interoperan unos con otros. Sólo tienen que ponerse de acuerdo en la información que deben intercambiar entre ellos, y de este modo cada uno tiene una visión completa del sistema.

En la Figura 14 se puede ver un ejemplo de arquitectura distribuida con dos centros de control locales que comparten información entre ellos.

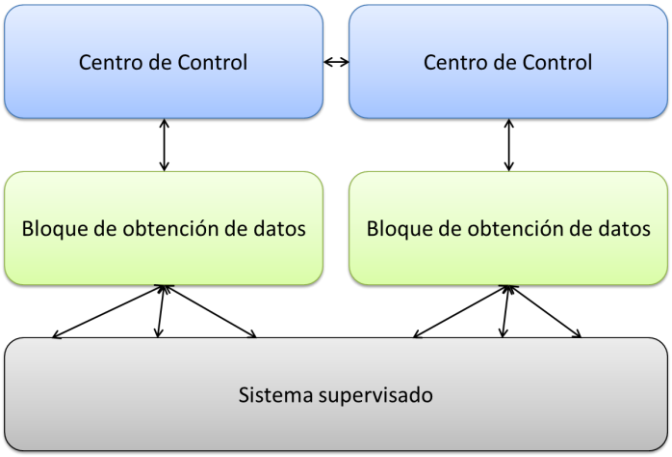

Figura 14. Visión de alto nivel de una arquitectura distribuida

3.4.3. Arquitectura híbrida

Una arquitectura híbrida es aquella en la que existen elementos distribuidos que colaboran entre sí para tomar decisiones globales, pero además existe un elemento centralizado que obtiene la información más relevante de los elementos distribuidos. En este caso se consiguen las ventajas de ambas arquitecturas [193].

La arquitectura híbrida propuesta es una combinación entre la arquitectura centralizada y la distribuida, por tanto, existe un centro de control central donde se agrupa la información más relevante para la visión global del sistema, pero los centros de control locales también comparten información para tener una visión más completa.

En el proyecto FASyS es interesante una arquitectura híbrida, ya que cada edificio de la fábrica puede tener un centro de control local que evalúe sus funciones. Pero después dispondría de un centro de control central que controle toda la fábrica.

La Figura 15 es un posible ejemplo de arquitectura híbrida con un centro de control central y dos locales que comparten información entre ellos.

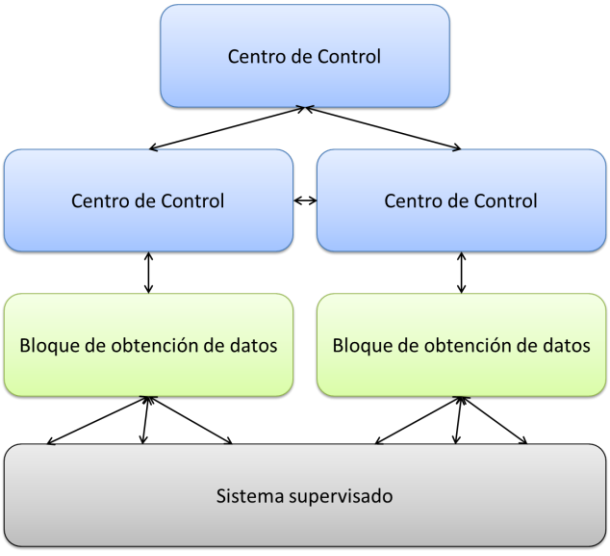

Figura 15. Visión de alto nivel de una arquitectura híbrida

4. Caso 1: FASyS

4.1. Introducción

Las tecnologías de seguridad para entornos industriales han evolucionado considerablemente en los últimos años, pero todavía hay riesgos relacionados con la seguridad y salud de los trabajadores. En este contexto, el concepto de las Fábricas del Futuro (FoF) europeas [194] [195] se centra en el desarrollo y la integración de las tecnologías de ingeniería, las TIC, y materiales avanzados para desarrollar nueva maquinaria y mejorar los procesos industriales. En este nuevo marco, los trabajadores representan un activo más importante para la competitividad y la productividad de fabricación, y se deben llevar a cabo todas las acciones necesarias para mejorar su salud y la seguridad en su entorno laboral. Todo lo que sucede en la fábrica, desde los niveles ambientales, a la posición de todos los elementos deben ser monitorizados, y los riesgos potenciales deben ser anticipados a través de acciones preventivas automatizadas.

Es importante entender que una fábrica absolutamente segura no está ausente de riesgos, sino que es una fábrica en la que los riesgos y la salud están en todo momento controlados. Para lograr estos objetivos, el proyecto FASyS [8] desarrolla un nuevo modelo de fábrica dirigido a minimizar los riesgos para la salud y seguridad del trabajador, y garantizar su bienestar y confort en las fábricas de manipulación, mecanizado y montaje, dentro de la iniciativa española CENIT (CEN-20091034). El proyecto aborda varios aspectos tales como el desarrollo de protocolos de prevención y soluciones de monitorización de salud personalizada, técnicas de procesado de datos de salud, y la inteligencia para el análisis y la toma de decisiones, entre otros. El proyecto se centra en un gran número de escenarios asociados a varios riesgos identificados en el entorno operativo. Entre ellos, se pueden encontrar control de atropello y colisión, control de golpes e impactos, control de trabajo en altura, control de posturas forzadas, control de manipulación manual de carga, control de exposición a químicos, control de ruido y vibraciones, etc.

En la segunda sección del capítulo, se presentan los objetivos principales que intenta lograr el proyecto FASyS. En la tercera sección, se visualiza la arquitectura con la que se ha llevado a cabo el proyecto, y en la siguiente, el funcionamiento más detallado de todas sus partes. En la quinta sección, se enumeran los logros que ha conseguido el proyecto. Por último, se analiza el simulador implementado para generar datos de sensores.

4.2. Objetivos de FASyS

El objetivo global del proyecto FASyS, consistió en diseñar y desarrollar un modelo de fábrica excelente de referencia en términos de prevención integral y personalizada de riesgos laborales, en empresas industriales de mecanizado y montaje. Actualmente, no existe un marco común, un paradigma integral, un modelo de empresa global que permita la aplicación holística del concepto de seguridad y salud industrial. FASyS permite formalizar tanto la propia fábrica excelente de referencia, como los procedimientos de funcionamiento operativo.

El objetivo del proyecto FASyS, fue desarrollar un conjunto de nuevas tecnologías que permitieran poner en marcha estrategias integrales e individualizadas de gestión del riesgo. Estrategias de gestión del riesgo que evolucionan de manera inteligente con la situación de las personas, la organización, los entorno de trabajo y los procesos.

Esta alianza entre salud, seguridad, tecnología y empresa que propone FASyS como base de productividad, ha identificado los siguientes retos comunes para liderar un salto tecnológico que propicie la aparición y consolidación de nuevos subsectores de actividad:

- Generar una metodología que permita la definición de modelos de excelencia de referencia de fábricas seguras y saludables.
- Crear nuevos métodos y técnicas de identificación y evaluación de riesgos laborales, que permitan el desarrollo de una fábrica centrada en el trabajador, para poder asegurar de manera maximalista el continuo cuidado y protección del trabajador en su actividad.
- Mejorar la calidad de vida del trabajador en el puesto de trabajo.
- Reducir el índice de enfermedad laboral, en particular dolencias musculo-esqueléticas y cardiovasculares mediante el desarrollo de nuevos sistemas de diagnóstico precoz basado en biomarcadores genéticos y vigilancia preventiva.
- Eliminar la alta siniestralidad laboral en la fabricación, a través del diseño de nuevos conceptos en puestos de trabajo, incorporando la gestión activa y pasiva del factor humano en la seguridad.
- Mejorar la salud y bienestar de los trabajadores, a través de programas de intervención, que aborden de manera conjunta organización del trabajo y supresión de estresores.
- Disminuir los impactos en el entorno de trabajo, derivados de las actividades de fabricación como ruidos, contaminación, vibración.
- Mejorar la visibilidad del impacto de la salud y la seguridad en el desarrollo de la actividad de la empresa para poder organizar la gestión de manera efectiva y eficiente.
- Optimizar el uso y diseño de los equipos y procesos de fabricación.
- Fomentar la creación de empleo de calidad, centrado en tareas intensivas en conocimiento, mediante la aparición de nuevas oportunidades abiertas y entornos seguros adaptados a personas con discapacidad o minusvalía.
- Desarrollo de la conciencia de la sociedad y la empresa acerca del valor competitivo de la seguridad y salud laboral integral.
- Posicionamiento diferencial de la industria de fabricación española.

4.3. Arquitectura de FASyS

Basándose en la arquitectura I3WSN, la arquitectura del sistema FASyS está organizada jerárquicamente, cubriendo áreas, zonas y un Centro de Control Global (GCC), como se muestra en la Figura 16. En la arquitectura, un área es considerada como un pequeño lugar de interés donde se han desplegado sensores para controlar una o más características físicas. Una zona es un lugar acotado que agrega varias áreas con el fin de vigilar la situación y los riesgos combinados, y puede requerir la fusión de los datos de las áreas cubiertas. Todos los datos de los sensores recogidos en una zona se almacenan en un SOS local. En cada zona existe un Centro de Control Local (LCC), el cual es el encargado de procesar los datos recogidos, aplicar algoritmos de evaluación de riesgos para detectan un problema potencial o local de riesgo para el trabajador y además reaccionar en tiempo real con un menor tiempo de respuesta.

La agregación de todos los datos de todas las zonas de la fábrica se realiza en el Centro de Control Global, con el fin de detectar los riesgos globales y tomar decisiones globales relacionadas con la seguridad en la fábrica. Está compuesto por varios bloques:

- HMI (Interfaz Hombre-Máquina): proporciona acceso a todo el sistema, lo que permite la configuración del sistema (local y globalmente); la distribución de los trabajadores, los sensores, las áreas, los riesgos, etc. Además de la configuración, los administradores también pueden visualizar información en tiempo real sobre lo que sucede en la fábrica (los niveles de riesgo, las alarmas, la ubicación de los trabajadores, etc.).
- Procesador de eventos: es el encargado de: (i) el seguimiento de todos los datos que se están monitorizando y (ii) que dichos datos concuerden con los criterios de configuración con el fin de detectar posibles riesgos. En la medida que la cantidad de información a procesar es enorme, es necesario un procesamiento de eventos complejos (CEP).
- Actuador: lanza y supervisa las acciones que tienen que llevarse a cabo una vez que se ha generado una alerta por el módulo de procesamiento de eventos.

El CCG también puede ponerse en contacto con otros sistemas y aplicaciones para recopilar información adicional. Los sistemas, aplicaciones o servicios pueden ser internos o externos en función de su disponibilidad en el momento del despliegue. Por un lado, los internos se refieren a sistemas, aplicaciones o servicios existentes que ya están disponibles en la fábrica antes de implementar el sistema, por ejemplo: una fábrica ya tiene una base de datos con información básica y personal de cada trabajador. El GCC puede correlacionar la información proveniente de los sensores (sistema FASyS) y los trabajadores (aplicación interna existentes) para tomar decisiones pertinentes e inferir los posibles riesgos. Por otro lado, los externos son los sistemas, aplicaciones o servicios disponibles en Internet para optimizar o mejorar el rendimiento del sistema. Además, Internet también puede servir como canal de comunicación para el envío de alertas y notificaciones a los trabajadores remotos y administradores.

La organización de fábrica en zonas y áreas depende de su tamaño y de su actividad, por ejemplo, para una pequeña fábrica un área y una zona pueden superponerse y ser idénticas, sólo sería necesario un SOS y ambos LCC y GCC pueden referirse al mismo centro de control. Para una fábrica media, pueden surgir varias posibilidades: un área puede referirse a un área física específica (línea de producción, almacén, oficinas, etc.) o a una zona lógica específica (en la que se ha desplegado una WSN especial porque está siendo monitorizada una característica de especial interés, etc.). Para una gran fábrica que está ubicada en varios lugares, una zona puede referirse a cada localización por separado.

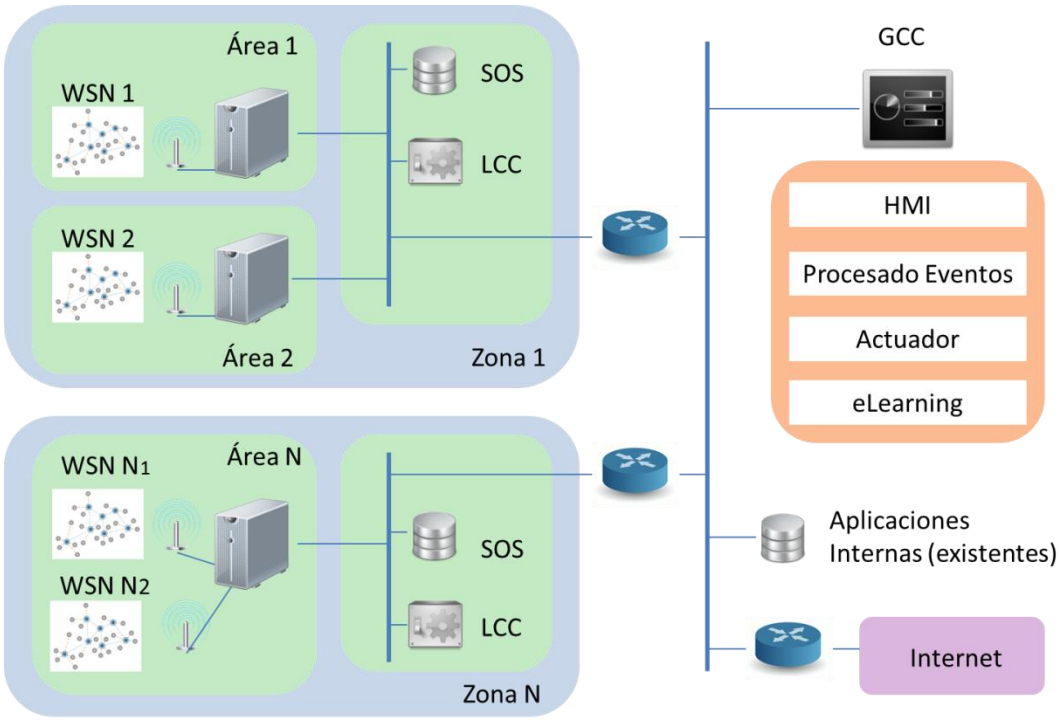

Figura 16. Arquitectura global del sistema FASyS

4.3.1. Arquitectura de comunicaciones

Debido a los requisitos que presentan los distintos escenarios y al diseño comentado, la arquitectura de comunicaciones es una arquitectura heterogénea que integra distintas tecnologías de comunicaciones, con distintas características técnicas, en una única plataforma cubriendo distintas necesidades (tasa de transmisión, latencia, calidad de servicio o fiabilidad).

Dados los distintos subsistemas que forman el sistema FASyS y las diferencias en los requisitos de comunicación de éstos, la arquitectura del sistema FASyS se organiza siguiendo una estructura jerarquizada que converge finalmente en una red de comunicación común o backhaul que ofrece soporte global al sistema. Esto permite que el sistema sea escalable, ya que es capaz de adaptarse a las variantes demandas del entorno industrial, ser flexible y tener la capacidad de auto-reconfigurarse ante cambios en el sistema como la caída de un enlace, o la incorporación de nuevos nodos en una subred.

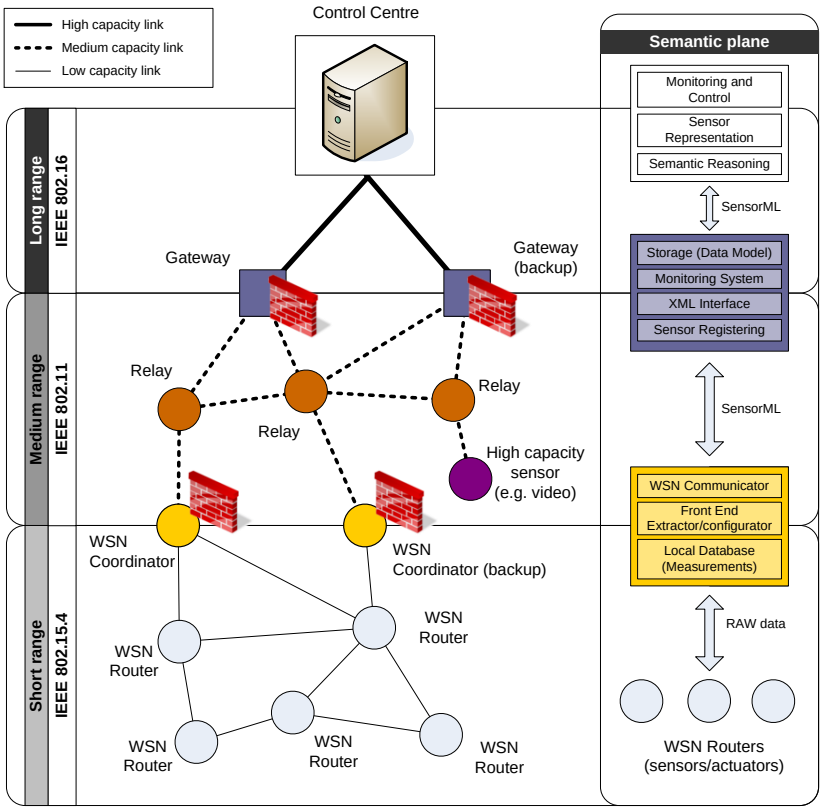

Figura 17. Arquitectura de comunicaciones inalámbricas heterogéneas de FASyS

Una de las propiedades más importantes es que el sistema está diseñado de manera que se garantiza una alta fiabilidad, para lo que es necesaria la introducción de redundancia en el sistema. Por ello, es conveniente utilizar tecnologías de comunicaciones inalámbricas que consideren topologías de red que permitan el nivel de redundancia necesario, como son las topologías de red malladas.

Para la correcta integración de los nodos móviles en la red, es necesaria la gestión dinámica de la topología de la red. Los nodos de la red son capaces de detectar la proximidad de otros nodos para la creación y destrucción de enlaces de comunicación. El establecimiento y mantenimiento de estos enlaces debe ser dinámico y dependerá de la cercanía de los nodos, la cantidad de elementos obstructores e incluso de la cantidad de tráfico de datos a transmitir.

Todas estas características se aplican a los distintos niveles de red que se pueden identificar:

- Red de nivel de Área (red intra-area): corresponde a una o más WSNs y consta de varios sensores de monitorización de una o más características. Este es el nivel de comunicación de red más bajo (nivel de sensor) donde los sensores comunican y alimentan el sistema con datos.
- Nivel de red de zona (red inter-área): esta red conecta varias WSNs con un SOS y un Centro de Control Local (LCC). El servidor correspondiente a cada área envía mediciones al SOS. Por lo tanto, todas las medidas de los sensores dentro de esa área son accesibles a través del SOS mediante un interfaz estándar (SensorML y

O&M). Dependiendo de la forma en que la zona se ha establecido, esta comunicación se puede producir a través de cable o una red inalámbrica.

- Nivel de red de control (red inter-zona): esta red conecta varias zonas próximas y permite la recopilación de toda la información necesaria en el GCC. En contra de los LLC, el GCC debe conocer todas las zonas existentes, ya que se pone en contacto el SOS de cada una de ellas.

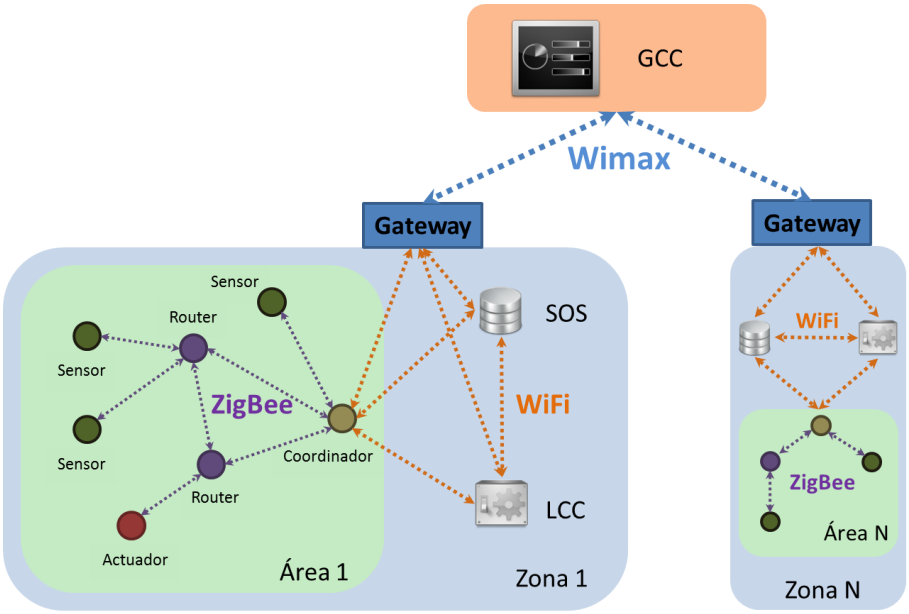

Figura 18. Arquitectura de comunicaciones

Las comunicaciones en FASyS, como en otras aplicaciones industriales que involucran sensores y redes de sensores, se basan en la tecnología inalámbrica debido a la facilidad de despliegue. Pueden coexistir diferentes tecnologías inalámbricas en una fábrica, y especialmente, dentro del sistema propuesto con el fin de dar soporte a comunicaciones de corto alcance, medio o de largo alcance. Las tecnologías inalámbricas COTS incluyen Wi-Fi (IEEE 802.11) y Bluetooth (IEEE 802.15.1), sin embargo, no son especialmente adecuados para entornos industriales, y por lo tanto, su uso es limitado. IEEE 802.11 ofrece altas tasas de datos, del orden de las decenas de Mbits/s y rango de alcance de hasta decenas o centenas de metros, mientras que IEEE 802.15.1 y IEEE 802.15.4 ofrecen tasas de transmisión de solamente centenares de kbit/s a varios Mbits/s con rangos de alcance hasta centenares de metros. Sin embargo, la tecnología IEEE 802.11 consume una mayor cantidad de energía para proporcionar tasas de datos y rangos de alcance mayores, hecho que puede llegar a limitar los beneficios obtenidos por las comunicaciones inalámbricas. En comparación con Bluetooth o IEEE 802.15.4 ofrece velocidades de transmisión más bajas, pero menos consumo de energía (Tabla 2). Como se demuestra en [196], también permite la interconexión de un número relativamente elevado de nodos para la construcción de una topología en forma de malla o mesh, lo que facilita el despliegue de redes flexibles y robustas, con capacidad de adaptación y reconfiguración ante posibles modificaciones del entorno de operación.

En la Figura 18, se muestra la arquitectura de comunicaciones heterogéneas de FASyS para entornos industriales. El enfoque adoptado facilita una implementación jerárquica, escalable y rentable.

Comunicaciones de nivel local

Hay diversas tecnologías basadas en el estándar IEEE 802.15.4, tales como ZigBee [197], WirelessHART [29] y ISA100.11a [30], todos ellos operando en la banda de frecuencias de 2.4 GHz. Las dos últimas tecnologías se han diseñado para soportar entornos industriales, ya que incorporan diversos mecanismos sólidos y fiabilidad. Por otro lado, aunque ZigBee fue inicialmente diseñado para entornos de automatización del hogar, más adelante se mejoró (ZigBee Pro o ZigBee 2007) para cumplir con las necesidades de la industria. Básicamente, ZigBee Pro mantiene las capas física y MAC de IEEE 802.15.4 y proporciona capas de red y aplicaciones con características de seguridad mejoradas.

ZigBee es también una relativamente buena elección tecnológica debido a su mayor disponibilidad, la interoperabilidad y el menor costo. Por lo tanto, por razones prácticas, ha sido elegido ZigBee como tecnología de comunicación inalámbrica base para la implementación en la fábrica. De todos modos, el cambio de una tecnología a otra (como WirelessHART o ISA100.11a) es relativamente transparente para el sistema. En [195] y [198] se ha llevado a cabo un análisis de la implementación WSN en entornos industriales.

ZigBee ofrece comunicaciones de área de corto alcance, incluidos los nodos router, sensores, actuadores y nodos coordinador que llevan a cabo la gestión del WSN. El nodo coordinador se encarga de transmitir los datos detectados a la LLC a través de una red backhaul inalámbrica que cubre tecnologías de medio alcance para las comunicaciones dentro de la fábrica, y las tecnologías de largo alcance para la transferencia de los datos agregados al GCC.

Tabla 2. Comparativa entre los principales estándares inalámbricos que usan la banda ISM [199]

	802.11b	**802.15.1**	**802.15.4**
Ancho de banda (Kbps)	11000	1000-3000	20-250
Alcance (m)	100+	~ 20 (Clase 2) ~ 100 (Clase 1)	20-70, 100+ (amplificador exterior)
Nodos soportados	32	7	2^{64}
Duración de la batería (días)	0.5-5	1-7	100-1000+
Consumo de potencia (en transmisión)	300 mA	45 mA (Clase 2) < 150 mA (Clase 1)	30 mA
Tecnología de espectro ensanchado	DSSS	FHSS	DSSS

Comunicaciones de nivel intermedio

El sistema de comunicaciones de FASyS, requiere el empleo de un nivel de comunicaciones intermedio, para servir de enlace entre la red mallada de comunicaciones a nivel local y el enlace de backhaul con el centro de control. Esta red de nivel intermedio, mejora la escalabilidad del sistema y distribuye el tráfico desde la red mallada hacia el backhaul (y viceversa) por diversos caminos para no saturar ninguno de ellos. Si además, este nivel intermedio lo forma un sistema en forma de malla, dicho nivel intermedio añade una mayor robustez ante caídas de enlaces al permitir reconducir las comunicaciones por caminos alternativos ante cualquier problema en un nodo de red. Por otro lado, el empleo de una tecnología de mayor capacidad de transmisión en el nivel intermedio permite la incorporación de sensores/dispositivos con elevados requisitos de transmisión directamente sobre dicho nivel, como puede ser las cámaras de video.

Las principales tecnologías de comunicaciones inalámbricas que podrían soportar el establecimiento de una red mallada son las enumeradas en la Tabla 3. Los estándares asociados a estas tecnologías han sido desarrollados por el IEEE, y se diferencian fundamentalmente en el ámbito de aplicación para el que fueron diseñadas. Por un lado, IEEE 802.16a es una evolución de IEEE 802.16/WiMAX, diseñado para redes inalámbricas de área metropolitana (MAN, Metropolitan Area Networks) y con una alta capacidad. El estándar IEEE 802.11s evoluciona la norma IEEE 802.11/WiFi para soportar redes malladas con comunicaciones multihop. Esta tecnología está diseñada para redes inalámbricas de ámbito local o corto alcance (LAN, Local Area Networks), y menor capacidad que IEEE 802.16. En tercer lugar, el estándar IEEE 802.15.5 define el nivel de red para la norma IEEE 802.15.4, diseñada para comunicaciones de corto alcance y baja potencia/consumo (PAN, Personal Area Networks).

Tabla 3. Tecnologías de comunicaciones inalámbricas mesh

Estándares comunicaciones inalámbricas mesh	Ámbito de operación
IEEE 802.16a	WMAN
IEEE 802.11s	WLAN
EEE 802.15.5	WPAN

IEEE 802.16 permite mayor alcance, ancho de banda y potencia que IEEE 802.11, y permite el empleo de funcionalidades avanzadas para proporcionar calidad de servicio y seguridad. IEEE 802.16 y IEEE 802.11 fueron diseñados para su empleo en diferentes ámbitos de aplicación. Por un lado, IEEE 802.11 surgió como una tecnología para redes de área local y un servicio best-effort (sin garantías de calidad). Sin embargo, IEEE 802.16 aparece como alternativa para dos grandes aplicaciones propias de operadores de telecomunicaciones, y no de usuarios finales. Por una parte, el IEEE 802.16 está destinado a ser la evolución del LMDS (Local Multipoint Distribution Service) y el MMDS (Multichannel Multipoint Distribution Service) para la implementación de radioenlaces punto a punto. Por otra, IEEE 802.16 es una tecnología adecuada para dar un servicio de acceso fijo, es decir, puede utilizarse como competidor o sustituto de la

red de acceso fija (DSL y cable) en determinados entornos, especialmente en entornos rurales, donde el despliegue de soluciones de cable es muy costoso y los radioenlaces punto-multipunto se presentan como una alternativa flexible y más barata. Dado que, inicialmente las aplicaciones estaban únicamente orientadas a operadores de telecomunicaciones, el estándar IEEE 802.16 permite su uso en bandas de frecuencia con licencia e incluye mecanismos de seguridad y QoS, requisitos obligatorios para servicios comerciales.

IEEE 802.16a incorpora el modo de operación mesh al modo PMP (Punto-Multi-Punto), ya existente en IEEE 802.16, donde la diferencia radica en la posibilidad de establecimiento de redes malladas. IEEE 802.16a opera en bandas con o sin licencia en la franja 2-11GHz, permitiendo comunicaciones con o sin visión directa y de hasta 50km de cobertura. Aunque este rango de cobertura es claramente excesivo para los objetivos de la red de nivel intermedio en la arquitectura FASyS, IEEE 802.16a presenta como principal limitación para el proyecto el hecho de no ser compatibles el modo mesh con el modo PMP.

Por otro lado, el empleo de esta tecnología en el nivel intermedio presentaría inconvenientes adicionales, como el mayor coste de los dispositivos disponibles actualmente, dada su menor cuota de mercado comparada con dispositivos IEEE 802.11, por ejemplo. Al tratar de desplegar redes malladas con un posible gran número de nodos, el aspecto económico podría ser relevante, fundamentalmente si a priori la red de nivel intermedio no requiere de una gran capacidad como la ofrecida por IEEE 802.16a. Por otro lado, es posible que el sistema FASyS requiera sensores de una mayor capacidad de transmisión a la soportada por las tecnologías de bajo consumo y alcance, consideradas para la comunicación de nivel local. Dichos sensores podrían conectarse directamente a la red de nivel intermedio, si soportaran la tecnología de comunicaciones.

El estándar IEEE 802.11s añade el soporte de redes malladas sobre IEEE 802.11, posibilitando comunicaciones multi-salto entre los nodos de la red. La especificación está compuesta de un nuevo conjunto de protocolos para la instalación, configuración y operación de redes malladas basadas en IEEE 802.11. Su implementación se basa en IEEE 802.11a/b/g/n, operando en las bandas 2.4GHz y 5GHz, e incluyendo aspectos como la incorporación automática de los nodos a la red. Además, el estándar IEEE 802.11s soporta el empleo de dispositivos multi-banda, que emplean múltiples radios para aumentar la capacidad de la red. La Figura 19, muestra la arquitectura básica de una red IEEE 802.11s. En esta red, los nodos MP (Mesh Point) son nodos capaces de establecer la red mallada gracias a funcionalidades como el descubrimiento y asociación de nodos vecinos o la selección de canal. Los nodos MAP (Mesh Access Ponit), es un nodo MP que además es capaz de actuar como punto de acceso para dar servicio a dispositivos IEEE 802.11 que no soporten el establecimiento de redes malladas. Estos nodos MAP, podrían ser los encargados de ofrecer conectividad a aquellos sensores de mayor capacidad que requirieran su conexión directa con la red de nivel intermedio. Los nodos MPP (Mesh Portal) son un tercer tipo de nodo MP, a través del cual pueden conectarse varias redes malladas WLAN. Los nodos MPP pueden también operar como

pasarelas y actuar como Gateway entre la red mallada IEEE 802.11s y otras redes. Los nodos MPP podrían servir de pasarela hacia las redes de backhaul y la red mallada local. De hecho, fabricantes como Alvarion tienen ya en su gama de productos dispositivos pasarela combinando interfaces WiFi mesh y WiMAX para la interconexión de ambas tecnologías. Sin embargo, también podrían emplearse nodos IEEE 802.11 tradicionales que implementen las tecnologías de backhaul o red mallada local, y se conecten a la red de nivel intermedio a través de un nodo MAP, en lugar de un MPP.

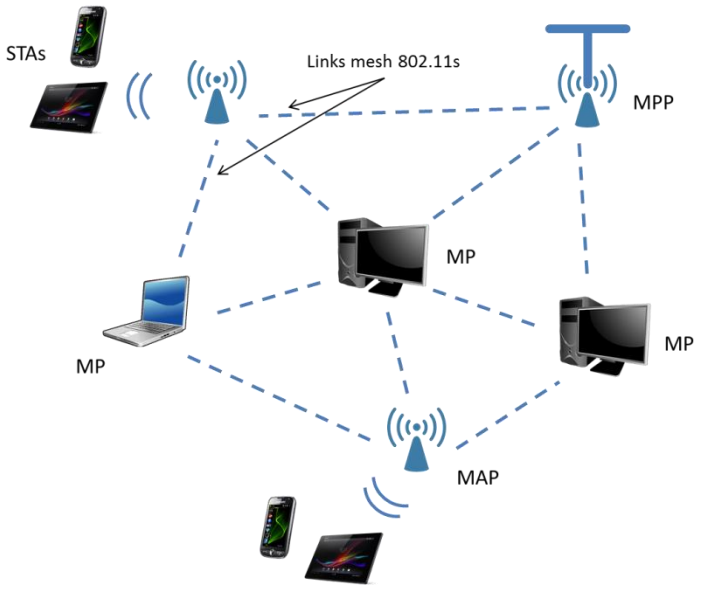

Figura 19. Ejemplo de arquitectura IEEE 802.11s

Comunicaciones de nivel de backhaul

Según los requisitos de los distintos niveles de comunicación definidos en la arquitectura de comunicaciones del sistema FASyS, el nivel de backhaul, es el que proporciona el enlace hasta el centro de control, en el cual, converge toda la información enviada desde y hacia la red mallada de nivel local. En este contexto, además de requerir un sistema con una tecnología de comunicaciones robusta y que proporcione una comunicación fiable, es necesaria la aplicación de una tecnología radio de gran capacidad de transmisión, capaz de dar cabida a todos los flujos de datos que llegan hasta o desde el centro de control.

Las tecnologías de comunicaciones inalámbricas, actualmente, son capaces de proporcionar tasas de transmisión de hasta 124Mbps, en el caso de WiMAX, las cuales son suficientes para su aplicación en el nivel de backhaul del sistema FASyS. Sin embargo, la principal ventaja de las tecnologías inalámbricas es su flexibilidad, ofreciendo la posibilidad de llegar a localizaciones remotas y/o peligrosas a las que es imposible llegar mediante comunicaciones cableadas. Además, en condiciones de entorno, tales como el entorno industrial, el cableado puede degradarse muy rápidamente. Asimismo, otra de las diferencias entre ambas comunicaciones es el coste de instalación y mantenimiento, así como la versatilidad que ambas ofrecen.

WiMAX opera en la banda de frecuencias de 2-11GHz, pudiendo ser utilizado con o sin licencia. Esta tecnología ofrece la oportunidad de trabajar en una banda sin licencia, lo

que implicaría el despliegue de una red propia, con la consiguiente inversión inicial, pero sin costes de contrato que implicaría el uso de una red comercial. En el caso de trabajar en la banda sin licencia, la tecnología WiMAX podrá verse afectada por interferencias de otros sistemas operando en la misma banda de frecuencias.

Por tanto, la tecnología para el nivel de comunicación de control de largo alcance está centrada principalmente en IEEE802.16 (WiMAX), aunque se prevé 3,5 G / LTE para ciertas opciones de conectividad.

4.4. Funcionamiento de FASyS

4.4.1. Fuentes de datos

El primer paso para la monitorización y gestión de una fábrica es conocer el estado de todos los elementos que la componen (ya sean trabajadores, maquinaria, productos, etc.) y del entorno.

Para lograr este cometido, definiremos fuentes de datos como cualquier origen que mantenga un flujo constante (stream) de datos o aquellas que generen la información de una forma asíncrona. Según la arquitectura FASyS, las fuentes de datos se encuentran directamente relacionadas con la tarea de la sensórica, son los elementos de la arquitectura que capturan el estado del entorno y los transmiten a uno o varios sumideros.

En una primera clasificación de las fuentes de datos, se pueden diferenciar en dos bloques: las que generan datos sensibles desde el punto de vista médico, y que no. Esta distinción es relevante, ya que el tratamiento de los datos que tenga algún componente relacionado con información médica, debe tener un tratamiento especial.

Todas las fuentes de datos deben estar registradas para que sean accesibles por parte de la aplicación de monitorización y control. El estándar que se ha elegido para la gestión de estas fuentes es el de OGC, y en concreto se utiliza el servicio Sensor Observation Service. Este módulo se debe instalar en las pasarelas FASYS, para que la aplicación de monitorización y control se encargue de acceder a la misma de forma homogénea.

Cabe destacar en esta situación que la mayor parte de la inteligencia tiene lugar en el nodo coordinador, quien es capaz de detectar en tiempo real, los cambios de estado de los nodos a través de las medidas de los sensores y actuar en consecuencia. Sin embargo, esta manera de proceder adolece de un conocimiento más general y completo de la fábrica.

Se han identificado diferentes fuentes de datos, las cuales deben ser tenidas en cuenta para diseñar la plataforma:

- Sensores físicos: los habrá de diferentes tipos dependiendo de la fábrica y la actividad: químicos, ruido, temperatura, humedad,…
- Sensores de presencia: que detecten en un determinado radio la presencia, o no, de personas, el resultado de dichos sensores es binario, es decir presencia o no.

- Sensores de seguridad: directamente relacionados con el control de acceso, pueden ser de tipo biométrico, con contraseñas, teclados alfanuméricos, lectores de tarjeta. Se emplearán en los casos de uso relacionados con el control de acceso.
- Sensores relacionados con la salud: es un tipo especial de fuente de datos con el que se deberá tener una mayor precaución en cuanto al proceso de intercambio y almacenamiento de datos. Se han seleccionado 3 dispositivos para recopilar datos médicos o biométricos: esfigmomanómetro digital (presión sistólica, presión diastólica y pulso), oxímetro de pulso (SpO2 y pulso), sensores vestibles (ECG, ritmo cardíaco, respiración y aceleración).
- Cámaras de vídeo: esta fuente de datos es especialmente sensible por el hecho de que requiere un ancho de banda grande, y por lo general constante, por lo que es necesario implementar mecanismos de gestión de la calidad de servicio. La información procedente de estas fuentes de datos se emplea por aplicaciones de tiempo real, como la encargada de detectar estado anímico de los trabajadores o la ergonomía.
- Otras fuentes de información son las externas al sistema, que se emplearán en la aplicación de control.

4.4.2. SOS

En el nodo pasarela, es donde residen el servidor SOS y el centro de control local (LCC), y donde se envían todas las mediciones de una zona. El intervalo en el cual cada sensor manda sus medidas se configura y se almacena en el modelo de datos al ser registrado.

El envío de los datos se realiza vía web (HTTP), mediante un mensaje POST como los vistos en el capítulo anterior. La principal información que deben enviar los sensores, además de la propia medida, es la fecha en la que se ha producido, las unidades y la propiedad observada.

A partir de todos estos datos es posible realizar un primer procesado, en el que se puede realizar por ejemplo una fusión de datos de medidas de varios sensores o detectar situaciones a evitar, ya sea mediante relaciones preestablecidas, o mediante algún tipo de razonamiento semántico. En el caso de una arquitectura centralizada, este procesado es únicamente local y se envían los resultados GCC. En caso de una arquitectura distribuida o híbrida, además debe haber intercambio de información entre los distintos LCCs para la toma de decisiones.

La información proporcionada por el SOS son metadatos temporales, metadatos espaciales y metadatos temáticos, en un mensaje XML que sigue el estándar SWE (SensorML, O&M), por lo que es sencillo y flexible acceder a ellos, desde el centro de control u otras aplicaciones en caso de ser necesario.

4.4.3. Modelo de datos

Dada la complejidad de la meta-arquitectura de FASyS, es necesario el diseño de un modelo de datos donde se identifican las entidades más relevantes de cada subsistema y se indican los elementos de información necesarios, así como sus relaciones.

La Figura 20, muestra un esquema general del modelo de datos FASyS, donde se pueden apreciar las principales entidades implicadas en la arquitectura. Desde un punto de vista general, se pueden apreciar una serie de entidades relevantes:

- Trabajador (tabla Worker): representa la información asociada a un trabajador en la fábrica FASyS. Esta información puede ser información general, así como la propia información de la empresa.
- Dispositivo (tabla Device): representa la información asociada a un dispositivo en la fábrica FASyS. Dicho dispositivo puede ser un sensor o incluso una máquina de la fábrica. Interesa su utilización como parte de una red de sensores.
- Tarea (tabla Task): representa las tareas que un trabajador puede realizar en la fábrica FASyS. Dependiendo de dichas tareas y de su información personal (médica), cada trabajador incurre en una serie de riesgos que el sistema debe monitorizar.
- Riesgo (tabla Risk): representa los riesgos principales que se pueden dar en una fábrica; la identificación de dichos riesgos compete a un técnico de prevención de riesgos laborales.
- Área (tabla Area): la gestión de riesgos está relacionada con la movilidad de trabajadores y máquinas, por lo que resulta relevante la definición de áreas para poder acotar las posibles incidencias. Desde un punto de vista de la monitorización y visualización, el concepto de Área también es relevante para poder filtrar actividad, según un área concreta de la fábrica FASyS.
- Alarma (tabla Alarm): representa las alarmas que surgen cuando se detecta un riesgo. Básicamente, se trata de establecer condiciones de riesgo que son detectadas por el CEP.
- Acción (tabla Action): representa las acciones que se deben acometer cuando se detecta una situación de riesgo (alarma), para solucionar un problema o evitar un riesgo y advertir a los trabajadores correspondientes.
- Rol (tabla Rolehmi): Cada uno de los trabajadores puede tener uno o varios roles que le den acceso a las diferentes partes de la fábrica o el HMI. Los roles pueden variar entre trabajador, supervisor, administrador, médico, recursos humanos, etc.
- Puesto de trabajo (tabla Workstation): representa los distintos puestos de trabajo que tiene una fábrica, y en él se indica las tareas que pueden realizarse en ese lugar, las herramientas que dispone, la formación necesaria para poder trabajar allí, sensores disponibles o que trabajadores deben utilizarlo.

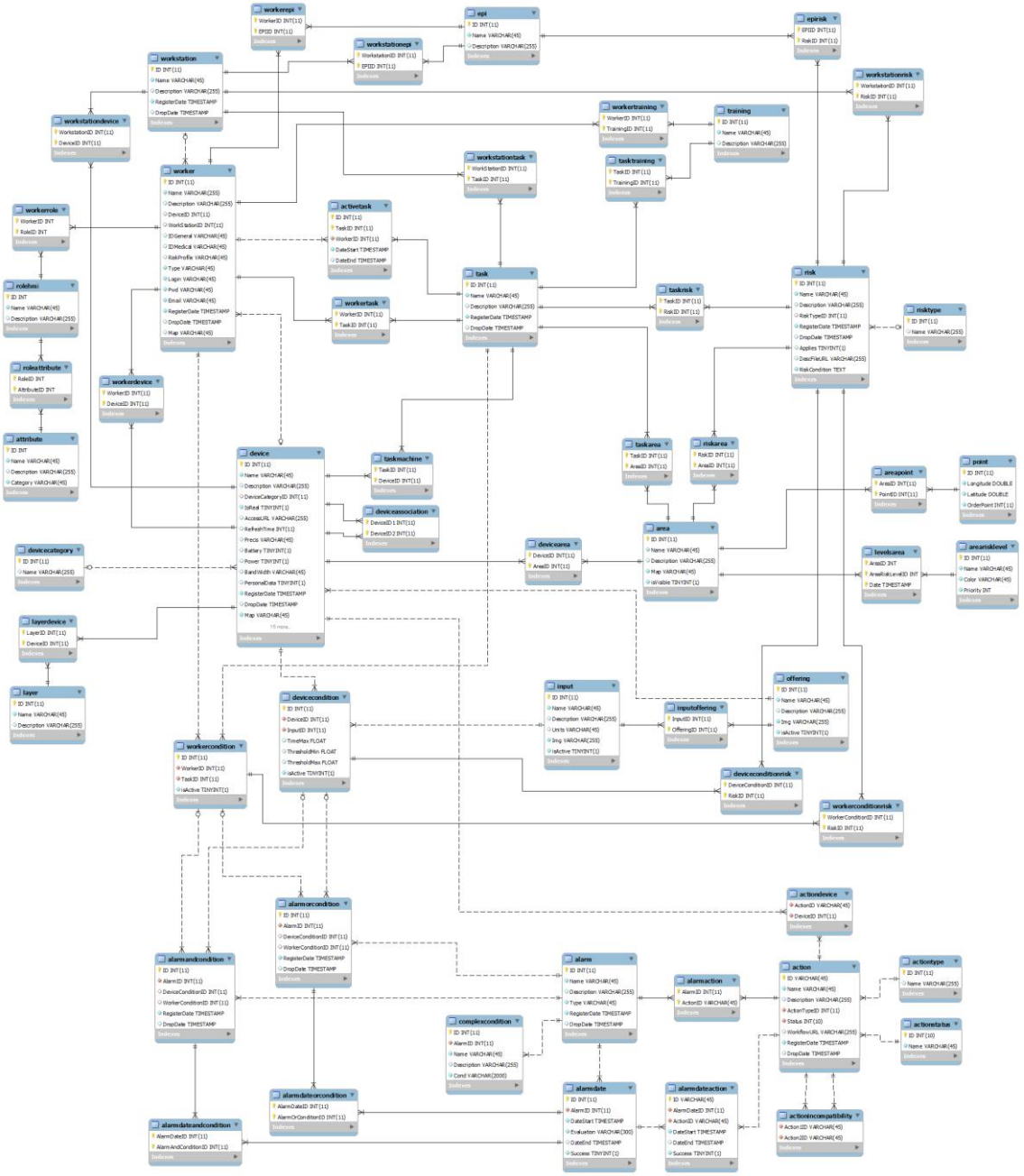

Figura 20. Modelo de datos FASyS

4.4.4. CEP

Uno de los elementos más importantes del Centro de Control es el CEP (Complex Event Processing) donde se procesan grandes volúmenes de datos entrantes o eventos, independientemente de si los datos entrantes son históricos o en tiempo real. Tiene acceso a la información de todos los servidores SOS y, por tanto, disponen de un conocimiento global de la fábrica.

El CEP analiza los datos de eventos en tiempo real, genera una visión inmediata y permite una respuesta instantánea a los cambios en las condiciones. Mientras que las aplicaciones reactivas estándar se basan en reacciones a eventos individuales, el CEP

reacciona a las situaciones en lugar de a los eventos individuales. Una situación es una condición que se basa en una serie de eventos que han ocurrido dentro de una ventana de tiempo dinámica. Estas situaciones incluyen eventos compuestos (por ejemplo, una secuencia), contando los operadores sobre los eventos (por ejemplo, la agregación) y operadores de ausencia.

Algunos de los requisitos funcionales que aborda esta tecnología incluyen el enrutamiento basado en eventos, observación, monitorización y correlación de eventos. La tecnología y las implementaciones de CEP proporcionan medios para definir y mantener la lógica de procesamiento de eventos de la aplicación de forma expresiva y flexible, y en el tiempo de ejecución que se ha diseñado para cumplir con todos los requisitos funcionales y no funcionales, sin que afecte al rendimiento de las aplicaciones, permitiendo la eliminación de una preocupación del desarrollador de aplicaciones y del administrador de sistemas.

La adquisición de datos por parte del CEP se realiza mediante modo pull, ya que el productor de los eventos que consume son los distintos SOS distribuidos en las diferentes zonas, los cuales tienen una operación estándar (vista en el capítulo anterior) que el CEP puede invocar para recuperar medidas.

Los consumidores de eventos son el lugar de destino de los eventos detectados. En la actualidad existen dos tipos de consumidores, como son el HMI y los actuadores. El HMI visualiza las alarmas configuradas cuando se cumplen ciertas condiciones relacionadas con algún trabajador o por una serie de sensores. Los actuadores son los más importantes, ya que son los responsables de llevar a cabo acciones concretas, a partir de los eventos detectados, con el fin de evitar amenazas o accidentes.

Las reglas del lenguaje por las que está compuesto el CEP constan de tres partes:

- Detección de patrones que hacen más relevante un conjunto de eventos, tales como:
    - Secuencia: los eventos necesariamente deben ocurrir en un determinado orden.
    - Agregación: calcular algunas funciones de agregación en un conjunto de eventos entrantes. Por ejemplo, calcular el porcentaje de los eventos de los sensores que llegó con un estado de error de todos los llegados en una ventana de tiempo.
    - Ausencia: no se recibe ningún evento dentro de la ventana de tiempo. Por ejemplo, puede indicar que la fuente está inactiva.
    - Totalidad: todos los eventos especificados deben llegar en un intervalo. Por ejemplo, esperar para obtener los eventos de estado de 4 lugares con datos de nivel de agua, y detectar cuando las reservas totales superan un umbral.
- Conjunto de condiciones (pruebas lógicas) formuladas sobre eventos, así como de datos externo. Estas condiciones pueden ser simples, hacen referencia al valor de un único evento, o complejas, se establecen como operaciones lógicas en los valores definidos sobre un conjunto de eventos de un tipo determinado.

- Conjunto de acciones que se llevarán a cabo cuando todas las condiciones establecidas en una regla están satisfechas. Puede incluir una o más acciones a ejecutar, derivadas de un evento.

Una de las implementaciones de CEP más importantes y la que se ha utilizado en el proyecto FASyS es Esper [200], la cual está disponible para Java y .NET.

Esper junto al lenguaje EPL (Event Processing Language) proporcionan gran capacidad de escalabilidad, un uso eficiente de la memoria, la computación en memoria, utiliza el estándar SQL, una latencia mínima, y con capacidad de procesamiento de Big Data en tiempo real.

Por tanto, se pueden definir fácilmente las reglas para definir patrones a partir de los eventos de entrada, a través de su interfaz gráfico. Además, el resultado se puede visualizar en una única cadena de texto, lo que permite que sea fácilmente almacenable en el modelo de datos.

4.4.5. HMI

El HMI (Human Machine Interface) es el punto en el que personas y computadores se ponen en contacto, transmitiéndose mutuamente tanto información, órdenes y datos, como sensaciones, intuiciones y nuevas formas de ver las cosas. Tradicionalmente al HMI se le ha denominado en aplicaciones y sistemas de control MMI (Man Machine Interface), generalmente basada en la visualización de gráficos de control industrial y elementos de monitorización. El HMI reside en un equipo ubicado en una sala o zona de control, y el mismo mediante una red de comunicaciones especializada interactúa con un ordenador o varios en la zona de planta.

En la actualidad, con el aumento de la utilización de dispositivos COTS, la introducción de redes inalámbricas, dispositivos de bajo coste, mecanismos de interoperabilidad y homogeneización de los protocolos de comunicaciones (ej. redes todo IP), los HMI de los sistemas de monitorización industrial tienen que dialogar y gestionar un mayor número de equipos de forma simultánea, recibir y procesar un mayor volumen de datos y controlar un mayor número de actuadores en planta.

Los principios de diseño del HMI se basan en la sencillez de visualización, la intuitividad en el manejo y la facilidad para la integración de nuevos módulos, pero al mismo tiempo debe incluir todas las capacidades necesarias para la realización de las tareas asignadas. Por ello, se ha empleado una tecnología basada en capas en lugar de en pantallas, que permite según el caso de uso o situación seleccionar las capas necesarias.

Los principales objetivos del diseño del HMI son:

- Proporcionar una interfaz de trabajo eficiente y sencillo para los usuarios del sistema de monitorización y control de FASyS.

- Definir y describir todos los aspectos relacionados con el sistema de monitorización y control, así como de la sala de control y sus equipos, dispositivos personales, señalización de fábrica, etc.
- Proporcionar los mecanismos adecuados para mejorar la percepción de la situación en el puesto de control de la salud laboral.
- Permitir la monitorización en tiempo real de todos los nodos que sean fuentes de datos presentes en la planta de fabricación.
- Monitorización y gestión de los elementos de comunicaciones disponibles en la red, para poder realizar la configuración más adecuada de los mismos.
- Acceso a las fuentes de datos, en tiempo real o histórico, de forma que se pueda hacer una revisión de la información almacenada.
- Diseño de sistemas que sean saludables y se adapten a los criterios de ergonomía y salubridad más exigentes.

El personal de la fábrica tiene múltiples maneras de interactuar con el sistema, a través de un smartphone, una PDA, una tablet o un PC en un puesto de trabajo en planta. Dependiendo del puesto de trabajo y sus requerimientos, se pueden especificar una serie de características para los interfaces gráficos: legibilidad ante el reflejo lumínico, resistencia a los golpes, tamaño reducido, pantalla táctil o alta resolución. Este tipo de interfaces son un valor añadido al sistema de gestión de FASyS y no tienen por qué ser necesarios. La ventaja del desarrollo de aplicaciones basadas en interfaz web es que su adaptación a este tipo de interfaces gráficas no supone un esfuerzo de desarrollo o adaptación excesivo. Además, se ha implementado como una aplicación web, de tal forma, que se pueda acceder a la aplicación de monitorización y control mediante cualquier dispositivo con acceso a Internet a través de un navegador web.

Aplicación real

En esta sección se presentarán algunas de las pantallas reales para su empleo en fábrica, así como su relación con los casos de uso.

Si bien la realización de la aplicación web se podría haber implementado de manera independiente, resulta más útil integrarla dentro de un sistema de gestión de contenidos (CMS, Content Management System). Estos sistemas, permiten crear una estructura de soporte (framework) para la creación y administración de contenidos, principalmente páginas web y aplicaciones sencillas, por parte de los administradores y participantes, aunque es posible definir un diverso número de roles. Ejemplos básicos de CMSs son las wikis y los sistemas groupware.

Los CMS disponen de un interfaz gráfico que permite controlar toda la información referente a la aplicación o sitio web. La información se almacena en varias bases de datos:

- Una o varias bases de datos internas, generan el framework del CMS en cuestión. Estas bases de datos almacenan, entre otros, los usuarios que pueden acceder al sistema y sus respectivos roles.
- Una o varias bases de datos externas, propias a la aplicación web específica que se desea implementar sobre el CMS. Estas bases de datos almacenan básicamente el modelo de datos correspondiente a la aplicación específica que se desea implementar.
- Otras bases de datos, que si bien son externas guardan cierta relación con las bases de datos internas del propio CMS. Corresponde a lo que típicamente se denomina plugins del CMS y se instala como módulo optativo del propio CMS. Algunos ejemplos de esto lo constituyen los foros de discusión.

Una de las ventajas de los CMS, es que permiten separar el contenido del diseño, haciendo básicamente uso de CSS y contenedores web para encapsular contenidos y mostrarlos con un formato u otro. Esto permite administrar más cómodamente la visualización de dicho contenido, incluso generar interfaces diferentes dependiendo del dispositivo. Sin embargo, los límites de esta separación entre diseño y contenido se encuentran en (i) los límites propios del CSS, así como en (ii) la propia aplicación específica. En el caso de FASYS, como se verá a continuación, la aplicación de monitorización y control impone cierta dependencia entre diseño y contenido.

Actualmente existen CMSs desarrollados en software libre y no libre. En FASyS, se ha tomado un CMS libre denominado Drupal [201], escrito en PHP, desarrollado y mantenido por una activa comunidad de usuarios. Drupal es un sistema de gestión de contenido modular multipropósito y configurable que permite publicar artículos, imágenes, u otros archivos y servicios añadidos como foros, encuestas, votaciones, blogs y administración de usuarios y permisos.

El uso de Drupal resulta especialmente útil por los siguientes motivos:

- Drupal es especialmente idóneo para construir y gestionar comunidades en Internet e intranets.
- Su flexibilidad y adaptabilidad, así como la gran cantidad de módulos adicionales disponibles, hace que sea adecuado para realizar muchos tipos diferentes de sitios y aplicaciones web. Algunos de estos módulos adicionales útiles en el marco de FASyS podrían ser los foros y la redirección de usuarios según su rol.
- La gestión administrativa general se puede realizar desde el propio Drupal. Los usuarios y sus roles, por ejemplo, se gestionan de manera nativa desde la aplicación de administración de Drupal. Esto no impide que nuestra aplicación específica disponga de una base de datos con usuarios propios.

Para el caso del proyecto FASyS, se ha tomado la última versión de Drupal (Drupal v7.x) y se ha adaptado el tema Garland a la iconografía FASyS.

Acceso al HMI

El acceso al HMI se realiza mediante autenticación web, con usuario y contraseña, como se muestra en la Figura 21.

Figura 21. Pantalla de login

La autenticación web es la forma más sencilla de login y es comúnmente empleada en aplicaciones web. Los navegadores permiten almacenar dicha autenticación, con lo que el acceso puede resultar inmediato si se configura de esta forma.

Sin embargo, en FASyS se ha empleado un mecanismo de autenticación federado, de forma que se emplean IdPs (Identity Provider) y SPs (Service Provider) capaces de integrar de manera unificada la interacción de trabajadores de diferentes organizaciones, bajo un mismo marco SSO (Single Sign On).

Pantalla de Mapa (supervisión general)

La pantalla de supervisión general está compuesta de tres áreas principales, como se muestra en la Figura 22:

- La parte superior incluye una barra de navegación con una serie de pestañas (Mapa, Capas, Alarmas, Estádisticas, Admin, Salud, Info, etc.) que corresponden a las pantallas principales de operación por parte del administrador.
- La parte central corresponde a la parte de visualización de dispositivos. Se trata de la parte más importante, visual e interactiva. Se pueden distinguir dos zonas:
  - Zona izquierda: esta parte contiene un menú con los componentes de FASYS, categorizados en Áreas, Trabajadores y Dispositivos.
  - Zona derecha: es el área de visualización georeferenciada (incluyendo una escala en la parte inferior derecha) de dichos componentes en la fábrica, donde incluso se puede visualizar los dispositivos asociados a alguna alarma.

- La parte inferior visualiza mediante una tabla todos aquellos eventos y alarmas que se están produciendo en la fábrica. Esta tabla se actualiza en tiempo real, por lo que solamente se visualizan las últimas alarmas generadas.

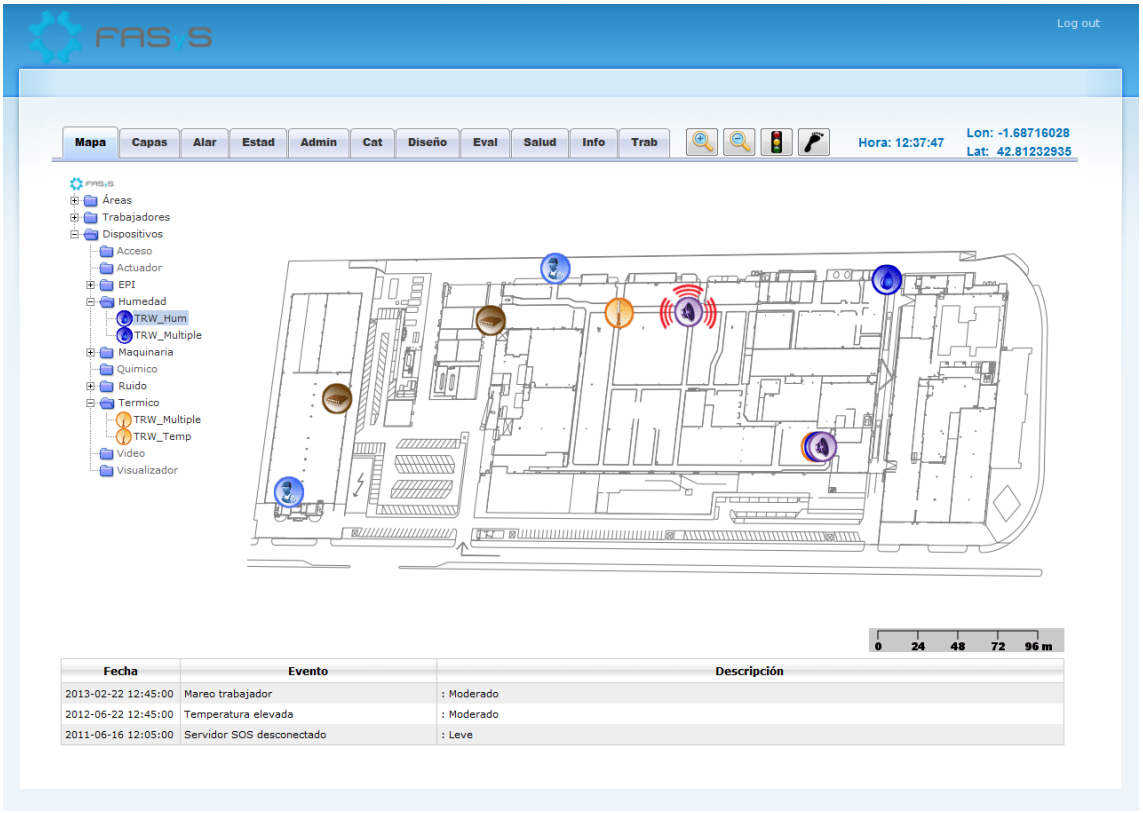

Figura 22. Pantalla de supervisión general

Es importante destacar las funcionalidades del área central. Una de las funciones básicas es acceder a la información de cada uno de los dispositivos disponibles en la fábrica. Para ello, se puede hacer clic directamente sobre el icono del sensor o desde el menú izquierdo podemos navegar por los directorios y hacer clic, por ejemplo, en Dispositivo → Humedad → TRW_Hum. Al hacer clic, sólo se visualiza en el mapa el dispositivo (sensor) seleccionado, denominado TRW_Hum, y se abre una nueva ventana con las características de dicho sensor, como se observa en la Figura 23. En esta nueva ventana se puede ver toda la información del sensor, ya sea se nombre, ID, descripción, tipo, fecha de creación, URL de acceso (en caso de disponer algún servicio, como por ejemplo una cámara de video), posición, últimas medidas tomadas (valores en tiempo real o gráficas con los datos del último día, semana o mes) y alarmas relacionadas con este sensor.

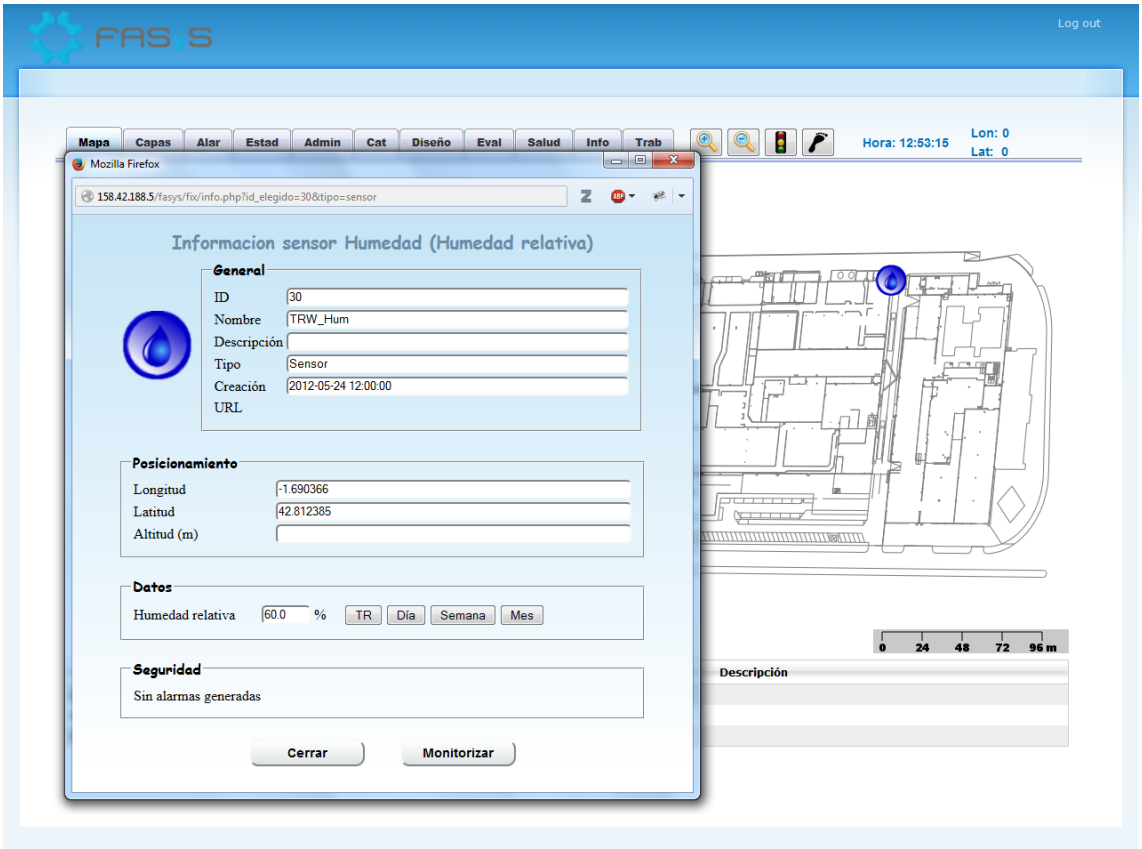

Figura 23. Información de un dispositivo

Desde el menú horizontal superior, se puede acceder a otras de las funcionalidades importantes de la pantalla de supervisión general, con los botones de mostrar trazas y mostrar áreas, además del zoom.

El primero de ellos, (el semáforo), hace visible u oculta todas las áreas de riesgo definidas en el mapa, así como el nivel de riesgo en tiempo real, representando el área con el color de dicho nivel de riesgo (verde, amarillo o rojo). En el caso de no tener ningún nivel de riesgo, no tendrá ningún color. En la Figura 24, se muestra el estado de todas las áreas de riesgo definidas de la fábrica y el nivel de riego correspondiente.

En la Figura 24, también se pueden ver las trazas del movimiento tanto de los trabajadores como de la maquinaria móvil. Con el cuarto de los botones (huella del pie) se hace visible u oculta las trazas de todos los elementos móviles del mapa. Para mostrar la traza de un trabajador en concreto, se debe seleccionar dicho trabajador (o crear una capa personalizada para dicho trabajador) y así queda filtrado para la visualización de la traza, sin que se visualicen el resto de dispositivos móviles. En la figura se puede visualizar la trayectoria que ha seguido el trabajador de la parte superior.

Para visualizar una zona concreta de la fábrica se puede utilizar el zoom de tres formas distintas. La primera de ella, es haciendo clic en los botones de zoom (lupa) para acercarse y alejarse. Además, se puede hacer zoom a una zona haciendo clic con el ratón y arrastrando. Por último, se puede centrar en un área en particular navegando entre las distintas áreas del menú de la izquierda.

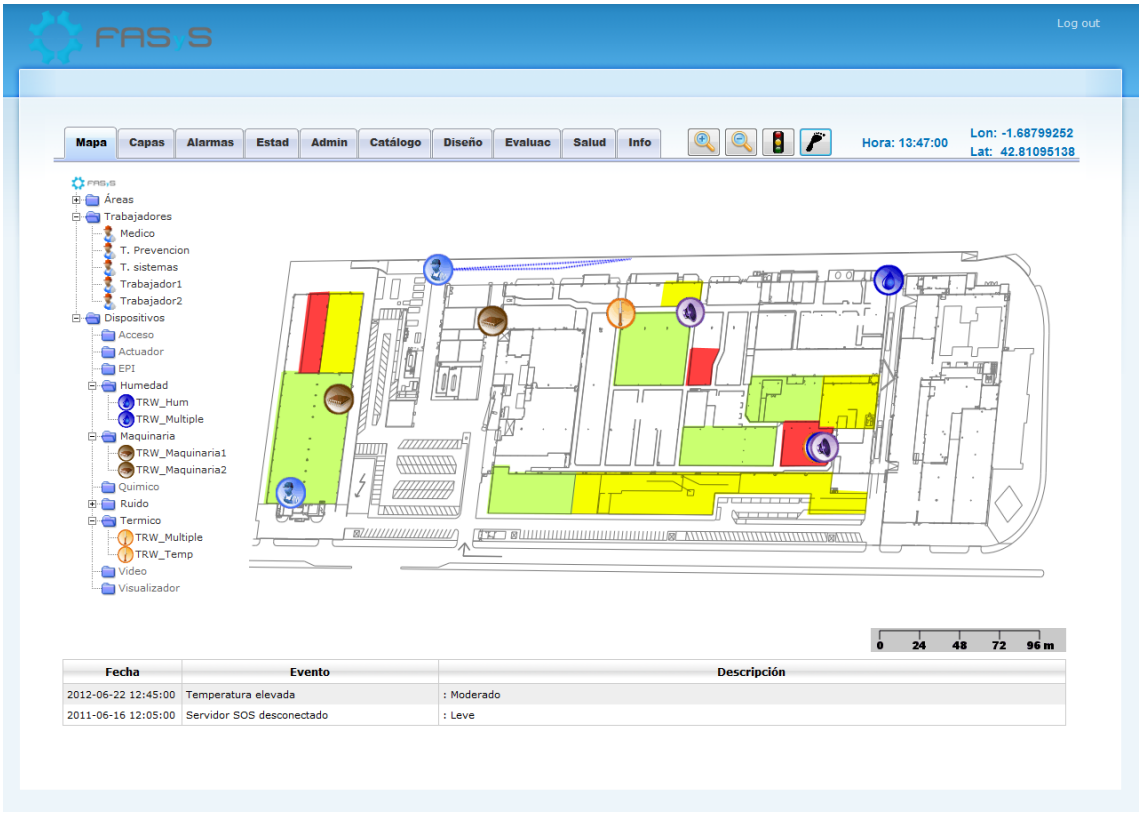

Figura 24. Nivel de riesgo por área y trazas

Menú de capas

La pantalla de capas permite ocultar o visualizar aquellos dispositivos o trabajadores que son del interés del administrador de FASyS, según su perfil. Evidentemente, todos estos dispositivos y trabajadores deben estar georeferenciados para poder ser tratados por la aplicación GIS y, por tanto, representados en la pantalla de supervisión general.

Actualmente los sensores se agrupan de manera lógica. Estos grupos permiten agregar sensores estableciendo una jerarquía superior. Por ejemplo, si disponemos de tres tipos de sensores químicos (aminas, CO, formaldehido) puede parecer lógico agruparlos bajo la misma denominación de sensor químico, de tal forma que todos ellos podrían representarse con el mismo icono en el mapa de supervisión general. Esto no impide que, haciendo clic sobre cada sensor químico en particular, conozcamos el tipo de sensor químico en concreto de que se trata (mediante una ventana emergente como se ilustraba en la Figura 23). También podrían tener un icono específico cada uno en caso de ser necesario.

Para esta fábrica en concreto, se han identificado 10 categorías distintas (ver Figura 25), aunque es posible añadir todas los que se necesiten. Además, es muy interesante poder crear capas personalizadas que permiten monitorizar ciertos sensores o trabajadores de interés, ya sean por zona, actividad o cualquier necesidad.

Además de la distinción de los sensores por categorías, el HMI también soporta la inserción de sensores reales y virtuales. La finalidad de estos últimos es permitir realizar pruebas de simulación con sensores simulados antes del despliegue de sensores reales.

Desde el punto de vista de funcionamiento del SOS y del HMI el resultado es el mismo, puesto que el simulador de sensores se comporta de la misma forma que un sensor real, al enviar datos periódicamente al SOS.

Figura 25. Menú de capas

Menú de alarmas

La pantalla de alarmas permite visualizar las alarmas que se producen en el sistema FASyS. Si bien en la pantalla de supervisión general ya aparece una tabla con las alarmas más recientes, esta pantalla de alarmas resulta mucho más completa y permite un análisis mayor debido a los siguientes motivos:

- El número de alarmas que se muestra es mayor, al disponer de prácticamente toda el área de visualización de la ventana.
- La información que se muestra por alarma es también mayor, ofreciendo datos de los motivos de la alarma y las acciones llevadas a cabo como respuesta.
- El menú de la izquierda permite discriminar o filtrar las alarmas por Áreas, Trabajadores y Dispositivos.

La Figura 26, ilustra la pantalla de alarmas. En ella se puede ver, para cada alarma, la siguiente información: fecha de creación, tipo de alarma, descripción adicional, causa de la alarma, acciones a realizar y el estado en el que se encuentran.

Como se ha comentado anteriormente, el menú de la izquierda permite filtrar las alarmas por Áreas, Trabajadores y Dispositivos. Esto resulta especialmente útil cuando se desea monitorizar algunas zonas concretas (ej. Almacén) o a algún trabajador en particular.

En caso de necesitar un filtrado más específico, es posible realizar combinaciones de búsquedas por área, trabajador, dispositivo y fecha desde el botón de filtrado complejo.

Una vez se dispone de las alarmas que se desea visualizar (ya sea aplicando filtros o no), puede resultar útil exportar esta información a un fichero en PDF, ya sea para imprimir o guardar.

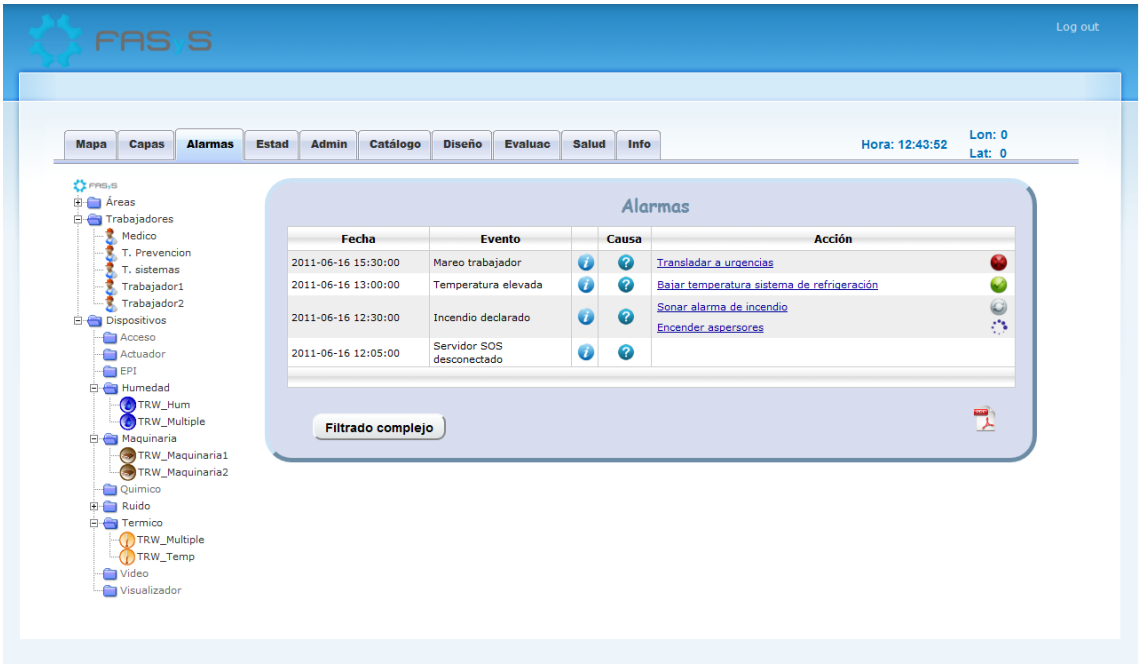

Figura 26. Menú de alarmas

Menú de estadísticas

La pantalla de estadísticas tiene por finalidad dar una visión general del funcionamiento de los elementos más importantes de FASyS, con el fin de poder tomar las medidas más adecuadas.

Desde el menú de estadísticas, se tienen varios botones para acceder a las estadísticas de las observaciones de cada uno de los dispositivos, de los niveles de riesgo de las áreas, de las alarmas generadas o un resumen general de todas las estadísticas.

En la Figura 27, se pueden ver algunos de los ejemplos de estadísticas que muestra el HMI, como son (de izquierda a derecha y de arriba abajo) datos históricos de las observaciones para cada dispositivo en el último día semana o mes, el nivel instantáneo de riesgo en cada área, el nivel medio de riego por área o el nivel medio de la peligrosidad de todas las alarmas.

Figura 27. Menú de estadísticas

4.5. Logros de FASyS

Seguridad en las comunicaciones

La arquitectura de comunicaciones FASyS es una plataforma de comunicaciones que incluye seguridad extremo a extremo. Los requerimientos básicos conseguidos para lograr la seguridad en la arquitectura de comunicaciones son los siguientes:

- Cumplimiento de los objetivos de seguridad: fiabilidad, confidencialidad, integridad, autenticidad, disponibilidad y el no repudio.
- Gestión de la seguridad: mediante la clasificación de activos, clasificación de las tecnologías de comunicación, estudio de amenazas y vulnerabilidades y el análisis de riesgos.
- Cumplimiento con el modelo de seguridad tomando como base los resultados del análisis de riesgos.
- Soluciones de seguridad heterogéneas para entornos de red heterogéneos, ya que la plataforma de monitorización puede acceder a las fuentes de datos con independencia de la red de acceso empleada por las mismas.
- Sistemas de detección de vulnerabilidades que se integra como una capa más del HMI.
- Virtualización de las soluciones, donde se puede instalar más de una máquina virtual en diferentes nodos de la red incluyendo el centro de control.
- Gestión de acceso y autenticación en base a roles: En la gestión de acceso y autenticación de roles nos encontramos ante un escenario en el que debido a la

heterogeneidad de los sistemas/redes así como las diferentes tecnologías de comunicación presentes, hacen de FASyS un escenario complejo de gestionar. Existen distintos roles que permiten acceder al sistema a todo tipo de usuarios de forma segura, a través de una autenticación federada.

Gestión del equipamiento de red

La gestión del equipamiento de red, es uno de los requisitos especificados dentro del proyecto FASyS, ya que es una de las tareas que realiza la plataforma de monitorización y control. La gestión del equipamiento de red se define como el despliegue, integración y coordinación del hardware, software y los elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlar los recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio a un precio razonable.

La gestión del equipamiento de red, permite que en el centro de monitorización y control sea posible obtener información sobre la disponibilidad actual, histórica y planeada. Además la gestión de la red, proporciona estadísticas de operación de la red (ej. tasas de transmisión o paquetes perdidos), así como monitorización de diferentes parámetros y gestión de fallos y alarmas. En el caso de FASyS se entiende como equipamiento de red todos aquellos elementos que sirvan para establecer la arquitectura de comunicaciones, incluyendo los sensores individuales.

- Gestión de configuraciones/cambios, manteniendo información del estado de la red, topología configuración, por ejemplo, información relativa a las subredes existentes, tablas de enrutamiento, etc. Teniendo en cuenta que esta gestión puede ser estática, sólo el administrador puede realizar los cambios, o dinámica en que cualquier cambio en la topología es detectado por la aplicación de gestión del equipamiento de la red y representada en el HMI.
- Gestión del rendimiento y utilización de la red, ya que los niveles de funcionamiento umbrales alcanzables o garantizados por la red de comunicaciones, y por tanto por los equipos que la componen deben ser consistentes. Para ello, se realiza una captura de datos de funcionamiento lo más detallada posible en función de la tecnología empleada, de esta forma es posible la realización de estadísticas por nodo, e incluso por interfaz de cada uno de los equipos integrantes de la red de comunicaciones.
- Gestión de fallos, es una de las tareas fundamentales de la aplicación de gestión del equipamiento de la red, ya que nos determinará la actividad o no de uno o varios de los elementos integrantes de la red. Cuando uno de los fallos se produzca será necesaria la identificación del mismo, para ello, la aplicación realiza sondeos periódicos del estado del equipamiento.
- Gestión de seguridad, aunque esta tarea no está directamente relacionada con la gestión del equipamiento y se desarrollarán en el sistema FASyS herramientas especiales, no deja de ser un requerimiento relacionado con la gestión de red y del

equipamiento de red. Por ello, las herramientas de gestión del equipamiento de red deben ser capaces de controlar el acceso a los recursos de red de una manera bien definida, siendo necesaria la creación de perfiles de seguridad.

4.6. Simulador de redes de sensores

Con el fin de probar la viabilidad y la escalabilidad de un sistema como FASyS previamente a la implantación en una fábrica real, es necesario introducir herramientas de simulación, ya que sería extremadamente costoso desplegar cientos de sensores para replicar cualquier escenario de riesgo potencial. Hay que tener en cuenta que un sistema simulado puede evaluar todo tipo de situaciones así como casos excepcionales o comportamientos a largo plazo, mientras que una fábrica real sólo pueden evaluar algunos riesgos desplegando sensores específicos para cada situación. El uso de herramientas de simulación para entornos de prueba, permite un tiempo de despliegue más rápido, más barato y exento de riesgos [202] [203].

Debido a la importancia de la simulación, ya hay varias herramientas que facilitan el estudio de las redes de sensores, como TOSSIM [204], que es un simulador de eventos discretos, basado en el sistema operativo sensores TinyOS. Otras herramientas para la simulación de eventos discretos son NS-2 [205] (ahora existe también NS-3) y OMNeT ++ [206], que son simuladores de redes de alcance general, totalmente programable y modular, y han sido diseñados para soportar el modelado de grandes redes construidas a partir de los componentes reutilizables del modelo. Otro simulador importante es Globosim, el cual es específico para las redes inalámbricas móviles.

Los simuladores anteriores no se adaptan a nuestras necesidades, ya que ninguno de ellos ha sido diseñado para introducir de forma nativa los datos en el SOS. Actualmente no existe ninguna aplicación disponible que utilice el SOS en cualquier entorno de simulación de sensores. Además, algunos de los sensores modelados en el proyecto FASyS pueden requerir un tratamiento especial, por lo que ha sido necesario desarrollar un simulador propio. El simulador cumple con los requisitos de FASyS, ya que es capaz de simular todos los sensores establecidos en los casos de uso y se pueden simular todos los escenarios posibles a través de las propiedades específicas.

El simulador se desarrolló como Tesina de fin de Master para poder llevar a cabo las simulaciones de todos los sensores que eran necesarios para la fábrica de FASyS. Desde entonces, se ha utilizado para la realización de todas las pruebas dentro del proyecto previas a la prueba final.

Desarrollo

El lenguaje elegido para el desarrollo del simulador ha sido Java, por su portabilidad y su capacidad multiplataforma, lo que permite una fácil integración con otros desarrollos. Además, Java permite gestionar eficientemente el uso de hilos de ejecución, lo cual es

relevante cuando se simula múltiples sensores en tiempo real. Otra razón es que el SOS de 52north también está desarrollado en Java.

Como entorno de desarrollo se ha sido utilizado Eclipse para desarrollar la funcionalidad principal del simulador. Con el fin de facilitar el uso, también se ha añadido una interfaz de usuario gráfica sencilla (GUI) al simulador, desarrollado con NetBeans.

Funcionalidad

El simulador está configurado a través de un archivo XML (llamado conf.xml), que incluye una lista de todos los sensores que se desea simular con su descripción y configuración especificada.

Algunos ejemplos de sensores a ser simulados en FASyS son: los propios trabajadores (alguna propiedad del trabajador, o simplemente su ubicación), sensores de temperatura, de humedad, de sonido, químicos, maquinaria (algunas propiedades de la máquina, o simplemente su ubicación), etc. Para cada sensor se puede especificar los siguientes parámetros:

- Valor mínimo y máximo que el sensor es capaz de proporcionar.
- Periodicidad (con qué frecuencia se envían los datos a la SOS).
- Modo de simulación (seno, gaussiano, exponencial, chi cuadrado, distribución gamma exponencial y al azar.). Este parámetro describe cómo se generan los datos durante la simulación. Además, cada modo es capaz de simular errores de medición de los sensores y anomalías en el medio ambiente.
- Localización (latitud y longitud). Esta propiedad puede ser aleatoria o lineal. El modo lineal define un número de pasos entre los puntos de posición mínimo y máximo y es útil para simular trayectorias en movimiento y colisiones.

Por simplicidad e interactividad, el simulador incluye una interfaz gráfica de usuario, que muestra todos los sensores para simular. El simulador implementado es capaz de generar mediciones de un alto número de sensores, considerando también los errores de medición y anomalías. En la interfaz gráfica de usuario (Figura 28) se muestra básicamente toda la información actualizada referente a los sensores creados. En la tabla se puede identificar el ID del sensor, la propiedad (física) que se mide, la ubicación (longitud y latitud) y la medición actual. Además, se puede ejecutar, detener o pausar cada sensor durante la simulación de forma independiente.

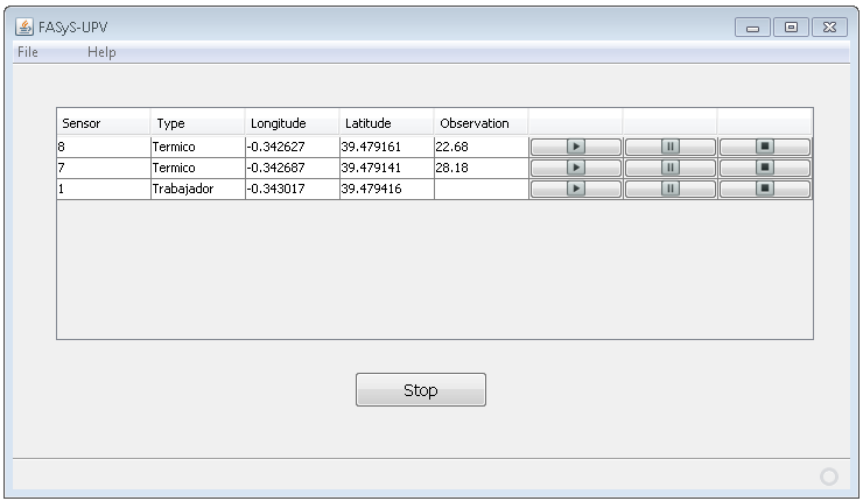

Figura 28. Aspecto del simulador (1)

El proceso de carga de datos se muestra en la Figura 29, donde los datos para alimentar el simulador se cargan del archivo de configuración. Todos los sensores incluidos en el archivo de configuración se muestran en la interfaz, y existe además la posibilidad de añadir nuevos sensores. Cuando se inicia el simulador (al hacer clic en el botón "Run") todos los sensores mostrados empezar a enviar sus mediciones al SOS, y las columnas del interfaz se actualizan cuando varían la longitud, latitud o el valor observación.

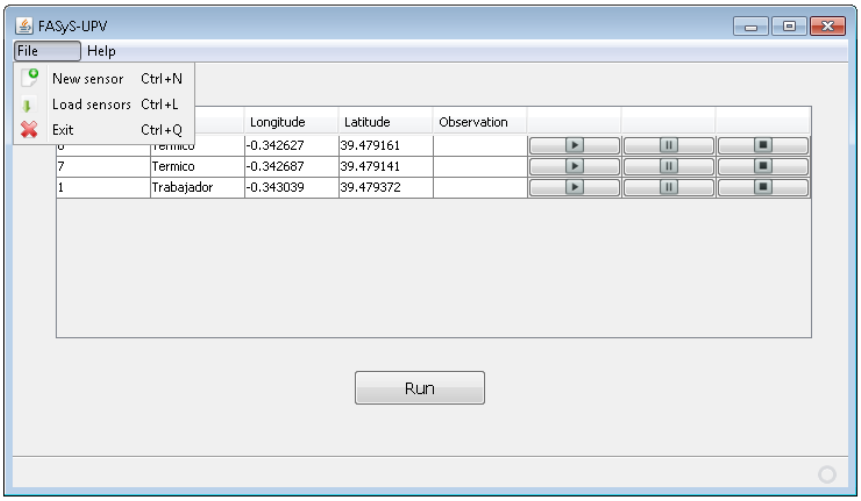

Figura 29. Aspecto del simulador (2)

Los datos generados por el simulador cambian en función del modo de simulación seleccionado. Como se ha comentado anteriormente, es posible introducir anomalías para simular situaciones extraordinarias, tales como un incendio en el caso de un sensor de temperatura, o un ruido excesivo en el caso de un sensor de presión sonora. También se puede definir la probabilidad de error del sensor, siguiendo una distribución particular.

Por ejemplo, en la Figura 30 se muestran los datos enviados al SOS de un sensor de temperatura, que presenta una distribución sinusoidal con una frecuencia de 0,01, una probabilidad de error del 4%, y dos anomalías en los instantes 8 y 44, lo cual representa variaciones elevadas de temperatura que se deberían evaluar. Otro ejemplo es la Figura

31, que representa un sensor de presión sonora con las mismas características que el anterior.

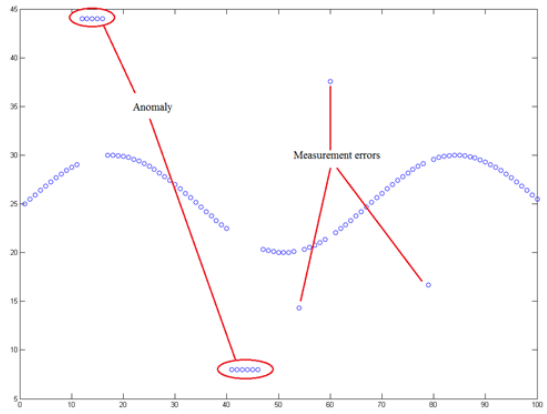

Figura 30. Ejemplo de datos de un sensor (1)

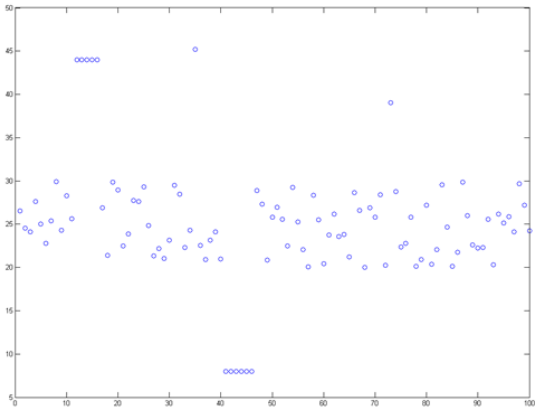

Figura 31. Ejemplo de datos de un sensor (2)

5. Caso 2: UniverSEC

5.1. Introducción

El smart grid integra la evolución de la ingeniería eléctrica y los avances en las TIC para recabar información, con el fin de mejorar la eficiencia, fiabilidad, ahorro de costes, la sostenibilidad de la producción y distribución de energía eléctrica [207]. La energía es un área estratégica en todos los países desarrollados, por lo tanto, el smart grid se investiga en todas las etapas de su estructura y arquitectura, incluyendo la generación de electricidad [208] [209], la transmisión [210] [211], la distribución [212] [213] y el consumo [214] [215]. El desarrollo del smart grid como mejora de las redes eléctricas actuales, es crucial para el logro de objetivos comunes como la seguridad energética y la fiabilidad, el desarrollo económico e incluso la mitigación del cambio climático.

Con el fin de mantener la seguridad en un sistema como el smart grid, el proyecto UniverSEC plantea el desarrollo de un sistema de monitorización y gestión capaz de controlar el aseguramiento de cada uno de los elementos que lo componen.

En esta primera sección del capítulo, se comentan algunos conceptos relacionados con los sistemas de gestión e infraestructuras críticas. En la segunda sección, se presentan los objetivos principales que intenta lograr el proyecto UniverSEC. En la tercera sección, se visualiza la arquitectura con la que se ha llevado a cabo el proyecto, y en la siguiente sección, el funcionamiento más detallado de todas sus partes. Por último, se enumeran los logros que ha conseguido el proyecto.

5.1.1. Infraestructura crítica

Las infraestructuras críticas (IC) son el conjunto de recursos, servicios, tecnologías de la información y redes cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales [216]. La normativa española considera doce sectores críticos: administración, agua, alimentación, energía, espacio, industria química, industria nuclear, instalaciones de investigación, salud, sistema financiero y tributario, tecnologías de la información y las comunicaciones y el transporte. En España, es el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) [217], el órgano encargado de impulsar, coordinar y supervisar todas las actividades relacionadas con la protección de las infraestructuras críticas españolas.

La importancia de proteger de forma adecuada los sistemas TIC de las infraestructuras críticas [218] [219], como el smart grid, ha crecido en relación directa al aumento del despliegue de las mismas, su vulnerabilidad y el impacto de un ataque a las mismas [220]. En el caso del smart grid, en el que se centra este caso de uso, su criticidad ha ido creciendo conforme lo ha hecho la penetración de las redes y sistemas de transmisión y distribución eléctrica en todo el mundo. Hay que tener en cuenta que cuando un sistema se hace más grande y aumenta el número de interconexiones entre los distintos elementos que la componen, el número de amenazas también crece proporcionalmente. La seguridad en sistemas grandes, tales como las infraestructuras críticas, no se puede aplicar en forma de parche que se añade cuando aparecen nuevas vulnerabilidades, sino

que debe ser una prioridad en la fase de requisitos y el diseño inicial de la arquitectura. En la actualidad, independientemente de los ataques físicos, la mayor parte de las amenazas identificadas contra infraestructuras críticas están relacionadas con los ataques cibernéticos, por lo tanto, es obligatorio un sistema que cuente con un alto nivel de seguridad cibernética [221] [222].

La protección de las infraestructuras críticas depende del conjunto de herramientas, políticas de seguridad, perfiles, conceptos, salvaguardas, mecanismos de evaluación de riesgos, acciones, formación, definición de buenas prácticas, grado de garantía de seguridad y tecnologías que pueden ser utilizadas para proteger las redes de comunicaciones, los sistemas de información y la información almacenada [223]. Todos estos activos requieren (incluso en ocasiones por imperativo legal), un nivel de protección adecuado por parte de la empresa u organización. Básicamente, es necesario disponer de los elementos adecuados para garantizar la confidencialidad, integridad y disponibilidad de los activos, entendiendo por:

- Confidencialidad: El acceso a los activos de una empresa u organización estará reservado únicamente a aquellos miembros de la empresa autorizados por la dirección y por la legislación vigente.
- Integridad: Los activos, especialmente la información, no deben ser manipulados, modificados o eliminados, salvo por aquellos miembros de la organización autorizados para ello.
- Disponibilidad: Los activos deben estar accesibles para cualquier miembro de la organización autorizado en cualquier momento.

5.1.2. Sistema de Gestión de la Seguridad de la Información

Los SGSI (Sistema de Gestión de la Seguridad de la Información) son herramientas de gestión que permiten conocer, gestionar y minimizar los riesgos que atentan contra la seguridad de la información de una empresa. Inicialmente, es necesario diferenciar entre seguridad informática y seguridad de la información. La seguridad informática se refiere a la protección de las infraestructuras de las tecnologías de la información y comunicación que soportan el negocio, mientras que la seguridad de la información se refiere a la protección de los activos de información fundamentales para el éxito de cualquier organización. Un SGSI, permite a la empresa:

- Analizar y ordenar la estructura de los sistemas de información.
- Facilitarla definición de procedimientos de trabajo para mantener la seguridad.
- Ofrecer la posibilidad de disponer de controles que evalúen la eficacia de las medidas llevadas a cabo.

Los riesgos de un sistema bajo análisis pueden ser identificados, gestionados y minimizados, pero nunca podrán ser erradicados del todo. Es aquí donde entra en juego un SGSI, debido a que la protección de los activos de información debe diseñarse tras

un profundo análisis de dichos activos de los que dispone una empresa. Fruto de este análisis se catalogarán en función de lo críticos que sean para la consecución y continuidad del negocio. Un SGSI por tanto, servirá para proteger a una organización frente a amenazas y riesgos que puedan poner en peligro la continuidad de los niveles de competitividad, rentabilidad y conformidad legal necesarios para alcanzar los objetivos de negocio.

Además, se trata de una herramienta dinámica que evoluciona en el tiempo, puesto que tanto los activos de información, los riesgos, las necesidades de la empresa, así como los demás factores que cubre el sistema son dinámicos. En este sentido, los SGSI son sistemas de gestión PDCA (Plan-Do-Check-Act), en español se conocen como: planificación, ejecución, seguimiento y mejora:

- Planificación: Se estiman las medidas que se van a implantar en función de las necesidades detectadas, en este sentido, se realiza un Análisis de Riesgos que valore los activos de información y sus vulnerabilidades. Se define la gestión de dichos riesgos y se establecen una serie de controles para reducir su vulnerabilidad a un mínimo asumible por la empresa.
- Ejecución: Después se implementan estos controles. Se incluye en esta fase la concienciación y formación del personal.
- Seguimiento: Se evalúa la eficacia y el éxito de los controles implantados. Hay que contar con registros e indicadores que provengan de estos controles.
- Mejora: Se lleva a cabo el mantenimiento del sistema, Se corrigen o mejoran los puntos débiles detectados durante la fase anterior. Se cuenta con tres tipos de medidas: correctoras, preventivas y de mejora.

Figura 32. Ciclo de Deming (PDCA)

En la actualidad no existe ningún SGSI que realice la valoración del cumplimiento de las normas en tiempo real, es decir valorando de forma continua y no en un instante puntual que los criterios y métricas definidos se cumplan. Es por ello, que en el proyecto UniverSEC se pretende conseguir la evaluación del nivel seguridad en tiempo real.

5.1.3. Aplicación de un SGSI

Uno de los métodos más difundidos entre las empresas para implementar un SGSI es implantar dicho sistema mediante la serie ISO/IEC27000. La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). Proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

En dicha serie, se presentan las mejores prácticas identificadas en seguridad de la información orientadas a desarrollar, implementar y mantener las especificaciones para los SGSI. Dentro de esta serie de normas las más relevantes son: ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC27003 e ISO/IEC27004.

En España, el estándar más extendido para la gestión del riesgo de la seguridad de la información es el ISO/IEC 27001, correspondiente a la familia de normas ISO/IEC 27000. En esta norma, se indica que debe implementarse un sistema de gestión de riesgos que cumpla con determinados requerimientos, pero no se indica la metodología ni herramientas a utilizar. La norma ISO/IEC 27005 establece una guía metodológica a tales efectos.

5.1.4. Security Assurance

La garantía de seguridad o Security Assurance (SA) se define, según el Common Criteria, como la confianza objetivo que una entidad debe alcanzar para cumplir los requerimientos de seguridad fijados para la realización de sus actividades y mantener la confidencialidad, integridad y disponibilidad de la información y los servicios proporcionados por los sistemas de información basados en TI. La confianza es un concepto subjetivo, que debe traducirse en una evidencia medible y verificable que pueda ser recogida y obtenida del sistema objetivo bajo observación y mostrada al operador, administrador o cliente, y se basa en la utilización de técnicas de evaluación del aseguramiento como métodos formales, testeo o revisiones por empresas especiales de auditoría. Sin embargo, en la actualidad no existe ningún método, técnica o mecanismo que evalúe y gestione el nivel de SA en un sistema grande (teniendo en cuenta la escalabilidad) y complejo (diferentes tipos de servicio y actividad). Existen diferentes metodologías estándar relacionadas con la evaluación de la seguridad, como: ISO 17799, ISO 15408 y la más reciente ISO 27004. Pero ninguna de ellas es aplicable a grandes sistemas que tienen carácter distribuido y que empleen sistemas de comunicación heterogéneos, como por ejemplo, los que protegen las infraestructuras críticas, focalizándose más en el análisis y evaluación de las organizaciones y los pequeños sistemas.

Un elemento clave en la evaluación de la garantía de seguridad es el perfil de garantía o Assurance Profile (AP) que es una formalización de las necesidades en el que los proveedores de equipos, proveedores de soluciones, integradores de servicios, operadores y proveedores de servicios pueden definir un conjunto común de medidas de

garantía de seguridad en un objetivo para la medición. El concepto del perfil de garantía de seguridad, así como sus diferentes componentes están en fase de estandarización en la ETSI desde finales de 2011, habiendo sido presentada la propuesta por parte de los investigadores del proyecto Bugyo Beyond [224].

La evaluación del nivel de garantía de seguridad no es la evaluación del análisis de riesgos, es ir un paso más adelante. Existen herramientas que analizan vulnerabilidades, puertos abiertos, parches no instalados e incluso ataques específicos a un determinado sistema operativos. Pero ninguna de ellas tiene en cuenta la combinación y composición de los diferentes elementos que puede hacer que el nivel de seguridad de una organización sea reducido, por lo tanto, una metodología apoyada por un sistema distribuido de monitorización y evaluación que proporcione una medida cuantitativa además de cualitativa, es absolutamente necesaria para modificar el modelo de negocio existente en el ámbito de los SGSI.

Actualmente no existen herramientas que evalúen de forma automática la garantía de seguridad. Toda herramienta que realice la evaluación del grado de garantía de seguridad requiere de las siguientes actividades:

- Técnicas de modelado capaces de capturar las propiedades de las estructuras de los sistemas relevantes para la valoración del SA.
- Métodos para la medida y evaluación de la fortaleza del SA de las entidades de los diferentes sistemas con respecto a las características analizadas.
- Definición de un conjunto de atributos relativos al SA que se puedan mapear en métricas específicas para el SA.
- Definición de un conjunto de métricas del SA.
- Métodos de agregación de resultados de evaluación de entidades individuales, incluyendo otros factores que sean evaluables por parte del monitor del SA.
- Mecanismos y herramientas de presentación, evaluación y generación de informes de la evaluación.

5.2. Objetivos de UniverSEC

El proyecto UniverSEC ha tenido como objetivo principal, el desarrollo de una arquitectura de sistema SGSI extendido que permita además de la evaluación del cumplimiento de los parámetros de las normas de seguridad en sistemas de información, proporcionar información cuantitativa relativa a la garantía de la seguridad, todo ello, en tiempo real. Este objetivo general se desglosa en los siguientes objetivos específicos:

- Superar el nivel actual de seguridad de las tecnologías de la información y de sus herramientas, incluyendo además de la evaluación de los parámetros clásicos, los perfiles y métricas directamente relacionados con la evaluación de los niveles de confianza en la seguridad o aseguramiento de las organizaciones analizadas.

- Desarrollar métricas propias en correlación con los mecanismos de normalización y certificación relacionados, patrones de métricas, patrones de evaluación y soporte al modelado de mecanismos de aseguramiento como la herramienta propuesta en el prototipo.
- Desarrollo de algoritmos y herramientas para la evaluación continua en tiempo real de la eficacia de las salvaguardas y su contribución al nivel de seguridad global y de cada uno de los activos de información, en la infraestructura TIC de una empresa, incluyendo medios y mecanismos de comparación e intercambio de información de seguridad y aseguramiento entre diferentes operadores, incluyendo la propuesta de estandarización de las medidas y los niveles agregados.
- Monitorización continua, objetiva y eficaz del nivel de seguridad global del SGSI y de cada uno de los activos de información de una empresa, considerando elementos dinámicos y movilidad, teniendo en cuenta la inclusión de infraestructuras ubicuas y el despliegue semiautomático de sondas de medida para realizar la captura de datos..
- Demostrar los avances del proyecto en una medida a gran escala, en un dominio como es la protección de infraestructuras críticas, en concreto el smart grid. El sistema se valida mediante la utilización del puesto de mando de gestión de seguridad y las diferentes sondas desplegadas para la captura de datos en crudo y posterior análisis.
- Contribuir a la mejor protección de infraestructuras de información y comunicaciones, introduciendo mecanismos de comparación de los niveles de seguridad de las infraestructuras interconectadas, permitiendo generar mejores modelos de riesgos cuando los sistemas sean heterogéneos e interconectados.

5.3. Arquitectura de UniverSEC

El diseño de la arquitectura debe ser la estructura base que pueda solucionar todos los requerimientos actuales y pueda soportar la evolución de éstos con el transcurso del tiempo de forma satisfactoria. Debe cumplir todos los requisitos ya sean funcionales o no funcionales, tales como calidad, seguridad, disponibilidad eficiencia, rendimiento, etc. Para el diseño de la arquitectura es importante tener en cuenta a los usuarios finales del sistema, los objetivos y requisitos funcionales, y la metodología que se va a aplicar.

Las principales ventajas que aportan el uso de una arquitectura son:

- Definir la estructura para que todas las partes interesadas definan sus necesidades. Tanto el operador de la red como el fabricante de los dispositivos pueden definir requisitos para la definición de la arquitectura.
- Separar distintas tareas y objetivos de manera que se reduzca la complejidad y se pueda abordar cada parte por separado. Hacer varios bloques interconectados permite distribuir el desarrollo y hacerlo de forma más sencilla.

- Mejorar la calidad del sistema gracias a la tolerancia a fallos, compatibilidad, escalabilidad, disponibilidad o seguridad. El disponer de bloques más pequeños permite identificar fallos más fácilmente.
- Facilita la reutilización de arquitecturas estándar debido a problemas recurrentes. Si se diseña la arquitectura de forma genérica, puede ser más adelante en problemas similares.

A partir de la arquitectura genérica I3WSN vista en el capítulo 3, podemos ver que el sistema de SA de UniverSEC consta de dos componentes principales, el Centro de Control (CC) y el Sistema de Medida (SM). El CC evalúa toda la información y ofrece un interfaz gráfico de usuario para el sistema de aseguramiento de seguridad de UniverSEC, mientras que el SM se encarga de la recogida continua de la información requerida en la garantía de la seguridad del sistema observado por el CC. Ambos trabajan juntos para mantener, en tiempo real, la evaluación de la garantía de la seguridad de una infraestructura de energía, de acuerdo a un modelo específico de ésta, una política de seguridad operacional y una garantía de referencia. La Figura 33 muestra una visión general de alto nivel del sistema UniverSEC y sus principales componentes, los cuales se describen con más detalle en los siguientes apartados.

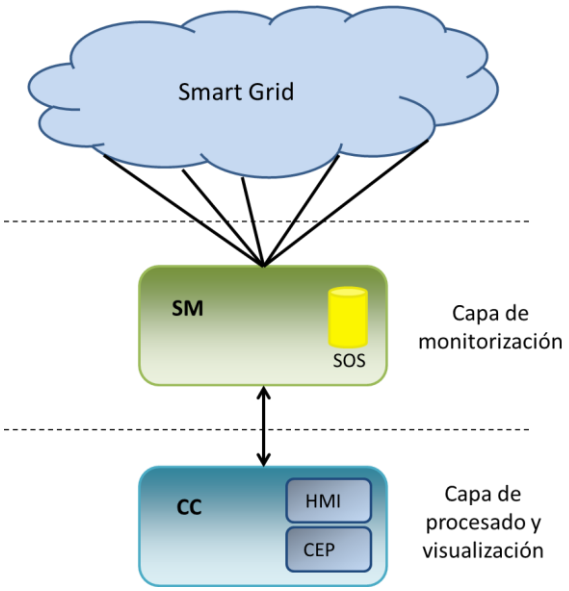

Figura 33. Arquitectura global del sistema UniverSEC

El enfoque del modelo se basa en una clara identificación de las amenazas y contramedidas desplegadas en el smart grid para obtener sistemas seguros y fiables.

Con la arquitectura se pretende proporcionar una visión global del sistema de UniverSEC, de manera que se muestren claramente los componentes que lo forman, así como la infraestructura de control y comunicación.

5.3.1. Sistema de Medida

El Sistema de Medida tiene la siguiente función: reunir y proporcionar las medidas base necesarias para la evaluación de la garantía de la seguridad en el Centro de Control. La principal evolución en el proyecto UniverSEC, consiste en procesar las mediciones requeridas por el Centro de Control para abordar explícitamente las exigencias necesarias para la realización de medidas de garantía de la seguridad en tiempo real. En relación con los objetivos del proyecto, están dirigidos especialmente a la evolución dinámica de la infraestructura, así como a la evolución dinámica de los requisitos de medición sobre el ciclo de vida del sistema.

El SM proporciona las diferentes medidas y eventos relacionados, tanto con datos como con la infraestructura del sistema, que solicite el CC. Los eventos relacionados con la infraestructura pueden ser, por ejemplo, la pérdida o la adición de objetos al sistema (sondas).

También debe conocer la topología de sondas de medidas (su tipo, la ubicación, sus medidas y la fiabilidad/calidad), la topología de servicios (dónde recoger las mediciones, o desplegar una sonda específica para un dispositivo). Básicamente, es responsable de establecer el vínculo entre las solicitudes CC y las sondas de medición.

Hoy en día, cada una de las redes de sensores son sistemas desarrollados para resolver un problema específico, y por tanto, suelen ser sistemas propietarios que dificultan la interoperabilidad con otros sistemas a la hora de añadir nuevos sensores o compartir datos. Por tanto, el sistema diseñado debe utilizar un método estándar a la hora de:

- Descubrir nuevos sensores.
- Configuración de los sensores de forma remota.
- Determinar las la propiedades que mide cada sensor y la calidad de las medidas.
- Acceder a las observaciones en tiempo real y a datos históricos.
- Capacidad de hacer filtrado a pedir datos.

Por ese motivo, para la arquitectura de UniverSEC se utiliza el SOS de SWE como repositorio estándar en el que almacenar todas las medidas base del SM, ya que al basarse en estándares pueden insertar datos sensores de cualquier fabricante, y se puede acceder a las medidas fácilmente.

5.3.2. Centro de Control

La función principal del Centro de Control (CC), es proporcionar una visión global centralizada del estado del security assurance del sistema a monitorizar para el usuario. El CC tiene que proporcionar características de modelado del security assurance avanzada y una herramienta de monitorización. Además de modelar el security assurance, incluye funciones relacionadas con la obtención de datos inteligentes, almacenamiento, combinación, agregación, y, finalmente, la presentación de la medición de la garantía de la seguridad y su evaluación [225].

La centralización de toda la información de seguridad de los activos TIC de una infraestructura, como es el caso del smart grid en un único punto de control, facilita la evaluación y el soporte a la toma de decisiones. Adicionalmente, ya que la información es suministrada al centro de control en tiempo real desde los diferentes elementos de la infraestructura crítica (ej. elementos de red, servidores, contadores de luz inalámbricos, etc.), se puede determinar la existencia de riesgos, el cumplimiento de las normas, la valoración de la garantía de seguridad y la posibilidad de tomar acciones correctivas en tiempo real. La obtención de información en tiempo real, se realiza mediante la utilización de sondas específicas o mediante la interoperabilidad con sistemas previamente instalados.

El CC se encuentra en contacto directo con el usuario final del sistema, ya sea el administrador o el supervisor del smart grid. Además, interactúa con el Sistema de Medida, el cual, le proporciona una capa de abstracción para la recogida de los datos proporcionados por las sondas.

Aunque el CC es el responsable de la gestión y evaluación del modelo de aseguramiento de los servicios supervisados, no tiene conocimiento de la infraestructura de medición: el tipo de sondas, su ubicación y características. El CC define un conjunto de indicadores y proporciona un conjunto de definiciones de medición necesarios, para la evaluación global de la garantía de seguridad del modelo.

El CC se compone de dos elementos principalmente: un interfaz gráfico o HMI y un motor de monitorización del nivel de garantía de seguridad o CEP.

5.4. Funcionamiento de UniverSEC

La sección anterior describe la arquitectura general del sistema propuesto, ahora se explica de forma más detallada la aplicación de esta arquitectura al smart grid. En la Figura 34 se representa una vista más detallada de los componentes principales y bloques que los componen. Se pueden identificar tres etapas principales: obtener información del smart grid, entender y almacenar la información y procesar y mostrar resultados.

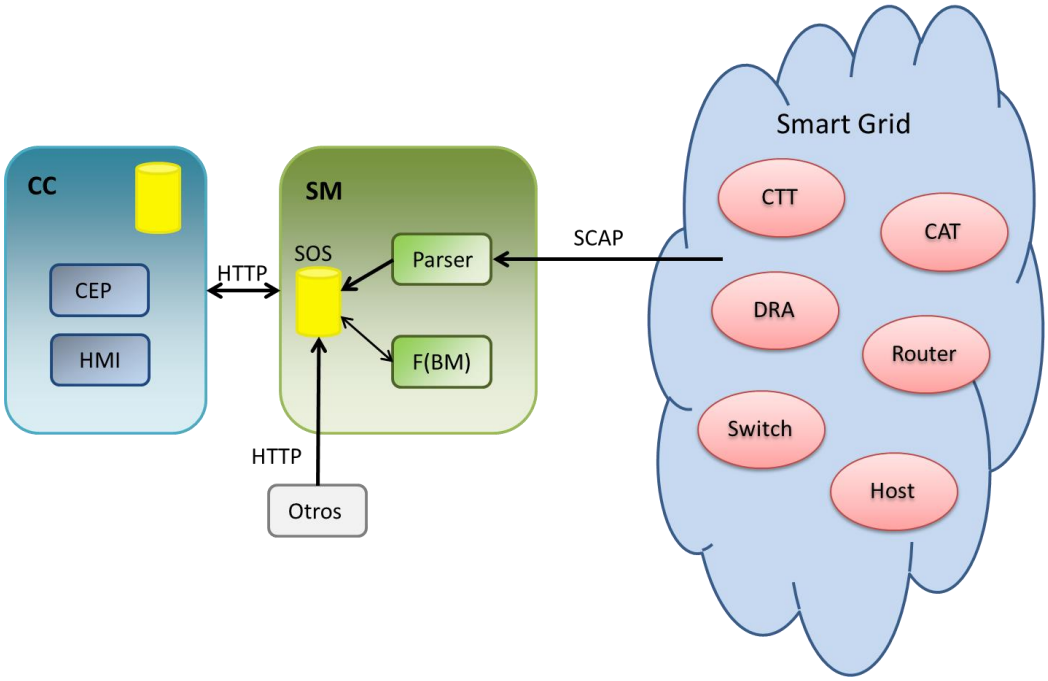

Figura 34. Arquitectura del sistema propuesto

5.4.1. Fuentes de datos

Para poder realizar el cálculo del valor de SA del smart grid, es necesario conocer el estado de todos los elementos que lo componen. A diferencia del caso de una fábrica, en el smart grid, la mayor parte de dichos elementos son equipos y dispositivos de los cuales se deben conocer sus vulnerabilidades. Se pueden clasificar en dos grupos, la red de comunicaciones y la red responsable de la generación, transporte y distribución de energía.

El mantenimiento de la seguridad de un sistema como el smart grid, es un reto debido a la cantidad y variedad de sistemas a asegurar, la necesidad de responder con rapidez a las nuevas amenazas y la falta de interoperabilidad entre las herramientas de gestión de la seguridad. En respuesta a este problema, el Instituto Nacional de Estándares y Tecnología (NIST) creó SCAP (Security Content Automation Protocol), un conjunto de estándares abiertos, que permite a las empresas y agencias gubernamentales la automatización de la gestión de vulnerabilidades, el cumplimiento de las políticas con las configuraciones de seguridad, enumerar los defectos del software, verificar la configuración de seguridad adecuada del sistema, y generar informes en un sistema automatizado, de manera consistente y repetible [226].

SCAP incorpora sistemas de medida para determinar la presencia de vulnerabilidades y proporciona mecanismos para clasificar los resultados de estas mediciones con el fin de evaluar el impacto de los problemas de seguridad detectados.

Para poder llevar a cabo la evaluación, se requiere que todos los dispositivos supervisados soporten SCAP y dispongan de un fichero OVAL (Open Vulnerability and Assessment Language) con todas vulnerabilidades acorde al sistema operativo que

utilizan y las pruebas que se deben realizar para verificarlas. En este caso se ha utilizado OpenSCAP [227], ya que es una herramienta abierta muy completa.

5.4.2. Sistema de Medida

Extracción de datos

Una vez todos los elementos del smart grid están registrados en el sistema, el SM puede empezar a reunir información de cada uno de ellos. Utiliza XCCDF (Extensible Configuration Checklist Description Format) [228] de SCAP que es un lenguaje de especificación utilizado para listas de control de seguridad, puntos de referencia y guías de seguridad en un formato estándar, que puede ser leído y comprendido por diferentes herramientas.

De este modo, el SM accede a cada uno de los elementos del smart grid donde se realiza la evaluación de sus vulnerabilidades. Una vez ha terminado se descarga el fichero de resultados, con el listado de las vulnerabilidades, indicando cuáles tienen algún riesgo y cuáles no. Gracias a SCAP se consigue medir cuantitativamente y en repetidas ocasiones las vulnerabilidades de defectos de software en todo el sistema.

Procesado de datos

Una vez se ha obtenido el fichero de vulnerabilidades, en el Sistema de Medida se debe llevar a cabo un primer procesado de los datos. El SM debe ser capaz de leer y entender el fichero de vulnerabilidades y extraer aquella información que sea relevante. Estos datos en bruto se le llaman medidas base o BM. Por tanto, la BM es launida más pequeña en la que se puede descomponer un SA. Debido a que en el smart grid existen muchas BMs, es interesante agregarlas de alguna manera, en medidas derivadas (DM). El sistema típicamente agrega una serie de vulnerabilidades para una tarea específica dentro del mismo dispositivo. Por ejemplo, un dispositivo con un sistema operativo determinado, puede usar Firefox como servicio de navegación. Suponiendo que hay 7 vulnerabilidades especificadas en el archivo de OVAL, cada vulnerabilidad constituye una BM, mientras que la agregación de todas ellas será una DM.

Por tanto, tras extraer los datos de los ficheros de vulnerabilidades, estas se agregan para formar DMs, que sirvan como unidad de medida para la creación de elementos de jerarquía superior. Esta tarea puede ser un proceso independiente o puede estar integrado dentro del CEP.

Almacenamiento de los datos

El sistema UniverSEC utiliza el SOS como repositorio de todas las medidas base y medidas derivadas que se obtienen de los distintos dispositivos a través de SCAP.

En el modelo teórico, el sistema de medida contiene dos SOS, uno en el que se almacenan las medidas base y otro para las medidas derivadas, de modo que estén

separadas. Pero en la práctica pueden estar recogidas en un único SOS. La manera de diferenciarlos es mediante un nuevo campo que se añade al insertar un nuevo sensor, que permite distinguir entre uno y otro. De esta forma, la puesta en funcionamiento del sistema es más sencilla, así como el envío de los mensajes al SOS.

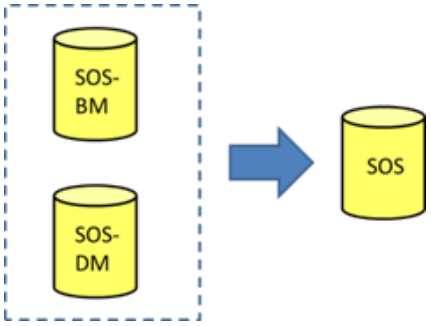

Figura 35. Modelo real de almacenamiento de datos en el SOS

Por tanto, al final del proceso tanto las medidas base como las medidas derivadas se encuentran en un mismo repositorio y son fácilmente accesibles.

5.4.3. Modelo de datos

Al igual que en FASYS, la meta-arquitectura necesaria para UniverSEC es muy compleja, y por tanto es necesario diseñar e implementar un modelo de datos en el que almacenar toda esta información. En la Figura 36 y Figura 37, se muestra el esquema del modelo de datos, en el que se pueden identificar algunos de los elementos más relevantes:

- Dispositivo (tabla Device): representa todos los equipos del smart grid, en los cuales se debe evaluar las vulnerabilidades para el cálculo del SA.
- Todos los elementos que componen un SA, desde las medidas base hasta el propio servicio, los cuales se ven a continuación. Se deben almacenar tanto los valores (salvo BMs y DMs que están en el SOS) como las relaciones entre ellos.

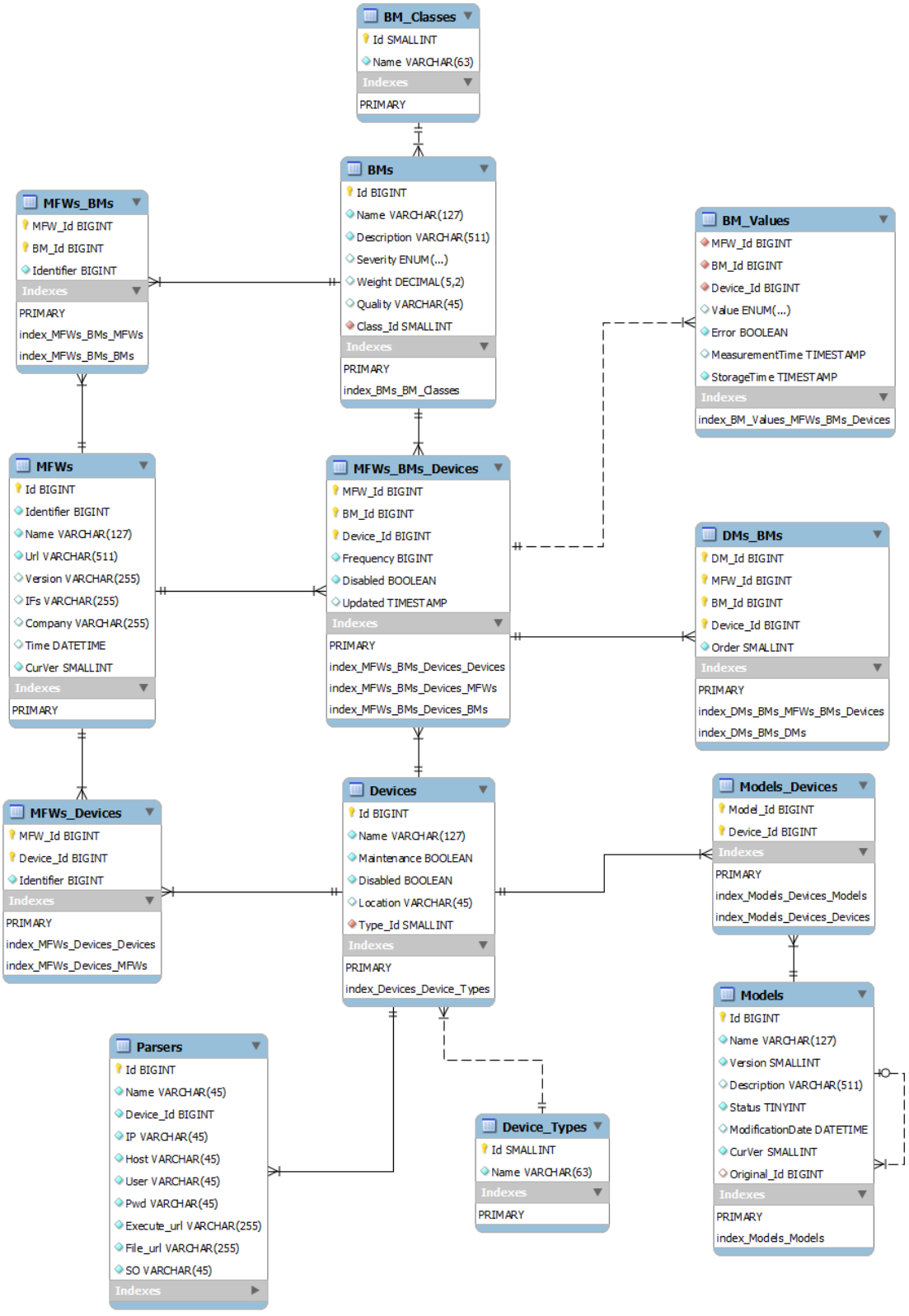

Figura 36. Modelo de datos UniverSEC 1

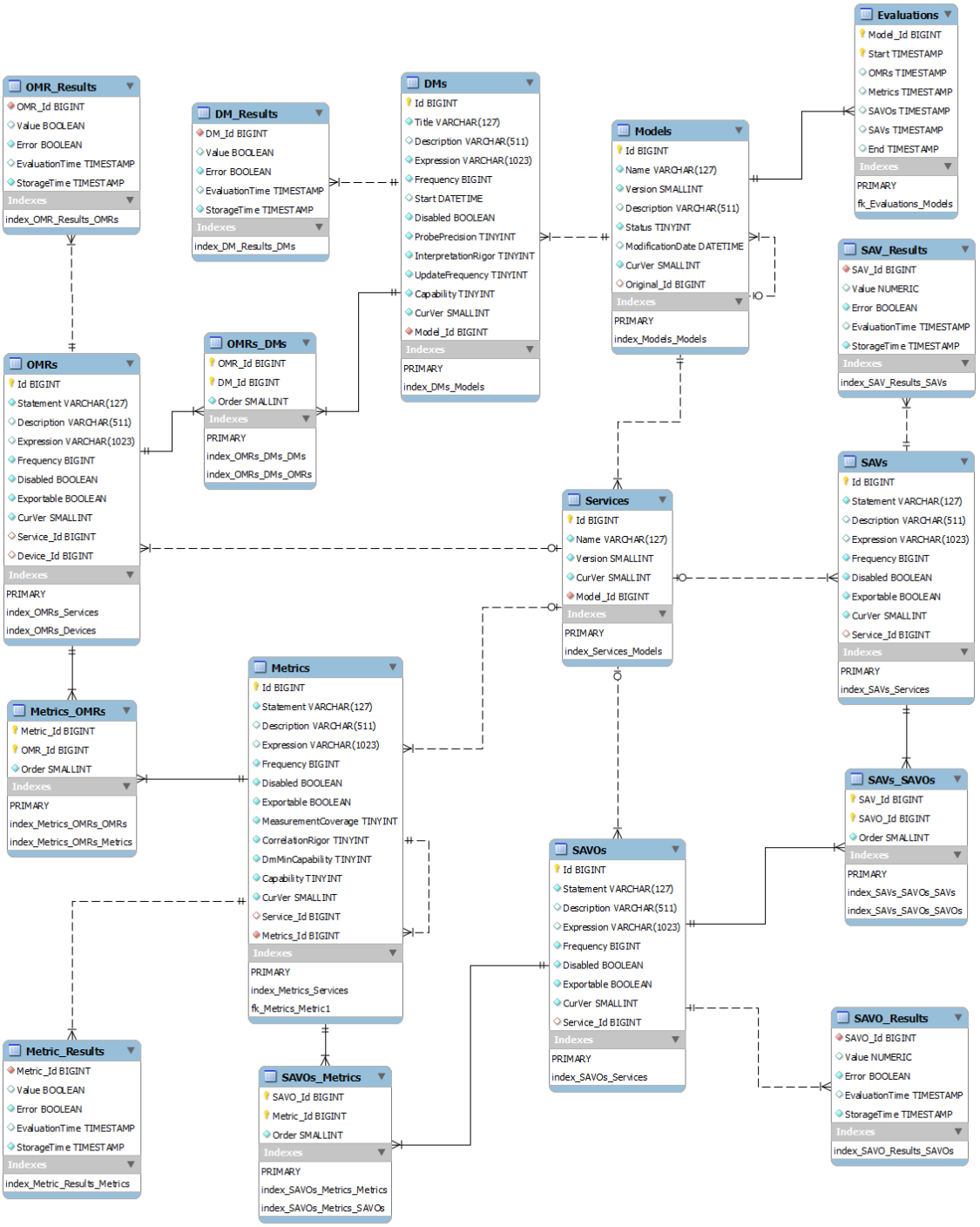

Figura 37. Modelo de datos UniverSEC 2

5.4.4. CEP

El procesamiento complejo de eventos es un concepto relacionado con la tarea de procesar múltiples eventos con el objetivo de identificar los más significativos dentro del conjunto de eventos recibidos. El CEP emplea técnicas como detección de patrones complejos de muchos eventos, correlación y abstracción de eventos, jerarquías de eventos y relaciones entre eventos como causalidad, afiliación, temporalidad y procesos dirigidos por eventos. La principal función del CEP es descubrir información contenida

en los eventos que suceden a través de las capas de la organización, analizar el impacto y determinar el plan de acción correspondiente en tiempo real.

Por tanto, en el Centro de Control el CEP permite extraer conclusiones fusionando datos monitorizados en tiempo real almacenados en el SOS, y permitiendo de esta forma valorar los riesgos, el cumplimiento de las normas y el grado de cumplimiento de la garantía de seguridad. El sistema debe ser capaz de analizar tanto sistemas sencillos como complejos, entendiendo estos últimos como aquellos que involucren una cantidad elevada de agentes interconectados, cuyos comportamientos agregados deben ser estudiados y comprendidos. La actividad agregada será generalmente no lineal, lo que supondrá que no podrá ser derivada de la suma de los comportamientos individuales de los sistemas simples.

En el CEP se realiza el cálculo del nivel total de SA del sistema y de los subsistemas a partir de las BMs y DMs almacenadas en el SOS. Como se puede ver en la Figura 38, el siguiente nivel de agregación son los Requisitos de Medición Objetos (OMR), que agrupa las diferentes DMs que pertenecen a un mismo grupo de servicios, como pueden ser Telnet o SSH, en un único servicio, que para este caso sería acceso remoto a un dispositivo (por ejemplo, a los smart meters).

Cada dispositivo del smart grid a ser evaluado, tendrá unos servicios u otros en función de la actividad realizada, por lo que la agregación de un mismo servicio u OMR de todos los dispositivos que lo proporcionen, es lo que le conoce como una métrica. Las métricas se pueden utilizar para el cálculo, entre otras cosas, de un servicio del SA.

Además de utilizar las métricas para construir servicios, es interesante hacer otro tipo de agrupaciones para la visualización de información. Esto no se refiere a la lógica de los datos, sino más bien a la configuración y agregación de datos para la visualización en función de las preferencias del administrador. Para ello, se definen las Vistas de Garantía de Seguridad (SAV, de sus siglas en inglés) y los Objetos de Vistas de Garantía de la Seguridad (SAVO, de sus siglas en inglés), que permiten reagrupar métricas según las preferencias.

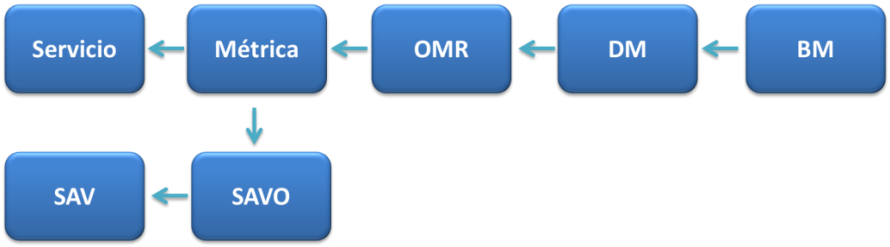

Figura 38. Elementos del SA

5.4.5. HMI

El HMI de la plataforma de monitorización y control es el punto de acceso de los usuarios al sistema UniverSEC. El HMI debe ser amigable y usable, pero al mismo tiempo debe incluir todas las capacidades necesarias para la realización de las tareas

asignadas. En esta sección se presentan las pantallas reales con el funcionamiento del sistema de evaluación y el aseguramiento del smart grid.

Con la finalidad de facilitar un acceso ubicuo, el HMI se ha implementado como una aplicación web, de tal forma, que se pueda acceder a la aplicación de monitorización y control mediante cualquier dispositivo con acceso a Internet a través de un navegador web. De esta forma, se pueden crear de forma sencilla contenidos con diseños innovadores y atractivos. Además permite crear aplicaciones ágiles, donde la facilidad de uso es una de las principales características.

Control de acceso

El acceso al HMI se realiza mediante autenticación web, con usuario y contraseña. La autenticación web es la forma más sencilla de login y es comúnmente empleada en aplicaciones web. Los navegadores permiten almacenar dicha autenticación, con lo que el acceso puede resultar inmediato si se configura de esta forma.

Cuando utilizamos HTTP, la información que mandamos y recibimos a través del navegador realiza una serie de saltos entre diferentes routers que se encuentran entre el cliente y el servidor web remoto. En cada uno de estos saltos la información puede retransmitirse a todos los dispositivos (PC's, servidores, etc.) conectados a la red del router en cuestión. HTTPS usa los protocolos de Capa de sockets seguros (SSL) o Seguridad de la capa de transporte (TLS) para proteger la información. El uso de HTTPS está especialmente recomendado cuando se usan redes wifi no seguras, pero su uso en todo tipo de redes es siempre positivo.

Pantalla de inicio

La pantalla de inicio del sistema UniverSEC está dividida en cuatro áreas principales, como se muestra en la Figura 39:

- En la parte superior hay una serie de pestañas que permite navegar entre las diferentes secciones de la aplicación. Estas corresponden a los principales elementos que definen el nivel de aseguramiento definido en la sección anterior, además de una parte de administración.
- En la parte central a la izquierda hay un mapa donde se localizan georeferenciados los dispositivos que se están monitorizando. Haciendo clic en cada uno de ellos es posible visualizar información personalizada.
- En la parte central, a la derecha, se pueden ver algunas gráficas con resultados globales del sistema, como son los datos históricos de un servicio o el porcentaje de servicios vulnerables.
- En la parte inferior, hay un listado de las alarmas más importantes, como puede ser cuando un servicio pasa a ser vulnerable.

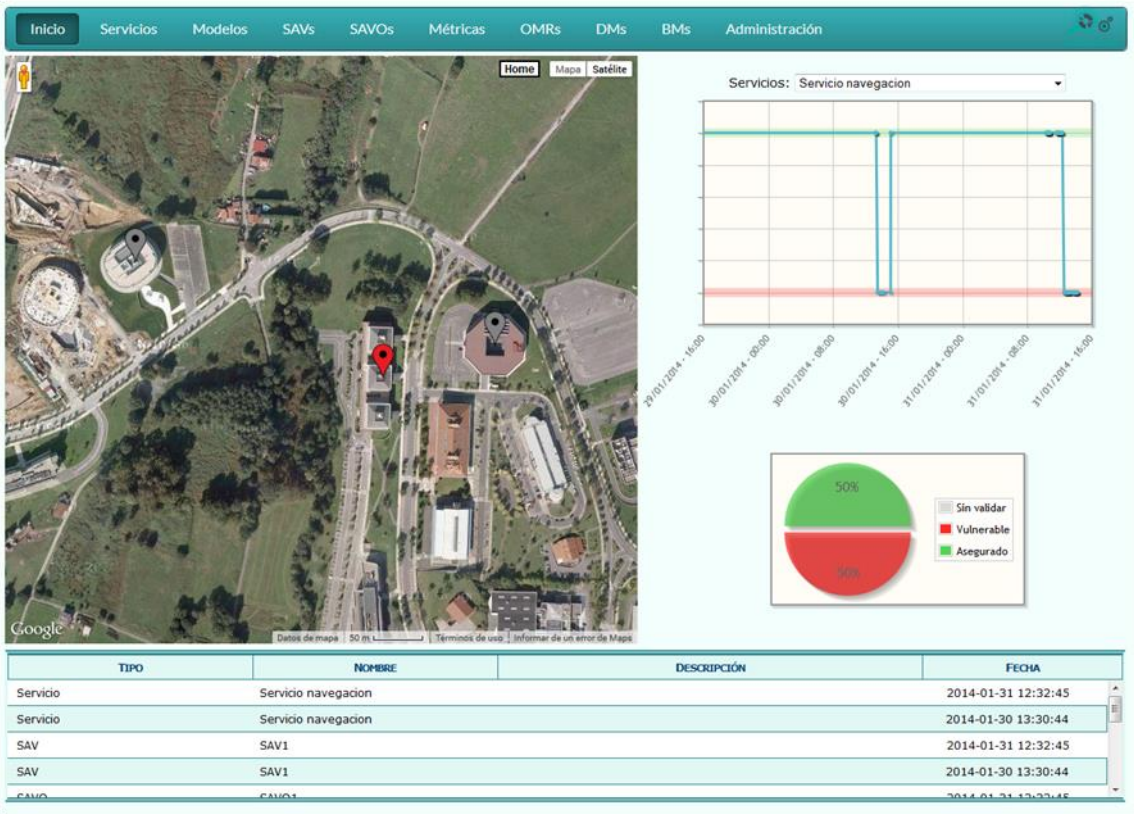

Figura 39. Pantalla de inicio

Sobre el mapa de la zona que se está evaluando se pueden ver posicionados todos los elementos que están siendo monitorizados. Los iconos que los representan pueden ser personalizados, así como el *title* (texto que aparece al poner el ratón encima). El icono varia de color en función de la evaluación del dispositivo, variando entre verde, si todos sus OMR están asegurados; rojo, si alguno de ellos es vulnerable; o gris si lleva cierto tiempo sin recibir nuevas medidas. Al hacer clic en cada uno de ellos su muestra el estado de los OMR específicos de cada uno (Figura 40). El mapa además de permitir zoom, arrastrar, Street View de google o cambiar entre mapa e imagen de satélite, tiene un botón de Home el cual te centra en el área de evaluación.

En la parte derecha, la primera gráfica muestra todos los valores históricos de cada servicio, por lo que se puede ver cuando ha tenido alguna vulnerabilidad en la última semana. Se puede observar la gráfica con más detalle gracias al zoom. Para cambiar entre los servicios existentes hay una lista desplegable encima de la gráfica.

La segunda gráfica muestra el estado en tiempo real de los distintos servicios definidos. Para ello, representa en una gráfica sectorial el porcentaje de servicios que están asegurados, que tienen alguna vulnerabilidad o que llevan tiempo sin enviar datos. El tiempo de validación de los datos es configurable por parte del usuario.

La tabla de la parte inferior nos alerta de cuando un servicio o cualquiera de los elementos del nivel de aseguramiento pasa a ser vulnerable. En ese caso nos muestra el nombre de dicho elemento, su descripción y la fecha del evento.

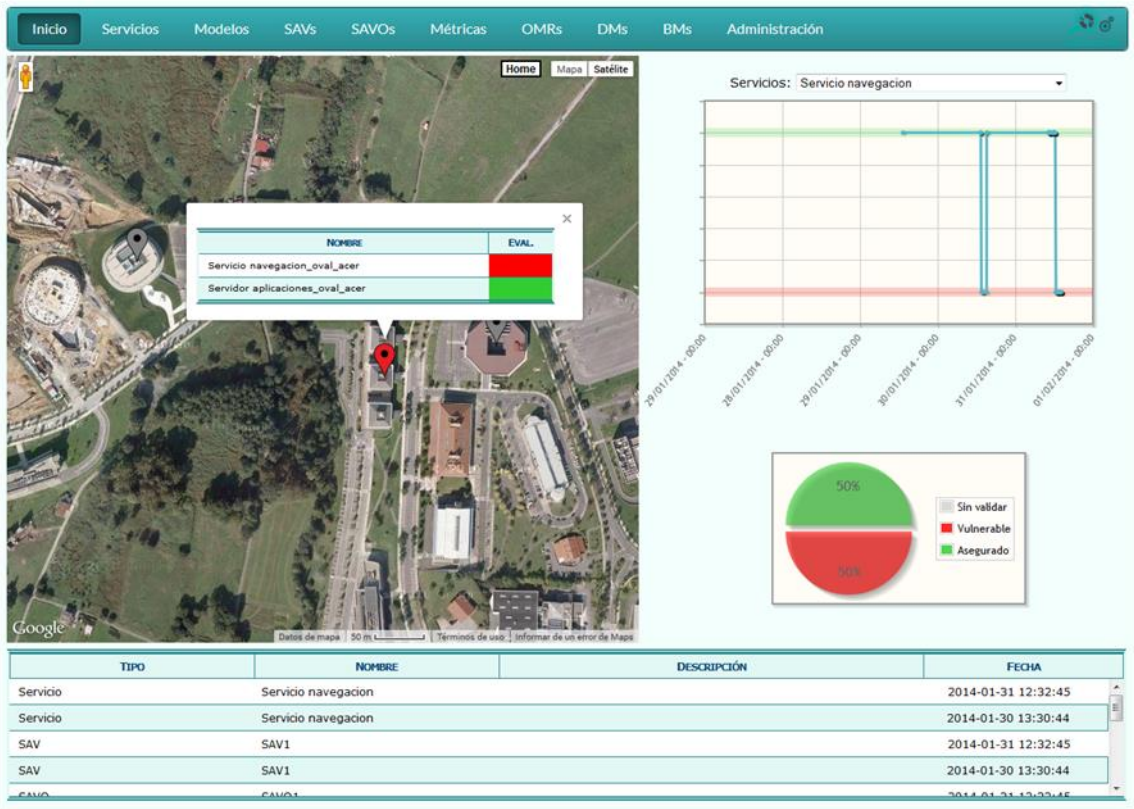

Figura 40. Detalles de un dispositivo

Servicios

Al hacer clic en el botón de "Servicios" de la barra superior, se accede al menú de servicios. En él, se muestra una tabla con un listado de todos los servicios definidos y algunos de sus parámetros principales. El más importante de ellos es el estado o evaluación actual del servicio que puede variar entre vulnerable (rojo), asegurado (verde), sin validar (gris) o inactivo (negro). El servicio no estará validado cuando no reciba datos durante cierto tiempo, el cual se puede definir en la configuración. La desactivación de cualquier elemento se puede hacer manualmente si el administrador del sistema lo considera necesario.

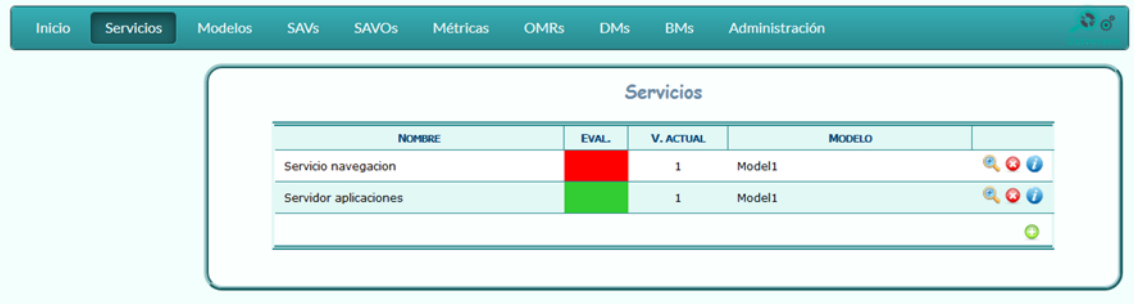

Figura 41. Menú de servicios

Cada uno de los servicios tiene varias acciones asociadas. La primera de ella (🔍) permite visualizar y editar todos los detalles de un servicio. La segunda (⊗), permite borrar un servicio. La tercera (ℹ), se puede visualizar los subelementos del servicio y el

estado de cada uno de ellos, con el fin de conocer la causa del estado actual (Ver Figura 42). Por último, en la parte inferior, hay otro botón ( ) para añadir nuevos servicios.

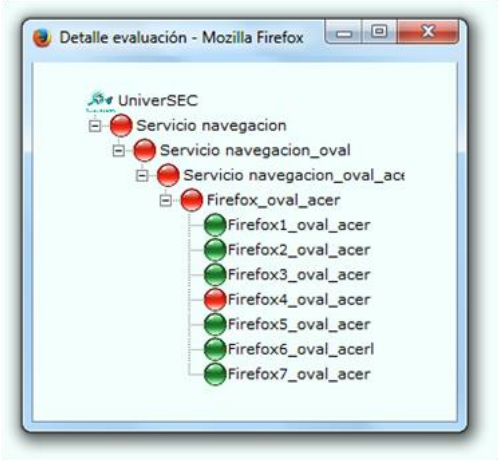

Figura 42. Estado de un servicio

Al hacer clic en mostrar los detalles de un servicio o al crear uno nuevo se mostrará el formulario de la Figura 43, en el primer caso con los datos del servicio seleccionado y en el segundo con los campos en blanco. La información disponible es la siguiente:

- Nombre: Nombre del servicio.
- Versión: Permite diferenciar entre las distintas versiones de un mismo servicio.
- V. actual: Versión actual del servicio.
- Modelo: El modelo al que pertenece el servicio.

Figura 43. Campos de un servicio

Modelos

La Figura 44 muestra un listado de todos los modelos existentes en el sistema con sus principales características. Cada modelo tiene varias acciones asociadas, como visualizar y editar todos los detalles de un modelo, borrarlo o añadir uno.

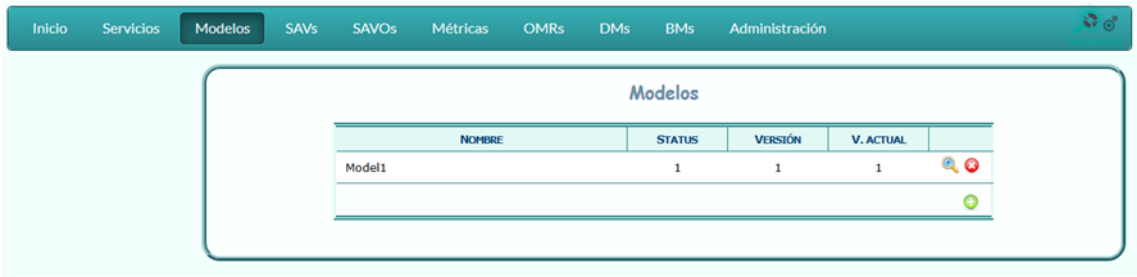

Figura 44. Menú de modelos

Al acceder a los detalles de un modelo o al crear uno nuevo se mostrará el formulario de la Figura 45, en el primer caso con los datos del modelo seleccionado y en el segundo con los campos en blanco. La información disponible es la siguiente:

- Nombre: Nombre del modelo.
- Descripción: Descripción del modelo.
- Estado: Estado en el que se encuentra el modelo.
- Versión: Distintas versiones del modelo.
- V. Actual: Versión actual del modelo.
- Fecha modificación: Fecha de la última modificación del modelo.
- Modelo original: Modelo de jerarquía superior en caso de existir.
- Dispositivos: Dispositivos que están asociados a un modelo.

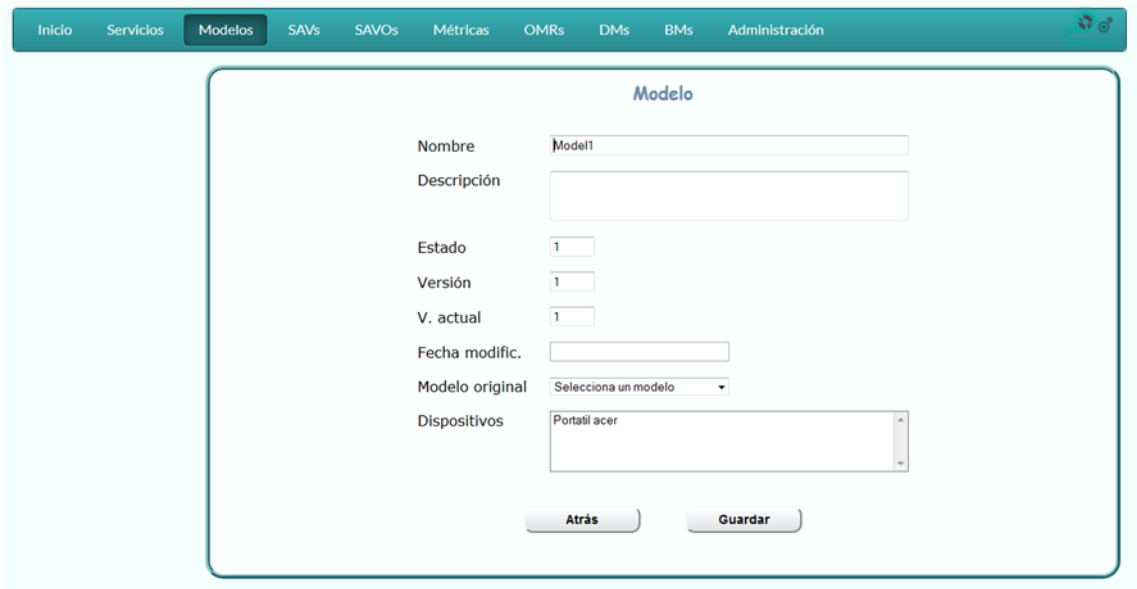

Figura 45. Campos de un modelo

SAVs

La Figura 46, muestra un listado de todas las vistas de garantía de seguridad existentes en el sistema con sus principales características. La más importante de ellas es el estado

o evaluación actual del SAV que puede variar entre vulnerable (rojo), asegurado (verde), sin validar (gris) o inactivo (negro).

Figura 46. Menú de SAVs

Cada uno de los SAVs tiene varias acciones asociadas: visualizar y editar todos los detalles de un SAV, borrarlo, añadir uno nuevo, o visualizar sus subelementos y el estado de cada uno de ellos, con el fin de conocer la causa del estado actual (Ver Figura 47). Por último, en la parte inferior, hay otro botón para añadir nuevos SAVs.

Figura 47. Estado de un SAV

Al acceder a los detalles de un SAV, o al crear uno nuevo, se mostrará el formulario de la Figura 48, en el primer caso con los datos del SAV seleccionado y en el segundo con los campos en blanco. La información disponible es la siguiente:

- Nombre: Nombre del SAV.
- Descripción: Breve descripción del SAV.
- Expresión: Fórmula para la evaluación del SAV a partir de los SAVOs, la cual interpreta el CEP.
- Activado: Permite activar o desactivar un SAV para cancelar la evaluación.
- Exportable: Permite exportar o no el SAV.
- Frecuencia: Frecuencia cada cuanto se evalúa el SAV.
- V. Actual: Versión actual del SAV.
- Servicio: Servicio al que pertenece el SAV.

- SAVOS: Conjunto de SAVOS que definen el SAV.

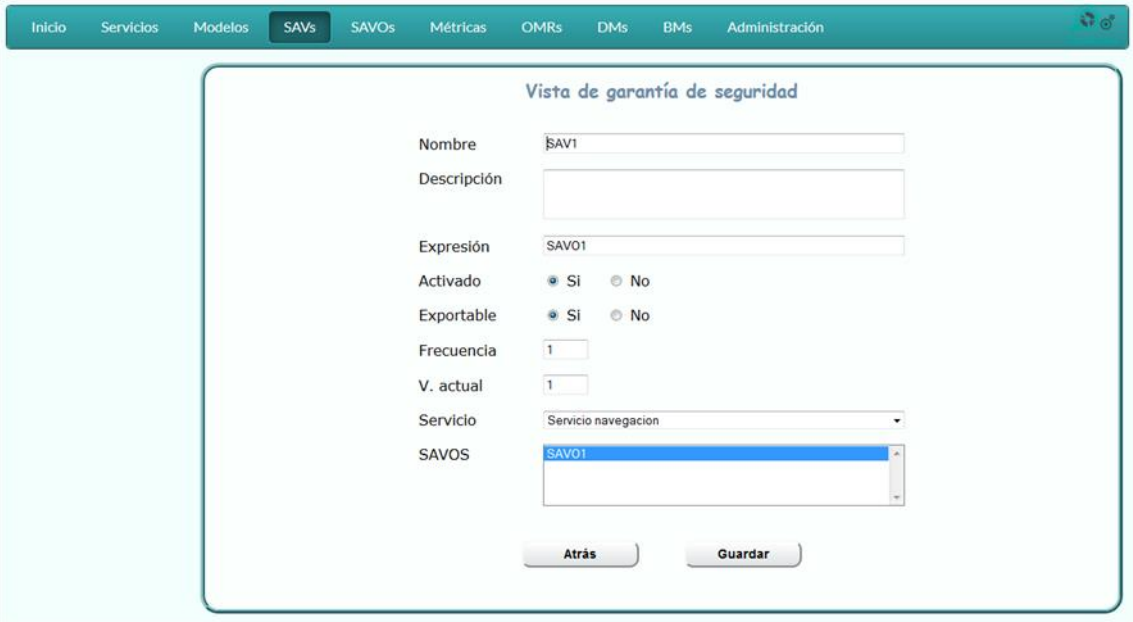

Figura 48. Campos de un SAV

SAVOs

La Figura 49, muestra un listado de todos los objetos de vistas de garantía de seguridad (SAVO) existentes en el sistema con sus principales características. La más importante de ellas es el estado o evaluación actual del SAVO, que puede variar entre vulnerable (rojo), asegurado (verde), sin validar (gris) o inactivo (negro).

Figura 49. Menú de SAVOs

Cada uno de los SAVOs tiene varias acciones asociadas: visualizar y editar todos los detalles de un SAVO, borrarlo, añadir uno nuevo, o visualizar sus subelementos y el estado de cada uno de ellos, con el fin de conocer la causa del estado actual (Ver Figura 50). Por último, en la parte inferior, hay otro botón para añadir nuevos SAVOs.

Figura 50. Estado de un SAVO

Al acceder a los detalles de un SAVO, o al crear uno nuevo, se mostrará el formulario de la Figura 51, en el primer caso con los datos del SAVO seleccionado y en el segundo con los campos en blanco. La información disponible es la siguiente:

- Nombre: Nombre del SAVO.
- Descripción: Breve descripción del SAVO.
- Expresión: Fórmula para la evaluación del SAVO a partir de las métricas, la cual interpreta el CEP.
- Activado: Permite activar o desactivar un SAVO para cancelar la evaluación.
- Exportable: Permite exportar o no el SAVO.
- Frecuencia: Frecuencia cada cuanto se evalúa el SAVO.
- V. actual: Versión actual del SAVO.
- Servicio: Servicio al que pertenece el SAVO.
- Métricas: Conjunto de métricas que definen el SAVO.

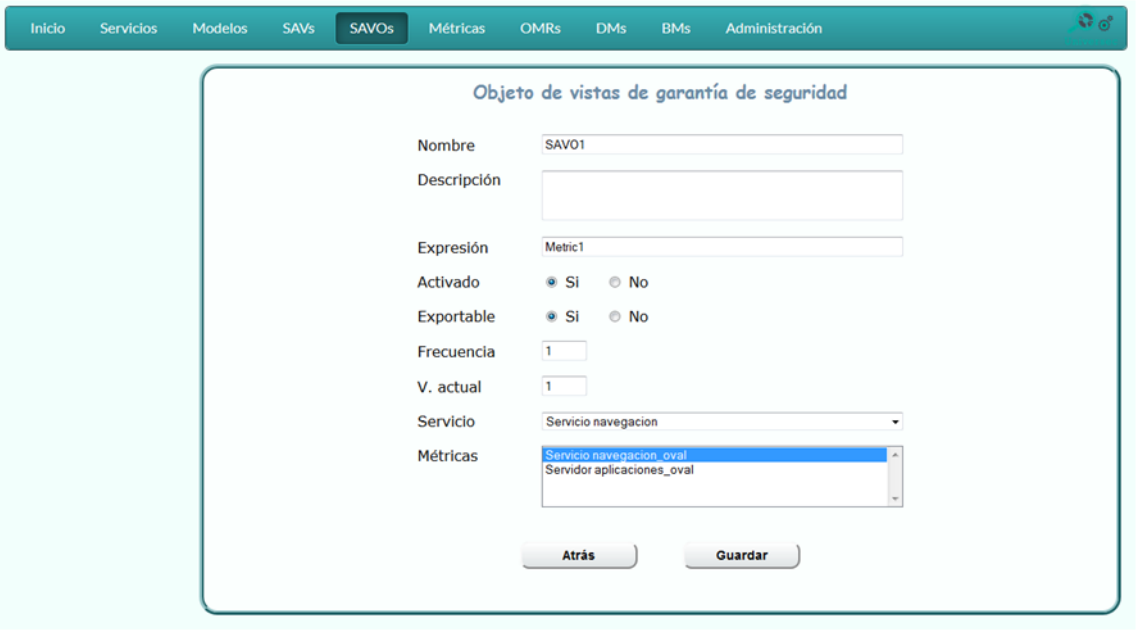

Figura 51. Campos de un SAVO

Métricas

La Figura 52, muestra un listado de todas las métricas existentes en el sistema con sus principales características. La más importante de ellas es el estado o evaluación actual de la métrica, que puede variar entre vulnerable (rojo), asegurado (verde), sin validar (gris) o inactivo (negro).

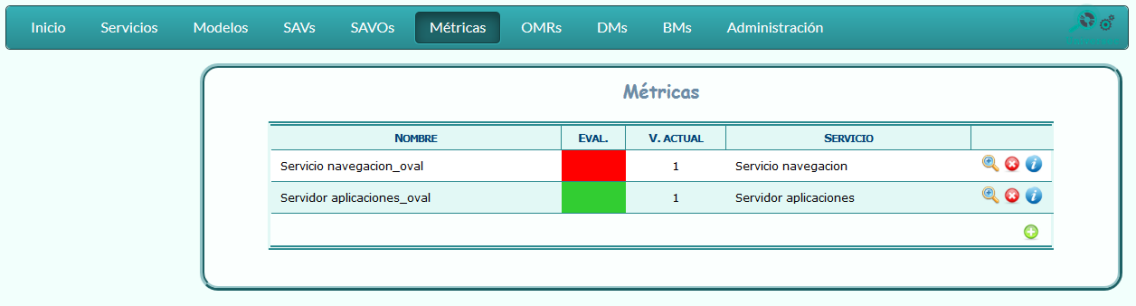

Figura 52. Menú de métricas

Cada una de las métricas tiene varias acciones asociadas: visualizar y editar todos los detalles de una métrica, borrarla, añadir una nueva, o visualizar sus subelementos y el estado de cada uno de ellos, con el fin de conocer la causa del estado actual (Ver Figura 53). Por último, en la parte inferior, hay otro botón para añadir nuevas métricas.

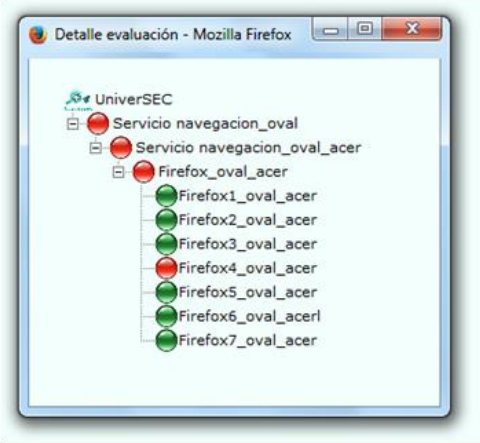

Figura 53. Estado de una métrica

Al acceder a los detalles de una métrica, o al crear una nueva, se mostrará el formulario de la Figura 54, en el primer caso con los datos de la métrica seleccionada y en el segundo con los campos en blanco. La información disponible es la siguiente:

- Nombre: Nombre de la métrica.
- Descripción: Breve descripción de la métrica.
- Expresión: Fórmula para la evaluación de la métrica a partir de los OMRs, la cual interpreta el CEP.
- Activado: Permite activar o desactivar una métrica para cancelar la evaluación.
- Exportable: Permite exportar o no la métrica.
- Frecuencia: Frecuencia cada cuanto se evalúa la métrica.
- Cobertura de medición: Cobertura de medición de la métrica.
- Rigor de correlación: Rigor de correlación de la métrica.
- Capacidad mínima DM: Capacidad mínima de las DMs de la métrica.
- Capacidad: Capacidad mínima de la métrica.
- V. actual: Versión actual de la métrica.
- Servicio: Servicio al que pertenece la métrica.
- OMRs: Conjunto de OMRs que definen la métrica.

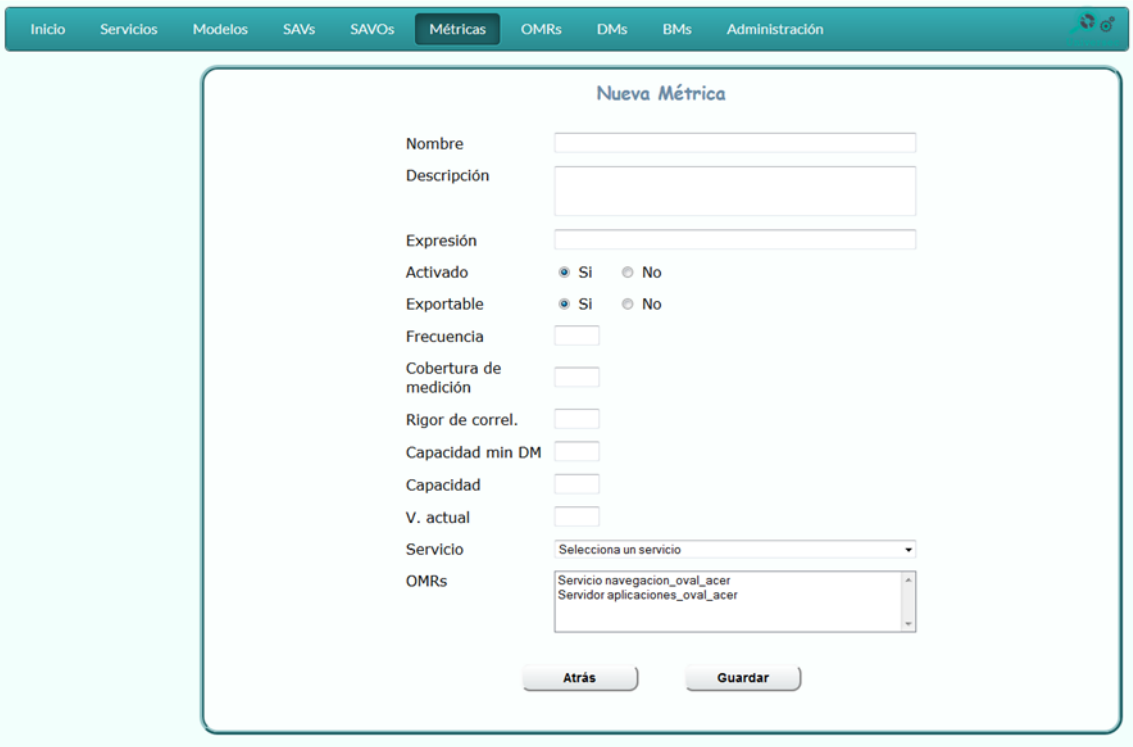

Figura 54. Campos de una métrica

OMRs

La Figura 55, muestra un listado de todos los requisitos de medición de objetos (OMRs) existentes en el sistema con sus principales características. La más importante de ellas es el estado o evaluación actual del OMR, que puede variar entre vulnerable (rojo), asegurado (verde), sin validar (gris) o inactivo (negro).

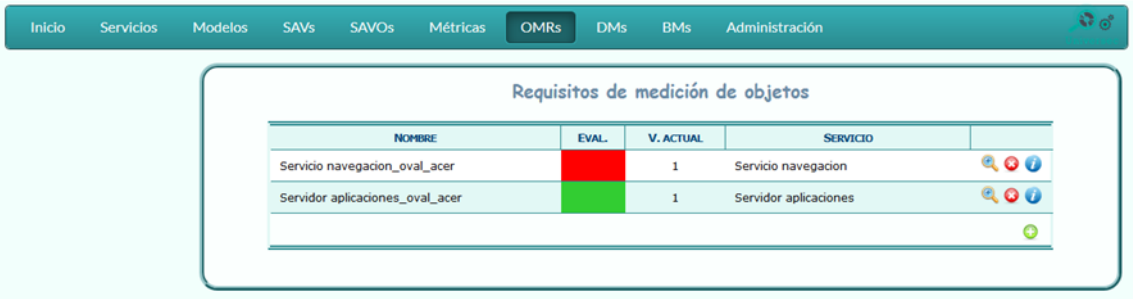

Figura 55. Menú de OMRs

Cada uno de los OMRs tiene varias acciones asociadas: visualizar y editar todos los detalles de un OMR, borrarlo, añadir uno nuevo, o visualizar sus subelementos y el estado de cada uno de ellos, con el fin de conocer la causa del estado actual (Ver Figura 56). Por último, en la parte inferior, hay otro botón para añadir nuevos OMRs.

Figura 56. Estado de un OMR

Al acceder a los detalles de un OMR, o al crear uno nuevo, se mostrará el formulario de la Figura 57, en el primer caso con los datos del OMR seleccionado y en el segundo con los campos en blanco. La información disponible es la siguiente:

- Nombre: Nombre del OMR.
- Descripción: Breve descripción del OMR.
- Expresión: Fórmula para la evaluación del OMR a partir de los DMs, la cual interpreta el CEP.
- Activado: Permite activar o desactivar un OMR para cancelar la evaluación.
- Exportable: Permite exportar o no el OMR.
- Frecuencia: Frecuencia cada cuanto se evalúa el OMR.
- V. actual: Versión actual del OMR.
- Servicio: Servicio al que pertenece el OMR.
- Dispositivo: Dispositivo al que pertenece el OMR.
- Medidas derivadas: Conjunto de DMs que definen el OMR.

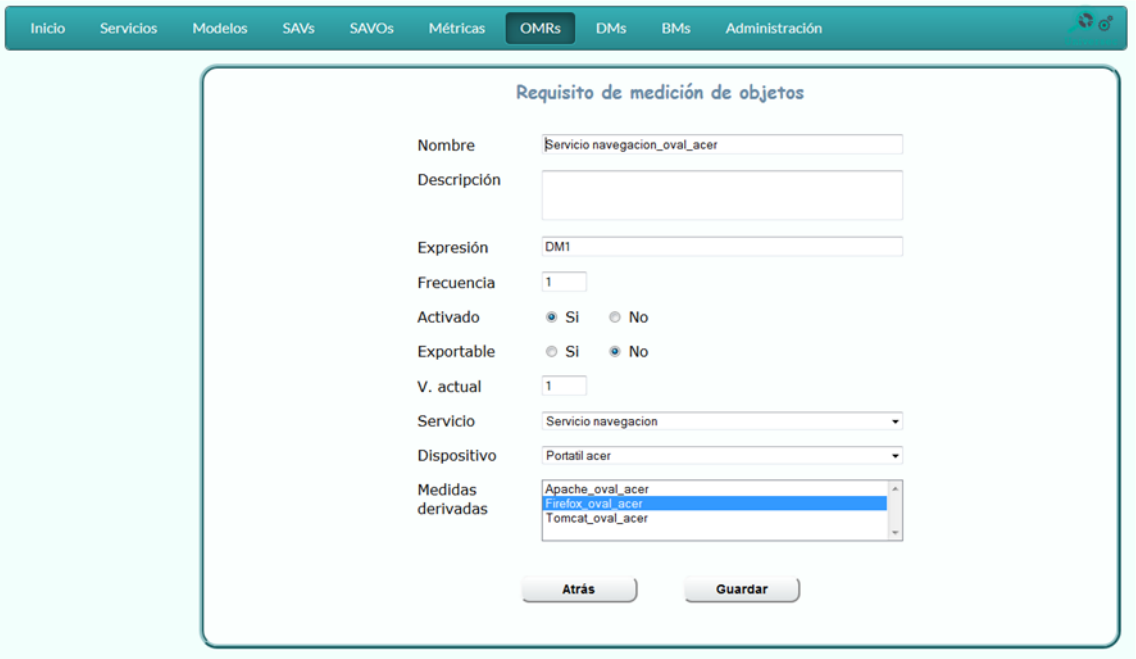

Figura 57. Campos de un OMR

DMs

La Figura 58, muestra un listado de todos las medidas derivadas (DMs) existentes en el sistema con sus principales características. La más importante de ellas es el estado o evaluación actual de la DM, que puede variar entre vulnerable (rojo), asegurado (verde), sin validar (gris) o inactivo (negro).

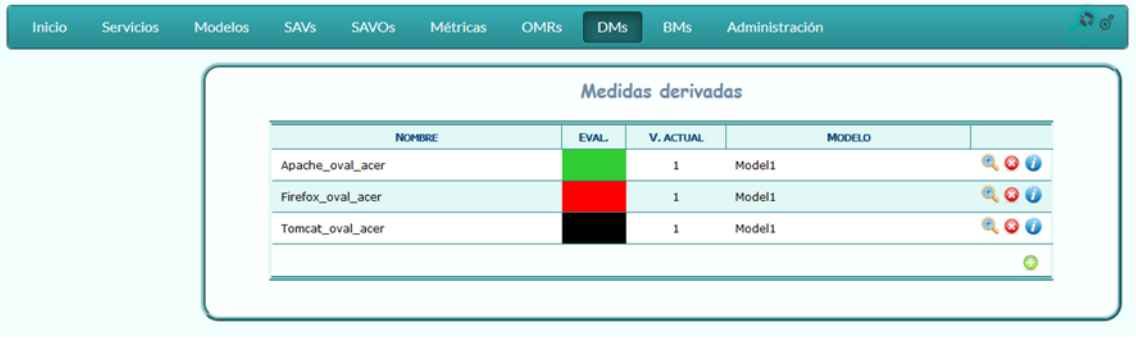

Figura 58. Menú de DMs

Cada una de las DMs tiene varias acciones asociadas: visualizar y editar todos los detalles de una DM, borrarla, añadir una nueva, o visualizar sus subelementos y el estado de cada uno de ellos, con el fin de conocer la causa del estado actual (Ver Figura 59). Por último, en la parte inferior, hay otro botón para añadir nuevas DMs.

Figura 59. Estado de una DM

Al acceder a los detalles de una DM, o al crear una nueva, se mostrará el formulario de la Figura 60, en el primer caso con los datos de la DM seleccionada y en el segundo con los campos en blanco. La información disponible es la siguiente:

- Nombre: Nombre de la DM.
- Descripción: Breve descripción de la DM.
- Expresión: Fórmula para la evaluación de la DM a partir de las BMs, la cual interpreta el CEP.
- Activado: Permite activar o desactivar una DM para cancelar la evaluación.
- Frecuencia: Frecuencia cada cuanto se evalúa la DM.
- Rigor: Rigor en las medidas de la DM.
- Capacidad: Capacidad de las medidas de la DM.
- Precisión: Precisión de las medidas de la DM.
- Frecuencia de actualización: Frecuencia de actualización de la DM.
- Inicio: Fecha de comienzo de la DM.
- V. actual: Versión actual de la DM.
- Modelo: Modelo al que pertenece la DM.
- Medidas base: Conjunto de BMs que definen la DM.

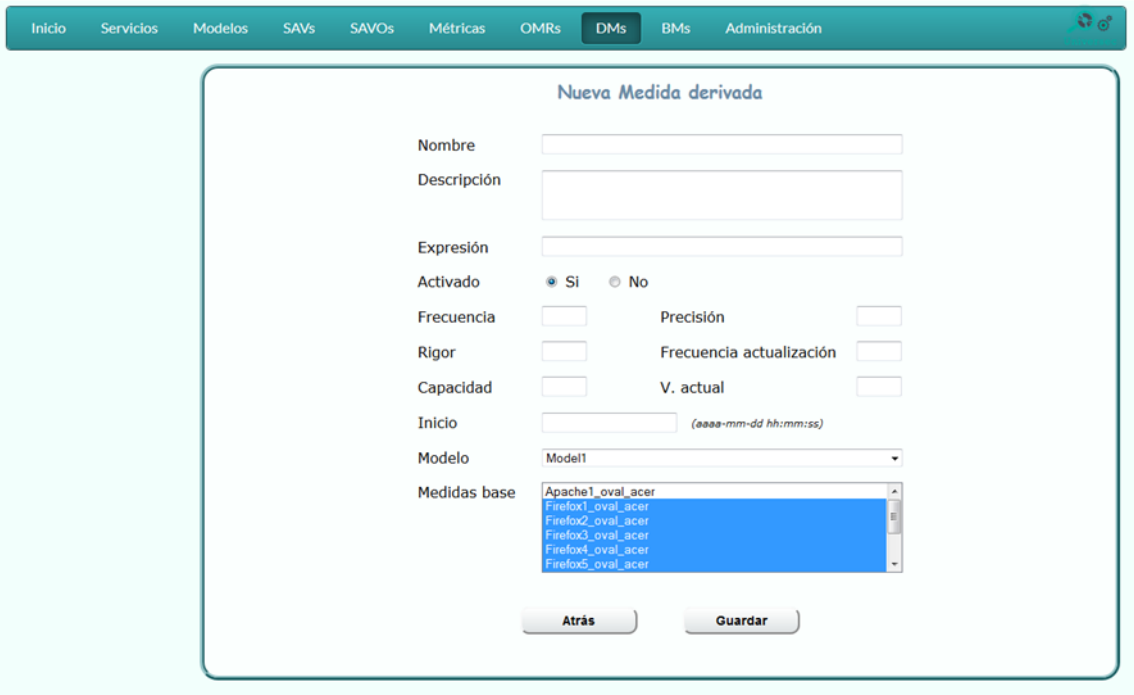

Figura 60. Campos de una DM

BMs

La Figura 61, muestra un listado de todos las medidas base (BMs) existentes en el sistema con sus principales características. La más importante de ellas es el estado o evaluación actual de la BM que puede variar entre vulnerable (rojo), asegurado (verde), sin validar (gris) o inactivo (negro). Cada una de las BMs tiene varias acciones asociadas: visualizar y editar todos los detalles de una BM, borrarla, o añadir una nueva.

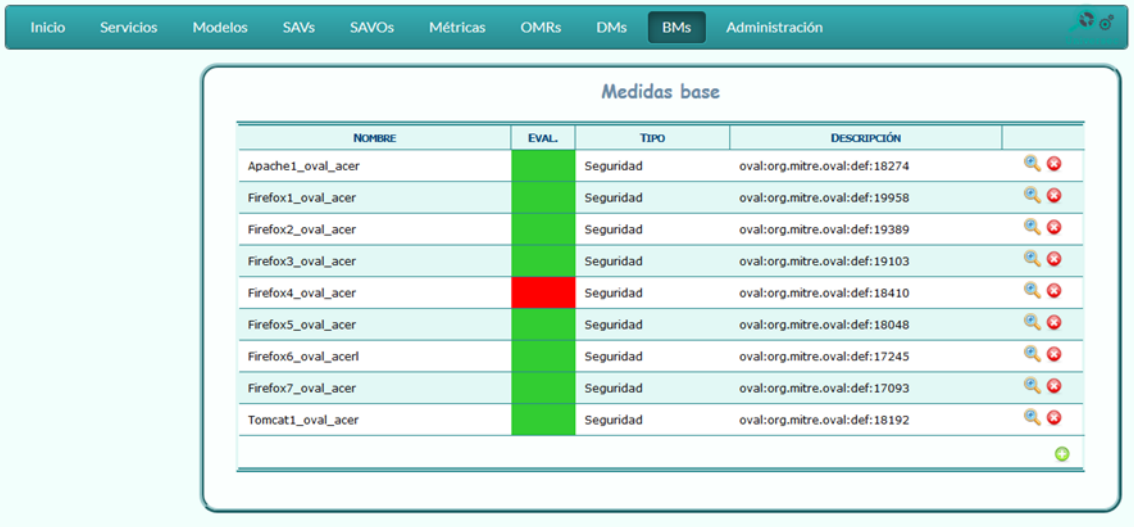

Figura 61. Menú de BMs

Al acceder a los detalles de una BM, o al crear una nueva, se mostrará el formulario de la Figura 62, en el primer caso, con los datos de la BM seleccionada y en el segundo con los campos en blanco. La información disponible es la siguiente:

- Nombre: Nombre de la BM.

- Descripción: Breve descripción de la BM.
- Gravedad: Gravedad de la BM, la cual puede variar entre baja, media o alta.
- Peso: Peso de la BM.
- Calidad: Calidad de la medida de la BM.
- Tipo: Tipo de BM de los definidos previamente.
- Dispositivo: Dispositivo al que pertenece la BM.

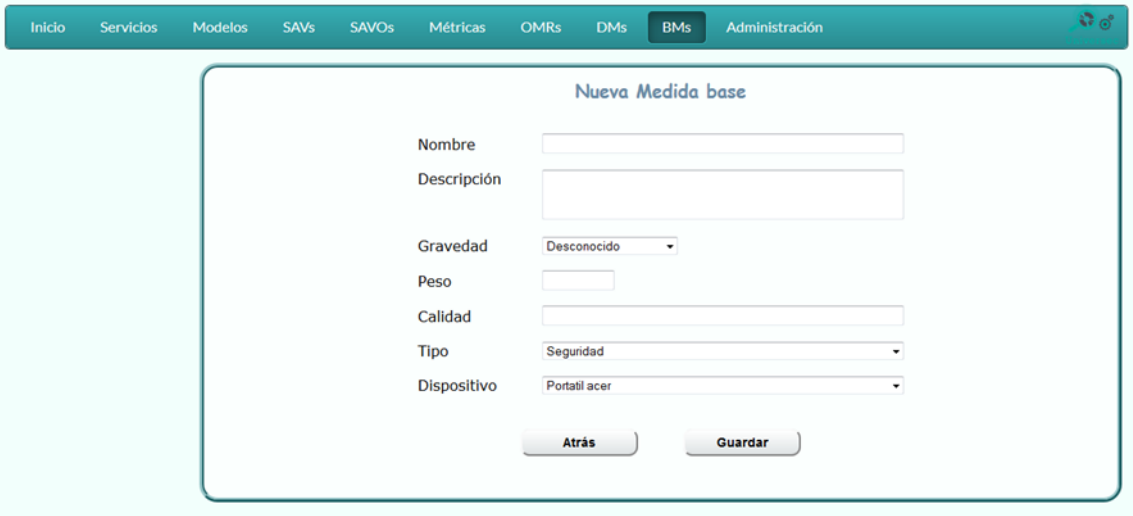

Figura 62. Campos de una BM

Administración

El menú de administración permite configurar todos los parámetros de utilidad en el sistema UniverSEC. La mayor parte de estos parámetros quedan definidos en el modelo de datos de UniverSEC donde se describen las principales entidades y relaciones.

Desde el menú de administración (véase menú izquierdo de la Figura 63), podemos configurar los dispositivos, los sistema de medida, los parsers, los servicios a ejecutar, así como unos parámetros de configuración general. A continuación se describen cada una de estas opciones.

Dispositivos

La Figura 63, muestra un listado de todos los dispositivos existentes en el sistema con sus principales características. Cada uno de los dispositivos tiene varias acciones asociadas: visualizar y editar todos los detalles de un dispositivo, borrarlo, o añadir uno nuevo.

Figura 63. Menú de dispositivos

Al acceder a los detalles de un dispositivo, o al crear uno nuevo, se mostrará el formulario de la Figura 64, en el primer caso con los datos del dispositivo seleccionado y en el segundo con los campos en blanco. La información disponible es la siguiente:

- Nombre: Nombre del dispositivo.
- Mantenimiento: Necesidad de realizar mantenimiento en el dispositivo.
- Activado: Se tiene o no que incluir en la evaluación del riesgo de seguridad.
- Localización: Ubicación del dispositivo.
- Tipo: Tipo de dispositivo. Puede ser específico de la Smart Grid (CAT, CTT, DRA) o de la red de comunicaciones (router, switch, equipo,..).
- Sistema de medida: Sistema de medida al que el dispositivo envía los datos de sus medidas base.

Figura 64. Campos de un dispositivo

Sistemas de medida

La Figura 65, muestra un listado de todos los sistemas de medida (SM) existentes en el sistema con sus principales características. Cada uno de los SM tiene varias acciones asociadas: visualizar y editar todos los detalles de un SM, borrarlo, o añadir uno nuevo.

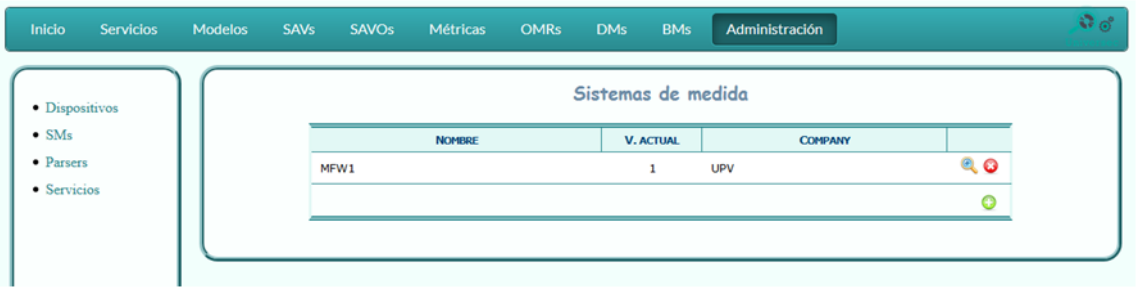

Figura 65. Menú de sistemas de medida

Al acceder a los detalles de un sistema de medida, o al crear uno nuevo, se mostrará el formulario de la Figura 66, en el primer caso con los datos del Sistema de medida seleccionado y en el segundo con los campos en blanco. La información disponible es la siguiente:

- Identificador: Identificador del sistema de medida.
- Nombre: Nombre del sistema de medida.
- URL: URL para acceder a la configuración del sistema de medida.
- Versión: Permite distinguir versiones del sistema de medida.
- IFs: Ifs del sistema de medida.
- Compañía: Compañía al que pertenece el sistema de medida.
- Fecha: Fecha de creación del sistema de medida.
- V. actual: Versión actual del sistema de medida.

Figura 66. Campos del Sistema de medida

Parsers

La Figura 67, muestra un listado de todos los parsers existentes en el sistema con sus principales características. El parser tiene como principal objetivo obtener los ficheros de vulnerabilidades de los distintos dispositivos, leer dicha información e introducirla

en el SOS. Para cada batería de pruebas que se realice a un dispositivo, hace falta un parser distinto, ya que los datos obtenidos y el formato en el que se envían pueden ser distintos. Cada uno de los parsers tiene varias acciones asociadas: visualizar y editar todos los detalles de un parser, borrarlo, o añadir uno nuevo.

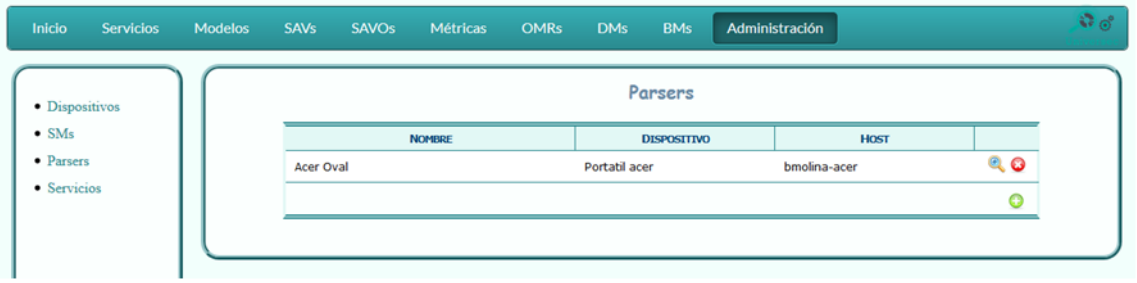

Figura 67. Menú de parsers

Al acceder a los detalles de un parser, o al crear uno nuevo, se mostrará el formulario de la Figura 68, en el primer caso con los datos del parser seleccionado y en el segundo con los campos en blanco. La información disponible es la siguiente:

- Nombre: Nombre del parser.
- Dispositivo: Dispositivo al que accede el parser para obtener información.
- IP: IP del dispositivo para poder acceder a él.
- Host: Host del dispositivo para poder acceder a él.
- Usuario: Usuario para poder acceder a los archivos en el dispositivo.
- Contraseña: Contraseña para poder acceder a los archivos en el dispositivo.
- Sistema operativo: Sistema operativo en el dispositivo.
- URL de ejecución: URL remota para la ejecución del script que evalúa las vulnerabilidades del dispositivo y crea el fichero XML.
- URL del fichero: URL local y nombre del fichero de vulnerabilidades una vez obtenido.

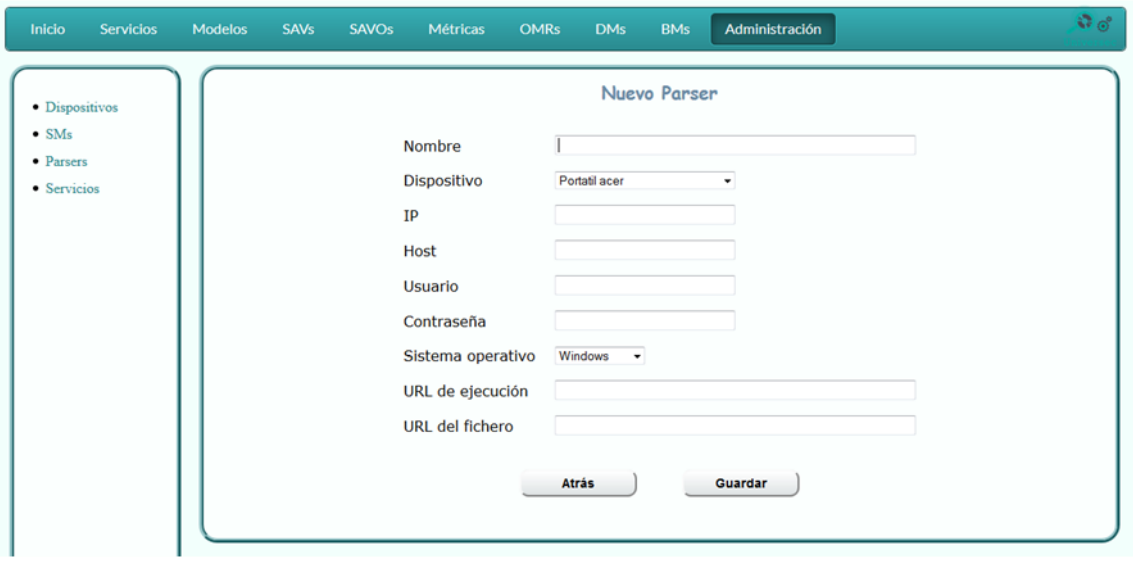

Figura 68. Campos del parser

Ejecución de servicios

Para su correcto funcionamiento, el sistema UniverSEC tiene algunos servicios que se ejecutan en *background*. Estos servicios sirven para obtener y procesar toda la información que luego mostrará el HMI. Para ello, se dispone de un botón para activar o desactivar cada uno de los servicios cuando sea necesario.

Figura 69. Ejecución de servicios

Existen tres servicios disponibles:

- Evaluación remota: Este servicio obtiene todos los dispositivos existentes de la base de datos y accede a ellos vía SSH para la ejecución de un script que evalúe las vulnerabilidades del dispositivo y cree un fichero XML de respuesta. A continuación, se descarga el fichero y lo procesa, permitiendo introducir en el SOS el valor de cada medida base.

- Función de DMs: A partir de las medidas base almacenadas en el SOS, calcula las medidas derivadas y vuelve a insertar los datos en el SOS y la base de datos.
- CEP: A partir de las medidas derivadas, el CEP calcula el resto de elementos de que definen el nivel de aseguramiento (OMRs, métricas, servicios, SAVOs y SAVs).

Persistencia

El menú de persistencia permite especificar los orígenes a las fuentes de datos y parámetros de configuración, como se refleja en la Figura 70. Se pueden distinguir cuatro bloques fundamentales:

- Servidor SOS
  - URL de acceso: URL para acceder al SOS a través de su API.
- Base de datos del sistema
  - Cadena de acceso: ubicación (IP) donde está el servidor de bases de datos.
  - Usuario: cuenta de usuario para acceder a la base de datos.
  - Contraseña: contraseña de usuario para acceder a la base de datos.
- Tiempos
  - Refresco de servicios: Tiempo cada cuanto se ejecutan los servicios: Evaluación remota, Función de DMs y CEP (en segundos).
  - Tiempo validación: Tiempo a partir del que un dato deja de ser válido (en minutos).
- Sistema
  - Sistema operativo: Sistema operativo del equipo.
  - Directorio de instalación: Directorio en el que está instalado el sistema UniverSEC.

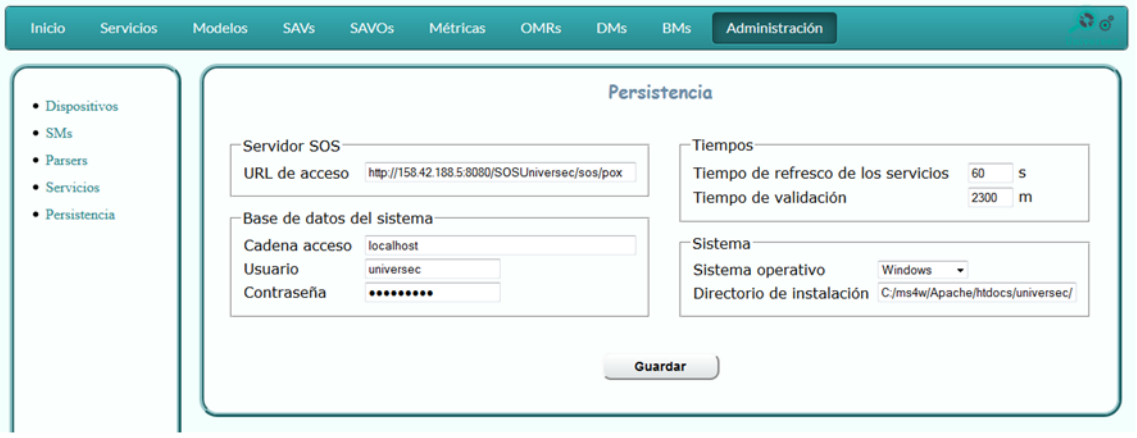

Figura 70. Menú de persistencia

5.5. Logros de UniverSEC

El prototipo de sistema UniverSEC proporciona el marco para la definición de una arquitectura de sistema de monitorización, evaluación y gestión de la seguridad de activos de infraestructuras críticas. El sistema UniverSEC proporciona las utilidades de protección necesarias en la actualidad al mismo tiempo que se adapta y crece para cumplir los requerimientos futuros, por lo que contribuye ostensiblemente a la mejora de las entidades que cuenten con infraestructuras críticas, siendo su impacto, multisectorial.

Los principales ejes innovadores del proyecto han sido:

- Infraestructura de medida, que proporciona los medios y los mecanismos para monitorizar las infraestructuras de la organización, considerando el posible carácter ubicuo de las mismas, así como su evolución en términos de versiones, nuevos servicios o redes. La infraestructura desplegada se basa en la utilización de sondas que están en todos los elementos que tienen que ser monitorizadas. Las sondas proporcionan de una forma continua información de las medidas solicitadas (ej. número medio de petición de conexiones TCP por unidad de tiempo o número de paquetes ICMP recibidos en un host). Todas estas medidas se obtienen de forma periódica y se almacenan en el sistema de medida de la infraestructura.
- El sistema dinámico de medida y supervisión del aseguramiento está alineado con las metodologías, casos de buen uso, herramientas y procedimientos de la certificación del proceso. Los perfiles de aseguramiento proporcionan un mecanismo estándar de interoperabilidad entre sistemas, además de permitir la definición de las necesidades de aseguramiento para un servicio dado, de forma que en cada organización se pueda definir un modelo de seguridad para la implementación de dicho servicio.
- El centro de control y supervisión de las medidas de aseguramiento, que obtiene las medidas almacenadas para analizarlas y proporcionar una valoración del nivel de aseguramiento. El centro de control, es capaz de trabajar en entornos multidominio, de forma que, pueda evaluar el nivel de aseguramiento, así como otras medidas de seguridad de servicios prestados por varias organizaciones y/o sistemas. El que esta evaluación esté centralizada permite que actualizaciones de patrones, métricas e introducción de nuevos niveles y perfiles se realice de forma centralizada.

Los principales avances que supone UniverSEC respecto al estado del arte son dos conceptos fundamentales:

- Monitorización continua de la seguridad de la información, el sistema UniverSEC proporciona una visión actualizada en tiempo real del estado de la seguridad de la información del sistema, proporcionando una información dinámica y fácilmente entendible, basada en indicadores de niveles de seguridad que se miden de manera

continua, viendo la adecuación de las mismas a las métricas, parámetros y patrones de las diferentes normas, así como una valoración cuantitativa de la garantía de seguridad. Para poder realizar estas tareas, es necesario realizar una monitorización en tiempo real, mediante diferentes sondas de la situación real de la seguridad en cada instante de tiempo. El sistema de captura de información es escalable y para tratar el elevado volumen de datos de múltiples fuentes que se puedan recibir se emplean técnicas basadas en stream processing.

- La evaluación de la contribución de las medidas de seguridad implementadas (salvaguardas), las metodologías, estándares y herramientas actuales para la gestión de la seguridad de la información, se basan en un compendio de recomendaciones, buenas prácticas y mecanismos habituales para gestionar los riesgos de los activos de información de una manera global, en base a las posibles amenazas y las vulnerabilidades detectadas. No evalúan ni categorizan la contribución de dichas salvaguardas al nivel de seguridad general, ni al nivel particular de vulnerabilidad de cada uno de los activos de información. El sistema UniverSEC proporciona a los responsables, información en tiempo real sobre el estado de cada una de las salvaguardas, reflejándose en el nivel de seguridad general y de cada uno de los activos de información, teniendo en cuenta el nivel de criticidad de cada uno de estos activos, facilitando de esta manera una reacción adecuada y a tiempo de los responsables en función de indicadores y del estado de cada uno de los activos. De forma adicional, empleando técnicas basadas en Complex Event Processing relaciona medidas y eventos de diferentes fuentes, sistemas y herramientas, siendo capaz de evaluar el grado de garantía de la seguridad. Se representa toda la información en un HMI que concentra toda la información necesaria del ámbito de trabajo y control.

6. Caso 3: STIMULO

6.1. Introducción

Los sistemas de transporte juegan un papel crucial en nuestra sociedad, con una influencia considerable en aspectos tan diversos como el consumo energético, la contaminación, el bienestar social, la seguridad, la productividad industrial y la prosperidad económica. Asegurando la movilidad de personas y mercancías de forma eficaz y eficiente, contribuyen positivamente al bienestar de personas y comunidades.

En la actualidad, las instituciones y organismos de transporte oficiales, han evolucionado desde las meras tareas de construcción y mantenimiento de la propia infraestructura de transporte, a operar las redes que gestionan de una manera integrada, con la finalidad de mejorar la seguridad, fluidez, comodidad y eficiencia. Estos sistemas ITS mejoran la movilidad, aumentan la seguridad, reducen el consumo de combustible y la emisión de contaminantes, e incluso son capaces de ofrecer información dinámica y efectiva al viajero [229]. Los sistemas ITS no solo brindan un servicio útil a las instituciones públicas, sino también al sector privado, principalmente al sector logístico, permitiéndole gestionar el transporte más eficientemente.

Mediante la previsión en tiempo real del estado de los diferentes componentes del transporte (infraestructura, vehículos, mercancías, usuarios, etc.), el proyecto STIMULO, tiene como principal objetivo el desarrollo de servicios de transporte altamente eficientes, mediante la combinación de modelos de simulación con la información en tiempo real, proporcionada por diferentes fuentes, sensores y equipamientos fijos y móviles (servicios de tránsito en la ciudad y carretera, dispositivos móviles en los vehículos, condiciones meteorológicas, cámaras de video con imágenes de la situación del tráfico, etc.) así como la información de datos históricos. La solución desarrollada en el proyecto, se aplica en diferentes entornos para mejorar la eficiencia y gestión de recursos y el tráfico en infraestructuras y zonas críticas como accesos portuarios, cruces de carretera, áreas urbanas, etc.

En concreto la solución desarrollada se prueba con un demostrador en el Puerto de Valencia, cuyo principal objetivo es el desarrollo de un sistema de predicción en tiempo real de la llegada de contenedores de mercancías al puerto de Valencia. En combinación con información de la carga/descarga y operaciones a realizar, se dota de un sistema de alertas a los diferentes actores involucrados, lo que permite la anticipación a posibles problemas de congestión en diferentes puntos y la anticipación de la organización interna de las terminales, reduciendo los tiempos de espera en la puerta de la terminal y en su interior, y por lo tanto, la mejora de la eficiencia de las operaciones del puerto.

En esta primera sección del capítulo se comenta el concepto de smart city. En la segunda sección, se presentan los objetivos principales que intenta lograr el proyecto STIMULO. En la tercera sección, se visualiza la arquitectura con la que se ha llevado a cabo el proyecto, y en la siguiente, el funcionamiento más detallado de todas sus partes. Por último, se enumeran los logros que ha conseguido el proyecto.

6.1.1. Smart City

El término ciudad inteligente o smart city, es un concepto empleado en el ámbito científico y en el marketing empresarial, siendo utilizado comúnmente tanto por organismos públicos como privados. Si bien aún no existe una definición clara para este concepto [230], se pueden identificar tres características principales comunes en esta denominación:

- No se debe dañar el medio ambiente
- Se valora el empleo de las TIC como herramientas para la gestión (inteligente)
- El objetivo principal es el desarrollo sostenible.

Si bien las principales iniciativas de investigación se centran principalmente en los sistemas energéticos, una de las medidas innovadoras en este sentido lo constituye la gestión eficiente de la energía en las redes de transporte que, entre otras ventajas, conduce a la disminución de emisiones CO2. Así pues, una de las principales áreas de actuación lo constituye la movilidad inteligente, la logística y la tecnología, con actividades como [231]:

- Análisis de los flujos de tráfico, dando prioridad al transporte de emergencias y al transporte público.
- Detección automática de las infracciones del código de circulación y los peligros en las carreteras, información mediante señales adecuadas o información online de los accidentes producidos en las vías de circulación a los vehículos próximos.
- Desarrollo de modelos matemáticos y simulaciones para poder comparar distintas vías de circulación y distintos escenarios de transporte, y así poder predecir posibles efectos sociales y ambientales.
- Implantación de servicios de información online para los ciudadanos: tiempos estimados de llegada del transporte público, servicios para compartir bicicletas o vehículos, etc.

El concepto de ciudad inteligente engloba una serie de sistemas de gran complejidad, y se puede catalogar como un sistema de sistemas, o un ecosistema, en donde coexisten múltiples procesos fuertemente relacionados y que resulta difícil abordar y entender de forma separada. Toda esta complejidad hace que la implantación de una ciudad inteligente afecte o interactúe con un número muy elevado de sectores.

En este nuevo modelo de ciudad, es necesario desarrollar sistemas inteligentes que suministren información proactivamente para la actividad diaria de los ciudadanos, tanto laboral, como personal. Sin embargo, para que la información generada sea útil, la ciudad inteligente se ha de sustentar en una completa red de comunicaciones que esté accesible a todos los agentes que la constituyen: ciudadanos, empresas y administración.

No existe una solución universal que permita garantizar el éxito de una ciudad en su búsqueda de inteligencia, sino que hay que tener en cuenta muchos aspectos diferentes desde distintos ámbitos: gobierno, edificios, movilidad, energía, medio ambiente, y

servicios. El nivel de coordinación entre todas las iniciativas existentes y previstas, puede variar en función del nivel de madurez de la transformación de una ciudad. En su búsqueda de la inteligencia, una ciudad puede pasar por distintos niveles de madurez. Estos niveles se pueden describir en un modelo simplificado que se basa en tres niveles, representados en la Figura 71 [232]:

- Disperso: Estas ciudades están comprometidas a mejorar en una o más dimensiones, introduciendo por ejemplo sistemas de transporte inteligentes o reduciendo el consumo de energía. En este nivel, las iniciativas inteligentes están dirigidas por estructuras departamentales como una serie de proyectos aislados.
- Integrado: En este nivel de madurez, las iniciativas empiezan a estar mucho mejor coordinadas, tratan de aprovechar sinergias y las ciudades gestionan los proyectos con un mayor grado de colaboración. El valor total que aportan las iniciativas es mayor que la suma de las partes.
- Conectado: En este nivel, las iniciativas inteligentes forman parte de un plan integral dirigido por un equipo de gobierno específico que incluye a ciudadanos y empresas. Las ciudades conectadas consiguen los mejores resultados sociales.

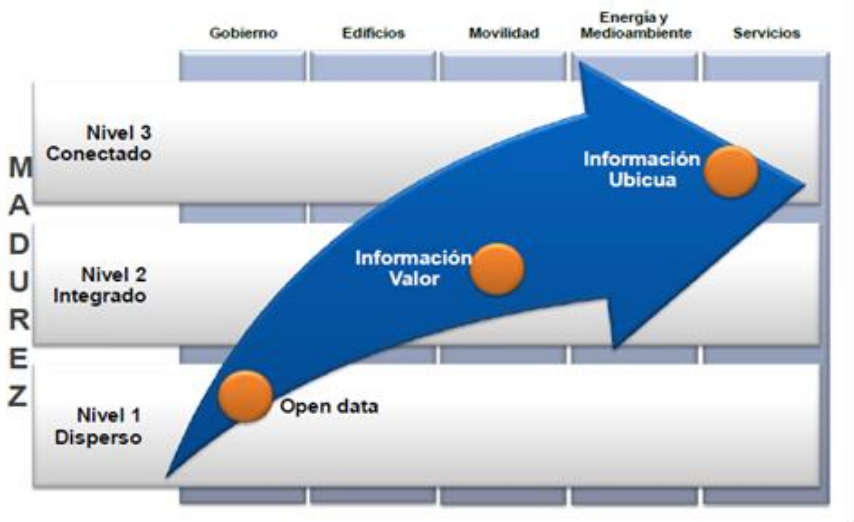

Figura 71. Nivel de madurez de una ciudad inteligente [232]

Una ciudad inteligente no sólo puede tener distintos niveles de madurez en momentos diferentes, sino que también puede tener distintos niveles al mismo tiempo, para cada una de las dimensiones inteligentes.

Las TIC son críticas para aumentar el nivel de madurez: desde una mínima digitalización, hasta plataformas digitales abiertas y conectadas para aplicaciones públicas y privadas; desde la ausencia de proyectos TIC importantes hasta un plan integral bien gestionado y articulado, que responde a la idea y los objetivos de una ciudad inteligente. La disponibilidad de la información y su correspondiente nivel de integración también van cambiando durante el proceso:

- Información abierta: Es la que existe cuando el nivel de madurez de una ciudad inteligente es disperso. La ciudad trata de ofrecer a sus ciudadanos y empresas

distintos tipos de información, principalmente a través de portales de internet. Esta información es genérica y no se adapta a distintas necesidades.

- Información valiosa: Se consigue cuando una ciudad da un paso adelante y alcanza el nivel integrado de madurez. Con respecto a la información abierta, la información valiosa es más fácil de encontrar y usar. También está en el contexto adecuado para las necesidades de ciudadanos y empresas.
- Información ubicua: Es característica del nivel más alto de madurez (conectado). La ciudad ofrece en cualquier momento y lugar a sus ciudadanos (pero sólo a los que lo deseen) información adaptada a sus necesidades sin que tengan que buscarla por sí mismos. Esto es posible gracias a Internet y a una amplia informatización de la sociedad. La información personalizada se compila en función de perfiles de ciudadanos y está organizada en plataformas abiertas y seguras.

Como se puede apreciar, el proyecto STIMULO enlaza directamente (aunque parcialmente) dentro del contexto de ciudad inteligente, desde el punto de vista de una correcta gestión de las TIC para mejorar la eficiencia de los procesos productivos llevados a cabo en el puerto de Valencia, principalmente mediante la correcta monitorización y gestión de las redes de transporte que permiten acceder a dicho puerto y, de esta forma, optimizar la carga y descarga de mercancías desde y hacia el puerto.

6.2. Objetivos de STIMULO

El proyecto STIMULO, ha tenido como objetivo la construcción de servicios inteligentes de gestión del tráfico, por medio de la predicción en tiempo real del estado de los componentes del sistema de transporte (infraestructura, vehículos, mercancías, usuarios, etc.). Los elementos principales de la infraestructura propuesta son: el modelo de simulación, la minería de datos de sensores heterogéneos en tiempo real, la generación de indicadores de tráfico y el uso de esos indicadores, junto con técnicas de inteligencia colectiva, para la provisión de servicios asociados al sistema de transporte, que permitan una mayor eficiencia y desempeño. Así, este objetivo general se desglosa en los siguientes objetivos específicos:

- Diseñar y desarrollar un modelo de simulación de sistemas de transporte, que incorpore todos los aspectos necesarios para poder implementar sobre él los mecanismos de toma de decisiones y servicios propuestos.
- Diseñar y desarrollar un sistema distribuido de adquisición y minería de datos, que permita agregar información presente en los diferentes elementos del sistema de transporte (infraestructura, vehículos, usuarios, etc.) en tiempo real. Se presta especial atención a la extracción de información de imágenes capturadas por cámaras en la infraestructura.
- Conceptualizar y evaluar servicios innovadores orientados a la eficiencia y sostenibilidad en sistemas de transporte, tales como encaminamiento anticipativo de vehículos o gestión distribuida interflotas.

- Diseñar y desarrollar nuevos servicios en el contexto de la infraestructura de transporte inteligente propuesta.
- Desarrollar un demostrador, que sirva para validar de la infraestructura y servicios propuestos, y facilite su posterior explotación por terceros.
- Diseñar incentivos y modelos de negocio para la aceptabilidad de los servicios propuestos, que impulsen la viabilidad institucional, económica y financiera de las nuevas soluciones encontradas.
- Promover la difusión de las contribuciones del proyecto, de cara a facilitar su estandarización.

6.3. Arquitectura de STIMULO

6.3.1. Componentes del sistema

El primer paso antes de especificar los detalles de una arquitectura, consiste en identificar los bloques principales que constituyen el sistema, que se ilustran en la Figura 72.

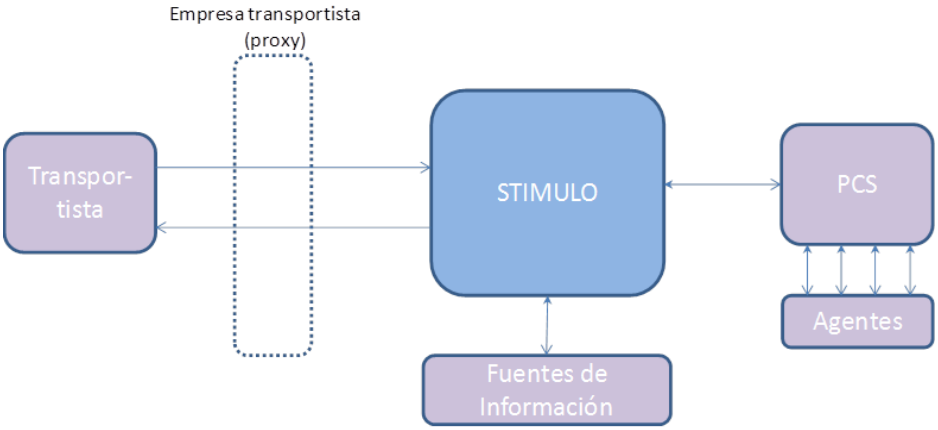

Figura 72. Componentes del sistema STIMULO

Estos bloques representados son los siguientes:

- STIMULO: Representa el núcleo del sistema, proporciona la inteligencia e interacciona con el resto de módulos y agentes implicados en el servicio.
- PCS (Port Community System): Es el sistema actualmente en uso en el puerto de Valencia. El PCS interactúa principalmente con el bloque principal (STIMULO), para solicitar una previsión de llegada de uno o más vehículos vinculados a una o varias órdenes de transporte (OT).
- Agentes: representa a todos los agentes que interactúan actualmente con el PCS. Aunque esta interacción ya está operativa, es interesante considerarla porque alguno de los mensajes (interacciones) de los agentes puede suponer representar un evento para STIMULO.

- Fuentes de información: Representa a todos los sensores externos capaces de proporcionar información relevante para estimar el tráfico en un tramo o ruta concreta. Algunos ejemplos son las cámaras de tráfico del Ayuntamiento de Valencia, de la DGT y de la Generalitat Valenciana y Catalana. Otros ejemplos puedes ser páginas web de la DGT con información de tráfico, redes sociales, etc.
- Transportista (TR): representa el elemento remoto y móvil que interactúa con STIMULO para señalizar su posición y obtener planes de ruta. El colectivo de transportistas se divide básicamente en dos grupos: empresas transportistas con sistemas de gestión de flotas y autónomos. Por simplicidad, se va a suponer inicialmente un TR que interactúa directamente con STIMULO. Aunque es posible la existencia de una empresa transportista en medio de ambas, actuando a modo de proxy transparente (como en la Figura 72).

6.3.2. Bloques de STIMULO

El principal componente es lo que se ha denominado el core de STIMULO, el cual está formado por un conjunto de bloques o módulos, dando lugar a una visión más compleja (asimilable en cierto modo a un sistema de sistemas). En la Figura 73, se representan todos estos módulos. Se trata básicamente de una arquitectura SOA (Service Oriented Architecture). La arquitectura es distribuida de tal forma, que los bloques se ejecutan en equipos físicos diferentes, aunque se puede observar una parte central, denominada Core, que agrupa una serie de servicios básicos:

- Generador de mapas: es el bloque encargado de generar un mapa para proceder a su simulación y calcular las rutas de los diferentes camiones.
- Modelado de tráfico: es el encargado de generar el tráfico de fondo a partir de la información en la BBDD.
- Sensor Observation Service: Servicio que ofrece una manera uniforme de integrar sensores por parte de terceros mediante estándares de comunicación (SensorML y O&M).
- Adquisición de datos: es un metabloque encargado de obtener datos desde diferentes fuentes.
- Centro de notificación: Se trata de un sistema que registra los eventos (alarmas) producidos por el sistema. Los diferentes módulos, son capaces de generar eventos que son enviados al Centro de Notificación, a los que cualquiera puede acceder mediante la subscripción.

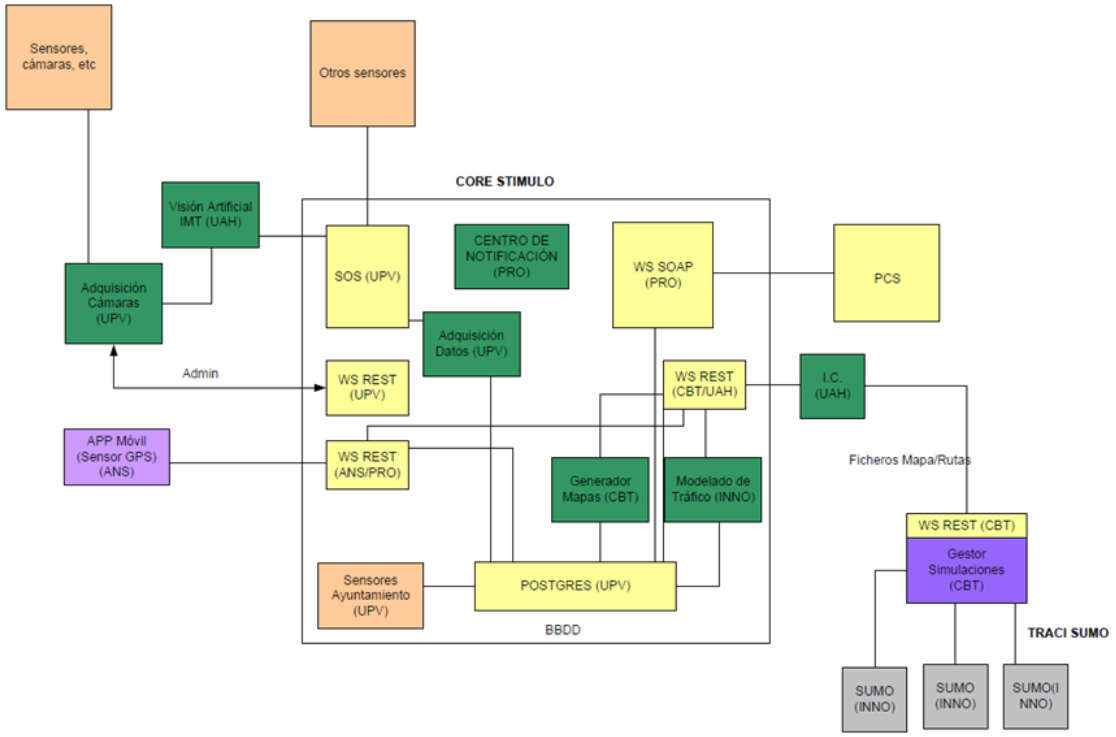

Figura 73. Principales bloques del componente servidor de STIMULO

Al margen de lo que se ha enmarcado como Core STIMULO cabe describir brevemente los siguientes elementos externos:

- Existe un módulo específico de adquisición de cámaras, que permite obtener imágenes de cámaras de tráfico y enviarlas al módulo de Visión Artificial (VA). Este módulo procesa la imagen y extrae una serie de conclusiones, típicamente un valor de IMT (Índice Medio de Tráfico) en su tramo de observación correspondiente, que luego se introduce en el SOS, (se percibe como un simple sensor).
- Existe un módulo de Inteligencia Colectiva (IC) encargado de realizar cálculos y predicciones de llegada de uno o varios camiones, estableciendo planes de ruta óptimos para cada uno de ellos.
- El Gestor de Simulaciones es otro módulo externo que permite gestionar varias simulaciones de SUMO, ofreciendo un API de alto nivel al módulo IC.
- La aplicación móvil es el módulo externo que interactúa con el TR ofreciéndole un interfaz para acceder a los servicios de STIMULO (previsión de llegada, planes de ruta, paradas).
- El PCS no es un módulo propiamente de STIMULO, pero es un módulo externo que interactúa con el sistema para obtener previsiones de llegada y facilitar OTs.

6.3.3. Arquitectura del SAC y VA

El bloque más interesante para el desarrollo de esta tesis, es el referente al Sistema de Adquisición de Cámaras (SAC) y el módulo de Visión Artificial. Es necesario un sistema capaz de obtener datos de múltiples fuentes (cámaras o sensores) y a continuación almacenarlos en un repositorio común al que tengan acceso diferentes actores. Por tanto, se aplica la arquitectura I3WSN. Como se puede ver en la Figura 74, el bloque de obtención de datos corresponde al SAC y el módulo VA, ya que son los encargados de obtener datos para el sistema. El Core de STIMULO contiene los bloques de procesado de los datos, gestión del sistema, y representación de los datos.

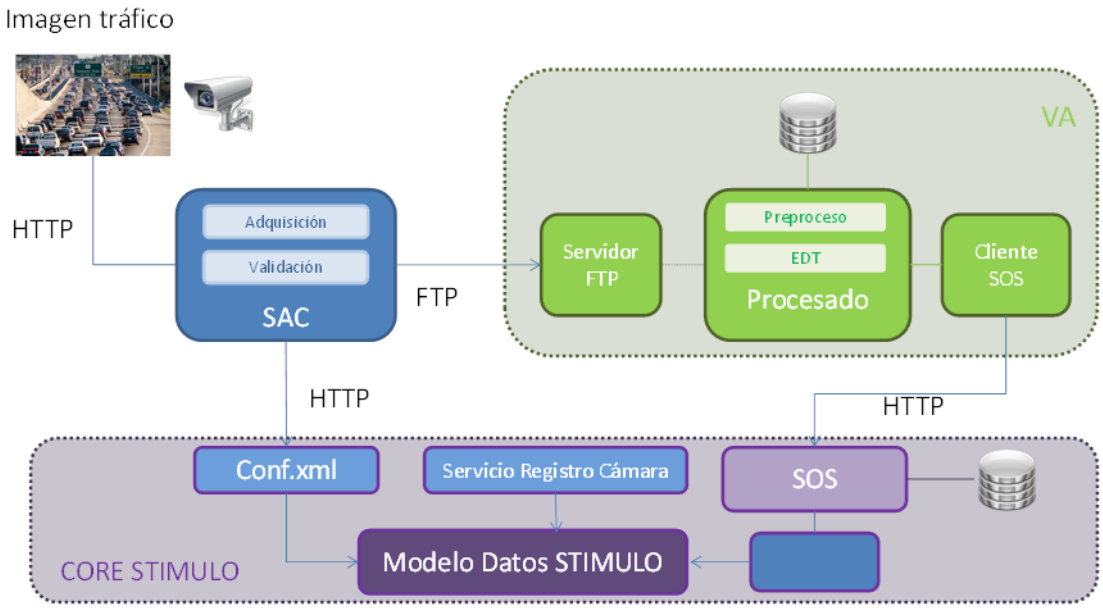

Figura 74. Arquitectura SAC-VA

El módulo SAC está compuesto de dos bloques principales:

- Adquisición: consiste en obtener (descargar) las imágenes de tráfico vía HTTP.
- Validación: consiste en comprobar que la imagen es válida (no es corrupta). Adicionalmente, el bloque de validación también comprueba la resolución, para ofrecer un formato homogéneo.

Una vez las imágenes llegan al módulo de VA, se realiza un procesado con dos funciones principales:

- Preproceso: su objetivo es acondicionar las imágenes para que éstas puedan ser procesadas por el módulo de Estimación de la densidad de tráfico (EDT). Detecta cámaras fuera de servicio, imágenes repetidas, mejora la calidad o diferencia entre día y noche
- Estimación del EDT: Se trata de la funcionalidad específica que proporciona una estimación del IMT por imagen.

Por último, una vez se obtiene el valor de ITM de una cámara para un instante determinado, se envía al SOS para que pueda ser utilizado más adelante en el modelado del tráfico y el cálculo de las rutas.

6.4. Funcionamiento de STIMULO

6.4.1. Fuentes de datos

La gestión de tráfico no sería posible sin una fuente fiable de adquisición de datos, tanto reales como históricos. Los dispositivos móviles están relacionados con el intercambio de información y geolocalización, y hoy en día, suponen una de las fuentes de datos más importantes para obtener información sobre el tráfico real.

A través de estos datos se puede conocer la posición de vehículos, tener en cuenta la velocidad de circulación y por tanto, el estado de tráfico en un determinado espacio y tiempo. Esto permite proporcionar información útil, para ayudar a la gestión del transporte de mercancías y la propuesta de itinerarios inteligentes para la mejora de la optimización de entregas en las empresas.

Las principales fuentes de datos de las que el sistema STIMULO se provee para su funcionamiento son las siguientes:

Datos de tráfico

Para poder disponer de un modelo de tráfico con cierto grado de fiabilidad que permita generar estimaciones útiles (tiempo de llegada de los camiones), es necesario disponer de información externa sobre el estado de tráfico, tanto urbano como de carretera. Esta información proviene de diferentes fuentes externas, que se pueden asimilar a sensores. Existen dos elementos de los que poder obtener el estado del tráfico: las cámaras de tráfico y las espiras que cuentan el número de vehículos.

Las imágenes de las cámaras de tráfico se obtienen, vía HTTP (URLs), de las administraciones que ofrecen este servicio, como son el Ayuntamiento de Valencia (AYV), la DGT y la Generalitat de Cataluña (GC). En el caso de las cámaras de la Generalitat Valenciana (GV) es necesario una transcodificación, ya que únicamente ofrecen de video en tiempo real.

Dentro de la ciudad de Valencia, el Ayuntamiento también proporciona el número de vehículos por hora en algunas de las principales vías. Para ello, utiliza los sensores de tráfico o espiras que están situadas bajo la calzada.

Modelo de tráfico

De forma general, llamamos demanda de tráfico al conjunto de datos a partir de los cuales es posible definir el comportamiento del sistema en un determinado periodo de tiempo. En los sistemas de tráfico vehiculares intervienen muchos factores tanto

externos como internos, que hacen complejo su modelado. Para abordar este reto se debe dividir el sistema en tareas más sencillas que permitan su correcto desarrollo.

El primer paso a la hora de poder comenzar a simular un escenario determinado es obtener una demanda de tráfico o planificación inicial de la dinámica que van a seguir los vehículos que participan en ella. Esto implica generar, a partir de unos datos estadísticos o un modelo de comportamiento determinado, una serie de planes de viaje que describan cómo van a realizarse los desplazamientos de acuerdo con las restricciones especificadas por los datos de entrada iniciales.

La aproximación llevada a cabo dentro del proyecto STIMULO, consiste en generar en primera instancia, un estado inicial a partir del modelo de tráfico. Este estado inicial, debe reflejar un comportamiento de la red basado en la información histórica de los volúmenes de tráfico obtenidos de fuentes con poca granularidad (ej. históricos anuales ofrecidos por la DGT). Este comportamiento debe combinarse con información estadística que permita cubrir de forma verosímil las zonas en las que no se tiene recogida información empírica.

El modelo de tráfico inicial debe ser actualizado con los diversos sensores externos, fundamentalmente cámaras de la DGT, la Generalitat de Catalana y Valenciana, que proporcionarán valores de IMT.

Mapas de carreteras

El componente IC necesita una representación estructurada de las carreteras, a fin de realizar los cálculos necesarios para obtener una Previsión de Llegada (PLL) dado un punto de partida, un punto destino y una serie de puntos intermedios. Esta representación estructurada tiene las siguientes características:

- Representar las calles y carreteras y sus intersecciones, es decir, debe ser topológicamente fiel a la realidad de la red.
- Contener información de la velocidad permitida en cada tramo.
- Contener información sobre número de carriles y sentido de la circulación.
- Contener información sobre ubicación de semáforos.
- Contener información sobre giros permitidos en cada intersección.

Como origen de datos, se ha utilizado la base datos vectorial OpenStreetMap (OSM) [233]. Contiene información sobre carreteras, siguiendo el esquema arco-nodo, y otras infraestructuras. Cada elemento tiene asociadas un número ilimitado de etiquetas, algunas de las cuales son útiles en el contexto del modelado de tráfico.

Planificación de transporte (PCS)

El sistema STIMULO dispone de un servicio básico, que corresponde a la previsión de llegada de un camión determinado al Puerto de Valencia y a la terminal que le

corresponde. Para ello, necesita conocer los datos en tiempo real de carga, salida, destino, etc. de los distintos camiones de transportes de mercancías. El sistema que utiliza el puerto para dicha gestión es el PCS.

Todos los datos necesarios están recogidos en un documento portuario llamado 'Orden de transporte' el cual se envía al Core de STIMULO. Este documento contiene:

- Matrícula del camión
- Tipo de operación (importación/exportación)
- Punto de recogida del contenedor (terminal/depósito)
- Punto de carga/descarga del contenedor
- Punto de entrega del contenedor (terminal/depósito)

6.4.2. Obtención de IMT

Para poder adquirir la información de las cámaras de tráfico, es necesario que dichas cámaras estén registradas en el sistema. Esta información es almacenada en el modelo de datos.

Cuando se han obtenido todas las imágenes de tráfico de las distintas cámaras, se validan: se comprueba que no son corruptas y se establece un formato homogéneo (resolución, tamaño y nombre).

Una vez se dispone de una imagen válida por parte del SAC, se envía al módulo de Sistema de Visión Artificial (SVA). Éste incorpora como front-end un servidor FTP donde se almacenan estas imágenes.

A medida que las imágenes llegan al módulo de VA se realiza un procesado con dos funciones principales:

- Preproceso: Evalúa y mejora las imágenes previamente a ser procesadas con el fin de optimizar los recursos. Las principales funciones que se desarrollan en este bloque son:
    - Descartar imágenes que no corresponden con una imagen útil para procesar. En ocasiones, las cámaras de tráfico se encuentran fuera de servicio, lo que se refleja en una imagen tipo, a título informativo, que no hace falta procesar.
    - Detectar imágenes repetidas. El módulo las detectará y descartará, de modo que el bloque EDT no tenga que procesarlas.
    - Mejorar la calidad. Se encarga de aplicar algoritmos de superresolución y de tratamiento digital de imágenes que mejoren la calidad de éstas. Esta funcionalidad se hace necesaria debida a la muy baja resolución de las imágenes proporcionadas por las fuentes identificadas.

- Estimar condiciones de luminosidad (día/noche). El sistema identifica de forma automática si se trata de un escenario de día o de noche, de modo que los parámetros puedan ajustarse en consecuencia.

- Estimación de la densidad de tráfico (EDT): Es el parámetro necesario para el cálculo de IMT. El procesado se realizará utilizando técnicas de visión artificial para la detección eficiente de vehículos en imágenes de baja resolución. El módulo empleará la librería de software libre OpenCV. En concreto, este módulo de la arquitectura obtendrá el IMT tras realizar una estimación del número de vehículos en la escena. Al no poderse disponer de vídeo, ésta estimación se realizará en cada una de las imágenes de forma aislada. De este modo, según el tipo de vía y la cantidad de vehículos detectados, se procederá a realizar un cálculo de IMT, que será comunicado al cliente SOS.

A medida que se estima el valor de IMT de las distintas cámaras, se envía al servidor SOS con el fin de utilizar estos datos para el cálculo de las rutas óptimas. Cada valor de IMT se almacena en el SOS como una medida de la cámara en el instante en el que se ha tomado la imagen evaluada.

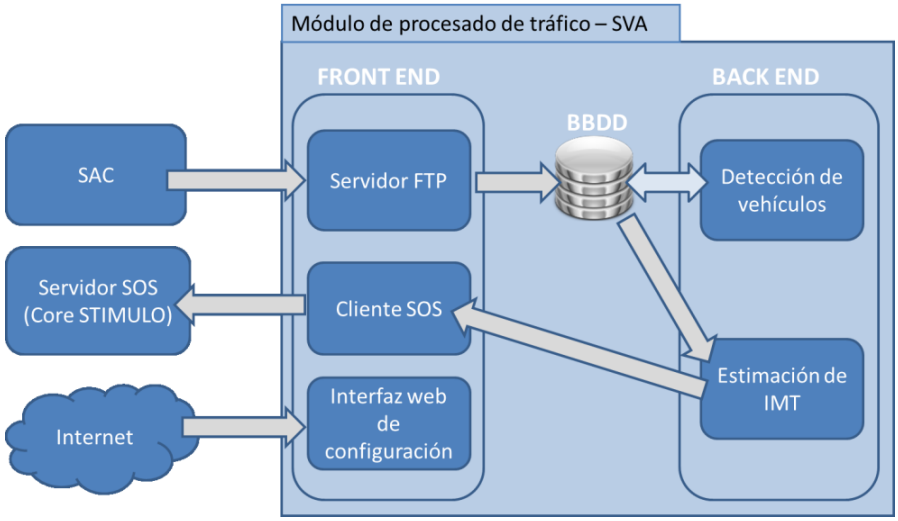

Figura 75. Descripción del SVA

6.4.3. Inteligencia colectiva y simulación

Inteligencia colectiva

El módulo de Inteligencia Colectiva o IC, es el núcleo del sistema de gestión de rutas dentro de STIMULO. En este módulo se desarrollan las funcionalidades relativas a la planificación optimizada de la llegada de vehículos a su destino. Su principal objetivo es ser capaz de ofrecer planes de viaje que permitan cumplir con las restricciones que imponga el punto de destino (en este caso el puerto), al mismo tiempo que se tienen en cuenta las preferencias de cada uno de los vehículos. El módulo también tendrá en cuenta la información que puedan aportar los diferentes vehículos (estado de la

carretera, modificaciones en su orden de transporte, etc.) de forma que pueda reaccionar ante eventos no reflejados en la planificación original.

Para llevar a cabo dicha optimización, el módulo se basa en varias fuentes de datos. Por una parte, el módulo toma como punto de partida las órdenes de transporte obtenidas de la base de datos de STIMULO, que permiten definir los vehículos que se deben planificar en un tiempo determinado. A partir de dichas órdenes de transporte, el módulo extraerá los puntos por los que debe pasar el vehículo (puntos de recogida, carga/descarga y entrega) y también las restricciones horarias que puedan existir para cada uno de estos puntos.

Junto con las órdenes de transporte, se tienen en cuenta otra serie de datos auxiliares como son las preferencias de dichos vehículos y las preferencias del destino al que se dirigen. Dentro del conjunto de preferencias relativas a los vehículos, se tienen en cuenta parámetros que engloban las diferentes variables que hacen que un conductor pueda estar más o menos satisfecho con el plan de viaje asignado. Esto incluye tanto parámetros que provengan del propio conductor (duración del viaje, número de paradas), como parámetros que puedan venir impuestos por la empresa transportista: consumo de combustible, emisiones de CO2, duración de las paradas, etc. El procesamiento de las preferencias de los vehículos se divide en dos fases: la especificación de la fuente de datos para cada uno de los atributos que se tienen en cuenta y la descripción de las funciones de evaluación para cada uno de dichos atributos.

Simulación

Uno de los elementos clave en el sistema STIMULO para la planificación de las rutas, es la utilización de un sistema de simulación de tráfico que permita la obtención de datos sobre el escenario en el que se va a llevar a cabo la optimización de rutas y planes de viaje. En este sentido, es necesaria la utilización de un sistema de simulación que permita la inclusión del escenario real sobre el que se van a mover los vehículos, el modelado de un patrón de tráfico de fondo de los vehículos que circulan por dicho escenario, así como la posición real de los camiones.

Sobre este escenario, se llevan a cabo una serie de simulaciones modelando los vehículos a evaluar y los planes de viaje (rutas, tiempos de salida, tiempos de parada, etc.) que deben llevar cada uno de ellos. Con estas simulaciones se obtiene una serie de datos que predicen el comportamiento de los vehículos en el escenario real, y por tanto, sirven de base para la evaluación de dichos planes de viaje. Concretamente, se obtienen datos sobre los tiempos de llegada de los vehículos y su adecuación a los tiempos estimados anteriormente, pero también datos sobre otros elementos que definen las preferencias de cada uno de los vehículos (es decir, datos sobre emisiones de CO2, distancia recorrida por cada uno, adecuación de las paradas realizadas, consumo de combustible, etc.). Estos datos adicionales hacen que la evaluación de cada plan completo sea más detallada y cercana a la realidad.

El software utilizado como base para su utilización en este proyecto es SUMO (Simulation of Urban MObility) [234]. Este sistema permite simular una determinada demanda de tráfico consistente, en vehículos individuales moviéndose en una red de carreteras determinada, teniendo en cuenta un gran número de características propias de los sistemas de tráfico vehicular. Se trata de un sistema de simulación microscópica, esto significa que cada uno de los vehículos a simular se modelará de manera independiente y explícita, y cada uno de estos modelos definirá una ruta propia, moviéndose de forma independiente en la red. Este tipo de modelado se contrapone a otros sistemas macroscópicos donde se definen flujos de vehículos y características comunes entre ellos.

El paquete SUMO ofrece una serie de funcionalidades relacionadas con la simulación, que permitirán añadir precisión y versatilidad a las simulaciones llevadas a cabo en el contexto del proyecto STIMULO. La principal funcionalidad ofrecida, como ya se ha comentado anteriormente, es la capacidad de realizar simulaciones tomando como parámetros la red de carreteras y las rutas a seguir por cada vehículo, y la capacidad de generar resultados a partir de dichas simulaciones. Además, ofrece las siguientes funcionalidades:

- Capacidad de simular el movimiento de los vehículos de forma continua en el espacio y discreta en el tiempo.
- Capacidad de modelar diferentes tipos de vehículo en una única simulación.
- Aceptación de redes de carreteras que modelen calles multi-carril (los vehículos simulan el cambio de carril dentro de una misma carretera).
- Modelado de reglas de prioridad en cruces y de semáforos.
- Inclusión de una interfaz gráfica de usuario.
- Capacidad de gestionar redes de carreteras grandes, de decenas de miles de enlaces.
- Simulación rápida de cargas de tráfico vehicular elevadas.
- Interoperabilidad con otras herramientas durante la ejecución de las simulaciones
- Obtención de resultados basados en la red, en cada enlace, en cada vehículo o en detectores configurados previamente en cualquier punto de la red.
- Capacidad de utilización de datos de diversas fuentes (VISUM, Vissim, Shapefiles, OSM, RoboCup, MATsim, OpenDRIVE, y otras descripciones basadas en XML)
- Capacidad de estimar valores a partir de heurísticas.
- Capacidad de cálculo de rutas (individuales para cada vehículo) utilizando algoritmos DUA (Dynamic User Assignment).
- Alta portabilidad mediante el desarrollo en C++ estándar y la utilización de librerías estándar.

- Ejecución multiplataforma: versiones Windows y Linux.
- Alta interoperabilidad: Todos los datos de entrada y salida se modelan utilizando únicamente XML

En la Figura 76, se detalla la integración de la plataforma de simulación en el sistema STIMULO a través de su utilización por parte del módulo de Inteligencia Colectiva. Este módulo se encarga de realizar la optimización de los planes de viaje, por lo que proveerá de datos y a su vez recuperará datos del simulador, con el objetivo de realizar dicha tarea de optimización. La comunicación entre ambos módulos se lleva a cabo mediante los siguientes eventos:

1. En cada iteración del módulo de Inteligencia Colectiva, se obtienen del modelo de datos los datos de entrada utilizados por el simulador (vehículos a simular, datos del escenario, etc.).
2. Estos datos se pasan al simulador indicándole todos los parámetros de configuración de la simulación.
3. La plataforma de simulación lleva a cabo la ejecución de una simulación, generando una serie de archivos de salida (rutas válidas para el mapa utilizado, paradas, tiempos estimados).
4. Los archivos de salida son leídos de nuevo por el módulo de Inteligencia Colectiva con el fin de obtener datos útiles para la mejora de la planificación en la siguiente iteración.

Este proceso se lleva a cabo en cada iteración del módulo de Inteligencia Colectiva, con el fin de optimizar el cálculo de dichos planes de viaje.

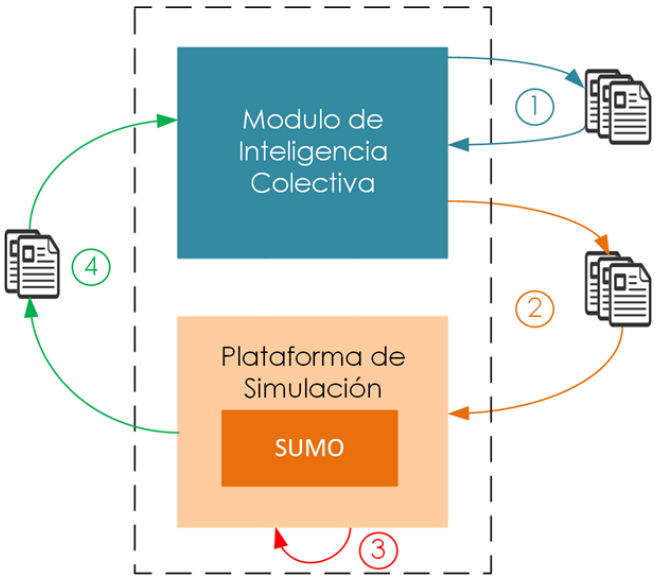

Figura 76. Plataforma de simulación

6.4.4. Modelo de datos

El modelo de datos representa una forma de referenciar todos los elementos necesarios en el sistema, su forma de ser almacenados y su relación con otros elementos.

Como base de datos se ha toma PostGRESQL, con soporte POSTGIS, de tal forma que se pueden georeferenciar cualquier elemento almacenado, así como aplicar operaciones geoespaciales. Para el modelado de la base de datos se ha empleado el Moskitt, una herramienta libre que permite generar modelos de datos y exportarlos después a PostGRESQL.

En el diagrama de la Figura 77, se puede ver el esquema del modelo de datos, donde se pueden distinguir principalmente:

- Sensores (tabla Sensor): Engloba a todas las fuentes de datos disponibles. Además existen otras dos tablas que permiten diferenciar entre cámaras de tráfico (Cameras) y espiras (traffic_counter).
- Camión (tabla lorry): Se almacena toda la información relativa a los camiones como puede ser su empresa, posición, orden de transporte, etc.
- Alarmas (tabla alarms): Todas las alamas que pasan por el centro de notificaciones se almacenan en el modelo de datos para tener un histórico de todos los eventos.
- Rutas (tabla routes): Las rutas planificadas para todos los camiones, después que la inteligencia colectiva determine cuál es la ruta óptima.
- Órdenes de transporte (tabla transport_order): Las órdenes de transporte reales que envía el puerto de Valencia a través del PCS.
- Eventos (tabla events): Log de todos los eventos que ocurren en el sistema, ya sea la generación de una nueva ruta o el comienzo de la ruta de un camión.
- Plano (tablas osm_roads, osm_service_points, ect.): Todas las vías y áreas de descanso necesarias para realizar las simulaciones.

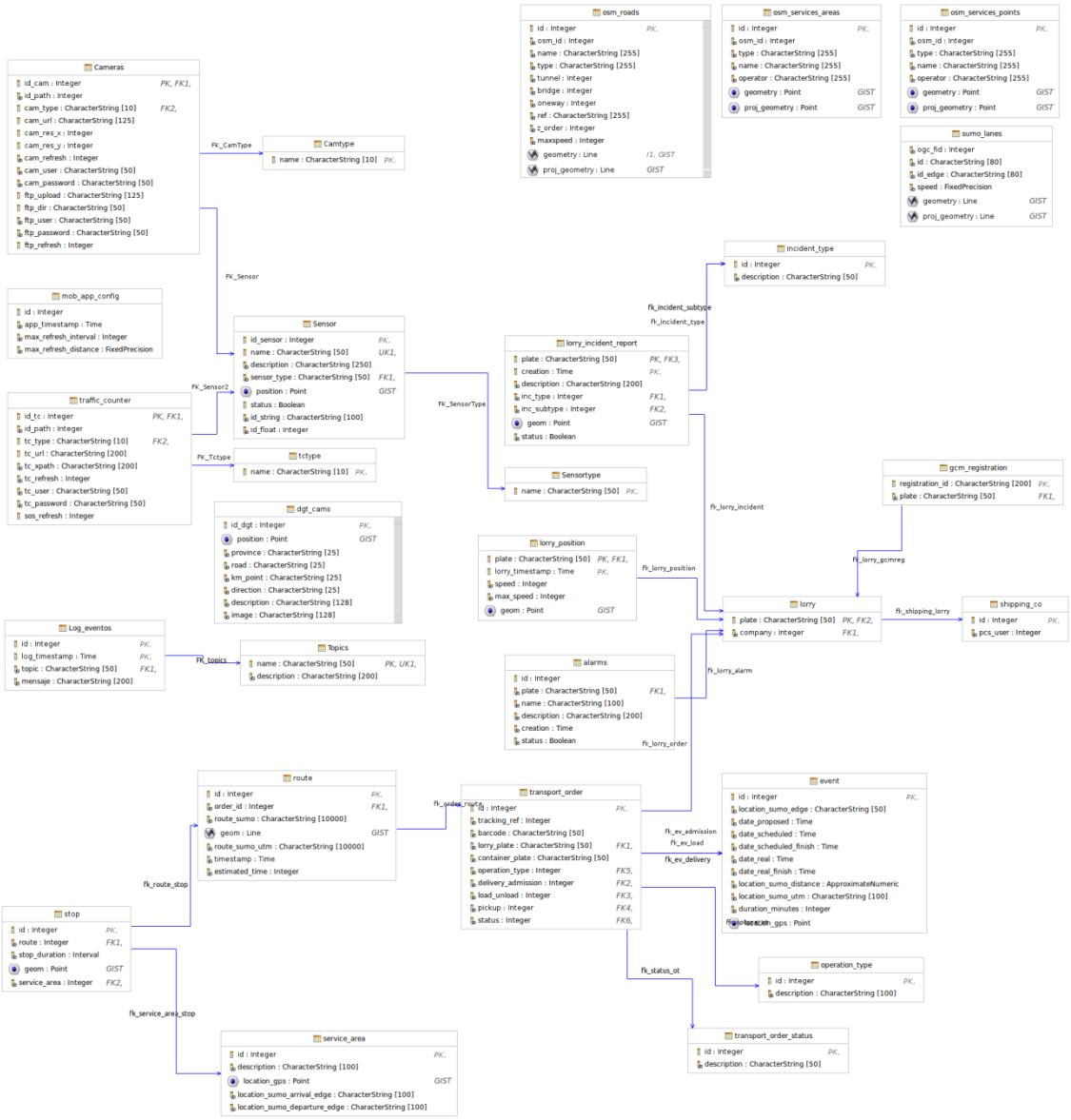

Figura 77. Modelo de datos

6.4.5. HMI

Para poder gestionar las fuentes de datos, principalmente las cámaras y las espiras, se ha desarrollado un interfaz de administración que permita dar de alta y visualizar los datos obtenidos. El HMI se ha implementado como una aplicación web para facilitar el acceso desde cualquier lugar y dispositivo.

Pantalla de inicio

Una vez iniciada la sesión con el usuario y la contraseña, se accede a la página de inicio (ver Figura 78), desde la cual se puede acceder a la parte de configuración de las fuentes de datos o monitorizar el sistema.

Figura 78. Pantalla de inicio

Configuración

Si se accede al menú de configuración (ver Figura 79), se pueden ver las distintas fuentes de datos que existen actualmente en el sistema. En este momento, se están utilizando las cámaras para obtener el valor de IMT de las distintas vías seleccionadas y espiras para obtener el número de vehículos por hora qué están disponibles en la ciudad de Valencia.

Figura 79. Fuentes de datos

Cámaras

La principal fuente de información para STIMULO son las cámaras de tráfico. En el menú de cámaras (ver Figura 80), se pueden ver todas las cámaras de tráfico registradas hasta el momento. En el listado de cámaras aparecen en verde aquellas que se están utilizando para el cálculo del IMT y en rojo aquellas que no. A la derecha, están las distintas acciones que se pueden realizar, como son:

- Dar de alta una nueva cámara.
- Ver y editar los datos de una cámara ya registrada.
- Borrar cámaras.
- Activar una o varias cámaras para que sus imágenes sean procesadas.
- Desactivar cámaras.
- Ver el fichero XML de configuración con todos los parámetros de las cámaras, para que una aplicación externa, como puede ser la visión artificial, pueda acceder a ellas.

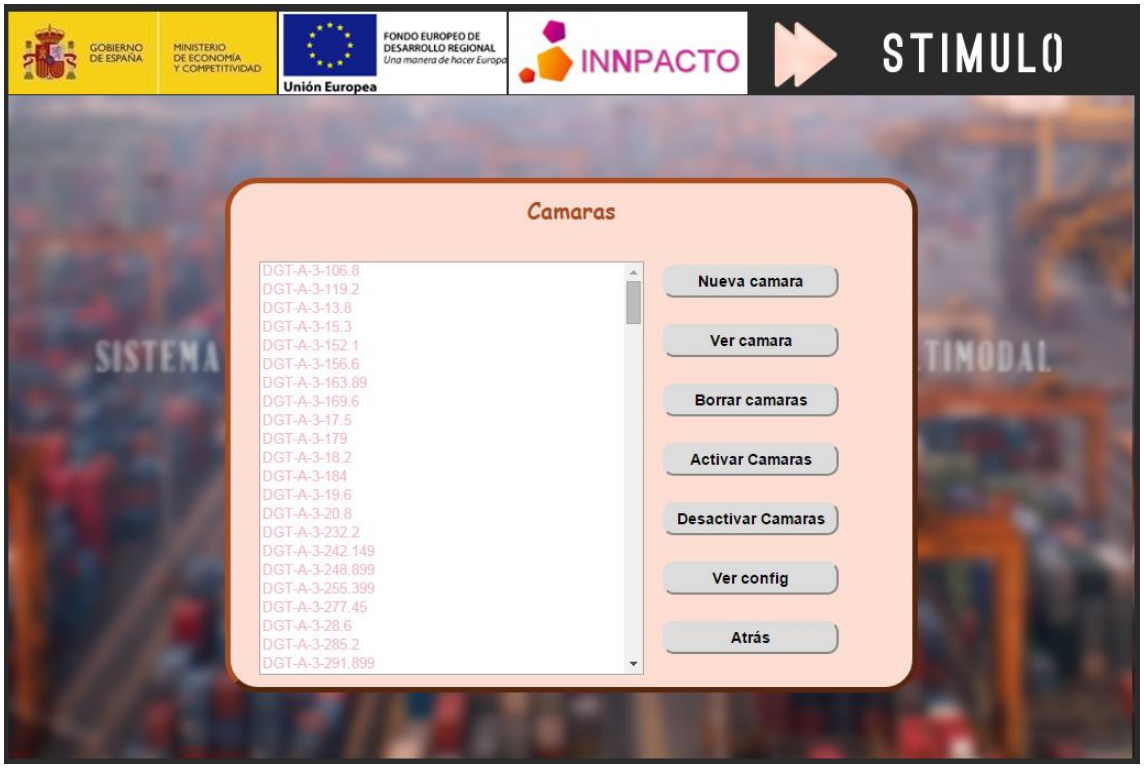

Figura 80. Menú de cámaras

Insertar nueva cámara

Cuando se accede al menú para dar de alta una nueva cámara o para editar alguno de sus campos, se visualiza el formulario de la Figura 81. Los principales parámetros de cámara son:

- Nombre: Es el nombre con el que está registrada en STIMULO.
- Tipo: Propietario al que pertenece la cámara.
- Latitud y Longitud: Posición de la cámara.
- URL: Dirección original de donde se obtienen las imágenes.
- Refresco: Frecuencia con la que se actualizan las imágenes.
- Resolución: Resolución en la que están las imágenes originales.
- FTP: Servidor FTP al que se envían las imágenes (URL, usuario y contraseña).

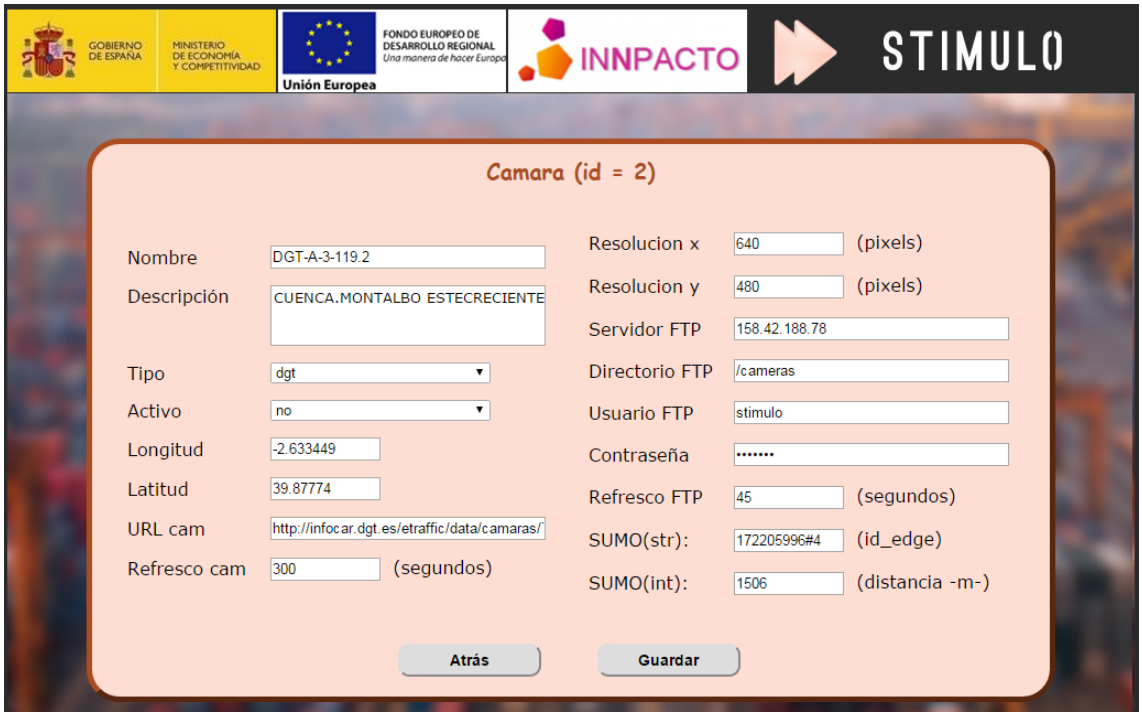

Figura 81. Menú de edición de una cámara

Espiras

Además de las cámaras también se obtiene información de las espiras de tráfico. Al igual que en el caso anterior en el menú de contadores (ver Figura 82) se tiene una lista con todas las espiras. Las acciones disponibles son las mismas que en el caso anterior. A diferencia que con las cámaras, los datos de las espiras no se envían a un servidor FTP, sino que se insertan de forma directa en el servidor SOS.

Figura 82. Menú de contadores

Servicios

Una vez se han dado de alta todas las cámaras y las espiras, se debe iniciar el servicio (SAC) para obtener las imágenes, validarlas, y enviarlas al servicio de Visión Artificial, en el caso de las cámaras de tráfico. En el caso de las espiras, se debe insertar el número de vehículos por hora en el SOS.

Para ello, en el menú de servicios (ver Figura 83), se dispone de botones que permiten activar y desactivar de forma independiente ambos servicios.

Existe un tercer servicio el cual proporciona acceso a los datos del SOS, mostrando el último valor obtenido y la fecha en la que se produjo.

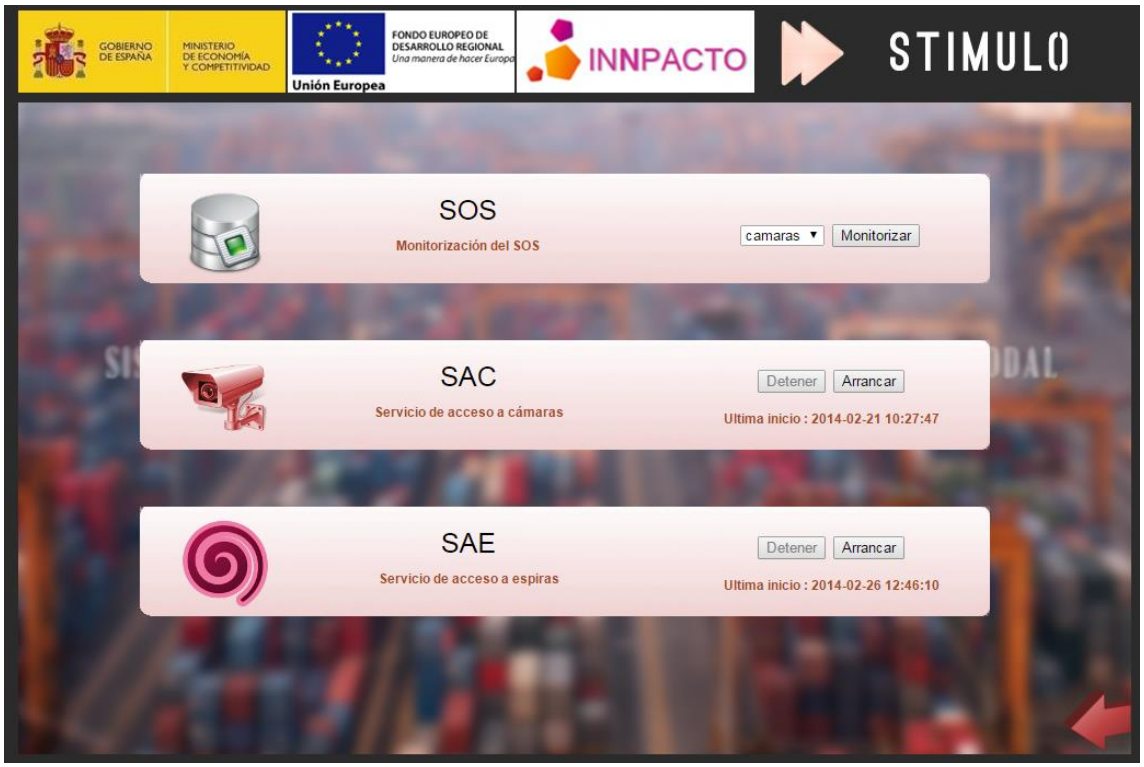

Figura 83. Menú de servicios

6.4.6. Aplicación móvil

El transportista representa el elemento remoto y móvil que interactúa con STIMULO para señalizar su posición y obtener planes de ruta. El colectivo de transportistas se divide básicamente en dos grupos: empresas transportistas con sistemas de gestión de flotas y autónomos. Ambos se contemplan en STIMULO.

El objetivo principal es el desarrollo de una herramienta móvil, que recopile información geoposicional de cada vehículo, y que se encargue de mostrar al usuario la información recibida desde el servidor sobre la ruta óptima o posibles rutas alternativas, así como otra información relativa a la vía en la que circula.

Los datos que la aplicación móvil debe enviar al sistema son:

- Datos de login: matrícula y orden de transporte.
- Eventos con fecha: Comienzo de transporte, parada, recogida de contenedor, carga o descarga de contenedor y entrega o admisión.
- Localización inicial y envío de localizaciones sucesivas cuando empieza el transporte: coordenadas GPS.
- Velocidad a la que circula el vehículo.
- Incidencias que pueda ver en carretera (localizadas).

Desde el módulo de comunicación se enviará al dispositivo móvil:

- Ruta inicial y paradas programadas
- Posibles rutas óptimas en función de su posición y las incidencias en carretera.
- Alarmas (en la ruta o en el punto de destino generales).
- Incidencias (en la ruta y geoposicionadas).

La aplicación se ha desarrollado en Android para facilitar su utilización, ya que hoy en día casi todo el mundo tiene algún dispositivo con Android.

En las Figura 84, se puede ver el interfaz diseñado para la aplicación móvil. En la imagen se ve la pantalla de login inicial, en la que el transportista introduce la matrícula y la contraseña para registrarse en el sistema.

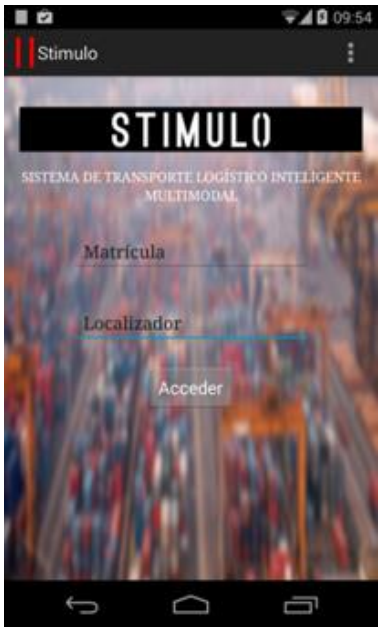

Figura 84. Diseño de la pantalla de login

Una vez el transportista está registrado se accede a la página de inicio (ver Figura 85), en la que se verá el mapa con la ruta y permite también navegar entre las distintas opciones de la aplicación.

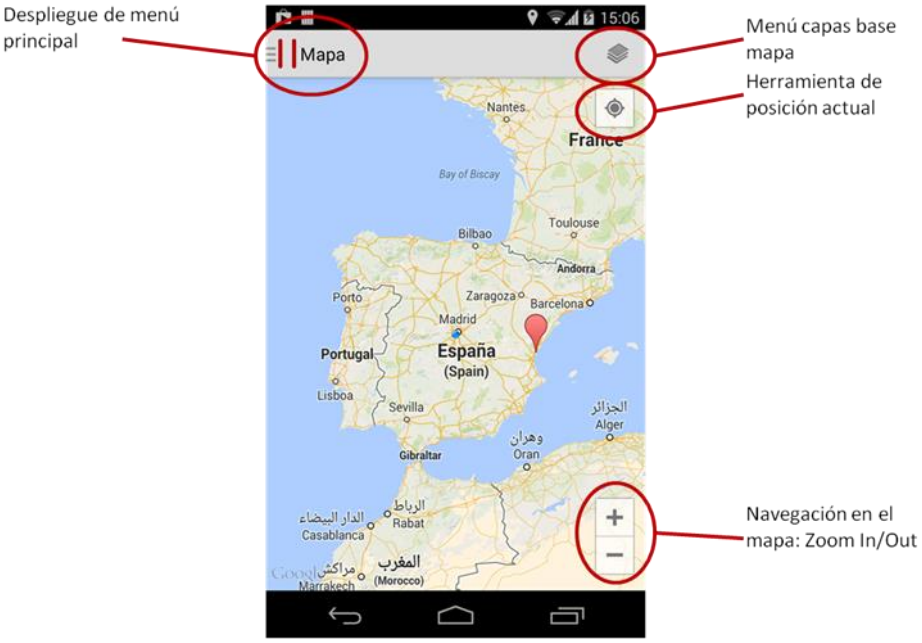

Figura 85. Pantalla principal de la aplicación

Una vez le asignan una ruta al transportista, esta estará representada en el mapa con las zonas de carga y descarga, y las paradas previstas para cumplir los tiempos establecidos (Figura 86). Cada vez que el transportista realiza una acción (llegada al punto de carga, llegada al punto de descarga, etc.) debe indicarlo en la aplicación, para que el sistema evalúe y optimice el tiempo.

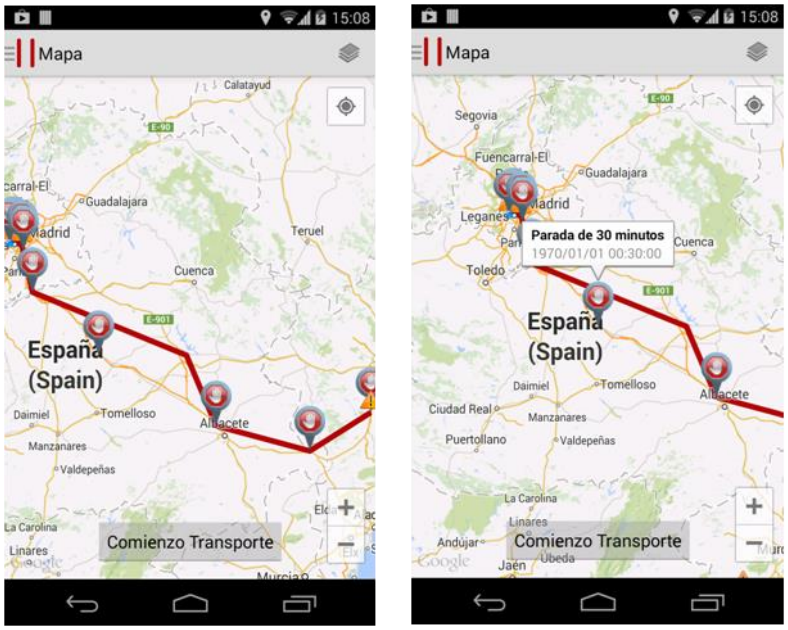

Figura 86. Diseño de la pantallas de plan de viaje

6.5. Logros de STIMULO

Actualmente vivimos en una revolución caracterizada por la ubicuidad, tanto de los sistemas de posicionamiento global, como de las TIC. Gracias al desarrollo de estas dos áreas, los sistemas de transporte inteligente pueden dar un nuevo salto cualitativo en la optimización de los procesos. STIMULO pretende unir áreas como la visión artificial, las técnicas de inteligencia colectiva, los sistemas de localización abordo y los mecanismos de simulación de vehículos para conformar un sistema que sea capaz de realizar predicciones más precisas y enriquecidas.

Los principales avances que ha logrado STIMULO han sido:

- Se ha definido una arquitectura modular y completamente multiplataforma, desplegando los componentes sobre un servidor Linux y utilizando diferentes estándares de mensajería y comunicación de datos, atendiendo tanto servicios propios como servicios externos.
- El despliegue de cámaras, con acceso abierto a sus imágenes, posibilita una monitorización del estado del tráfico que permite modelar y verificar un modelo de transporte capaz de predecir y planificar la llegada de un conjunto de camiones a un destino determinado.
- El sistema de procesado de imagen (Visión Artificial) es capaz de reconocer vehículos en condiciones muy adversas, producidas tanto por la baja resolución como por el ruido presente en dichas imágenes. Para paliar estos efectos, se ha recurrido a dos métodos: la superresolución, consistente en ampliar el tamaño de la imagen sin pérdida de calidad y la detección de las vías (áreas de interés), para mejorar la localización de los vehículos y evitar falsos positivos.
- La estimación del valor de IMT en las vías monitorizadas se realiza mediante técnicas de visión artificial, que utilizan la capacidad de procesado de la GPU para realizar una detección de vehículos utilizando características HOG.
- A partir de los datos de simulación de SUMO y de los datos obtenidos mediante distintos medios sobre la velocidad de vehículos en instantes periódicos prefijados, se ha podido realizar un primer modelo de tráfico y comprobar su grado de validez siguiendo el proceso a la inversa.
- La integración de los datos del proyecto OpenStreetMap, son una fuente de información importante para definir las carreteras y vías necesarias, con el fin de realizar el Modelo de Tráfico y calcular las rutas óptimas mediante la simulación.
- El módulo de Inteligencia Colectiva es el responsable de proporcionar mecanismos para la optimización distribuida de los planes de viaje de los camiones, de manera que se cumpla la planificación de llegadas al puerto, así como otras preferencias de los conductores o empresas de transporte.

7. Evaluación

7.1. Evaluación

Para poner a prueba la extensibilidad de la arquitectura propuesta en el capítulo 3, se ha llevado a cabo su aplicación en los tres proyectos de investigación descritos, en tres dominios de aplicación totalmente diferentes. Tras el proceso de especificación y desarrollo efectuado en cada uno de ellos, se va a pasar a la evaluación de los resultados.

En primer lugar, se describe el escenario inicial planteado para las pruebas en cada uno de los casos de uso, a continuación se detalla el funcionamiento del sistema particularizado para el escenario, y por último, se examinan los resultados que se han obtenido con el fin de valorar la efectividad de la arquitectura propuesta.

Debido que sería muy costoso desplegar grandes redes de sensores, para algunas de las pruebas, las WSN se simulan mediante el simulador desarrollado (véase sección 4.6). De esta forma, se pueden representar situaciones cotidianas y excepcionales, como son eventos peligrosos o comportamientos a largo plazo.

Por tanto, el capítulo está dividido en tres secciones, una por cada caso de uso. En la segunda sección, se plantea el escenario de la fábrica para FASyS. Después, en la tercera sección, se comenta la versión reducida de smart grid utilizada para probar el sistema UniverSEC. Por último, en la cuarta sección, se aplica el sistema STIMULO a la ruta de un camión de transporte de mercancías.

7.2. FASyS

7.2.1. Escenario inicial

En FASyS se han definido 13 entornos de riesgo que deben de ser monitorizados para evitar todo tipo de accidentes dentro de la fábrica. Entre ellos, se ha considerado la colisión como uno de los más graves y por tanto se ha elegido para probar el sistema. A partir de la arquitectura descrita en el capítulo 4 para FASYS, se ha diseñado un caso sencillo en el que validar su funcionamiento.

La arquitectura general del sistema consta de dos partes principales (ver Figura 87). Por un lado, se insertan en el servidos SOS los datos recogidos por los sensores (WSNs), que en este caso están recreados por un simulador de sensores, aunque incluso podrían coexistir WSNs reales. Por otra parte, está el centro de control (CC) agrega diferentes aplicaciones que toman decisiones basadas en la información disponible en el SOS, como son el CEP, el HMI y el actuador. Todos estos elementos se encuentran en un mismo servidor, aunque sería posible la conexión entre ellos, tanto por redes de comunicación por cable, como inalámbricas.

Se ha enfocado este escenario de dos formas distintas. En la primera de ellas, se utiliza un CEP para la evaluación de los riesgos, y en la segunda, la evaluación se realiza mediante la utilización de smart objects (SO).

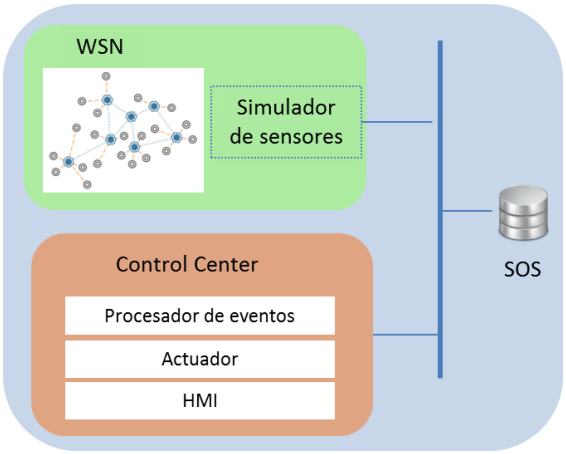

Figura 87. Escenario inicial

7.2.2. Prevención de colisiones con un CEP

Un escenario típico de seguridad, y uno de los muchos que prevé FASyS, es la detección de una colisión entre dos entidades móviles. Aunque puede implicar un trabajador o maquinaria móvil, tal vez el peor de los casos es entre dos carretillas elevadoras, como se muestra en la Figura 88.

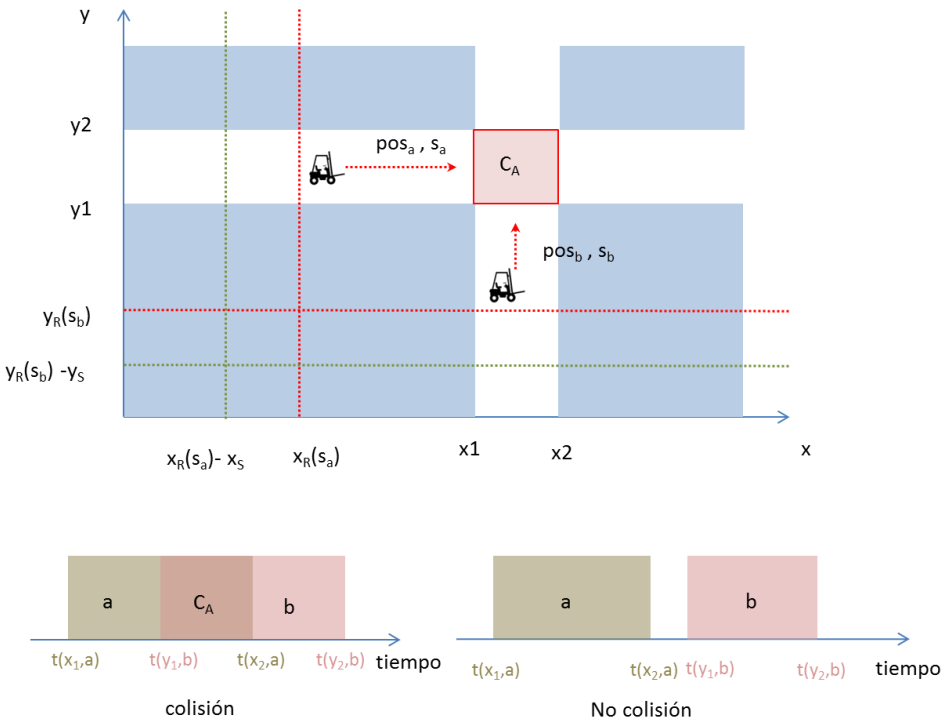

Figura 88. Detección de colisión

Como se puede ver en la imagen, el conflicto se emplaza en un posible lugar de colisión, situado en la intersección de dos pasillos dentro de una fábrica. Esta área se identifica como la zona de colisión (C_A) en la fábrica y está determinada por cuatro coordenadas (x_1, x_2, y_1, y_2).

Las carretillas elevadoras a y b están equipadas con sensores que proporcionan su posición (pos_a, pos_b) periódicamente (T_a, T_b). Para simplificar, supondremos que las carretillas elevadoras se desplazan a una velocidad uniforme, lo que facilita obtener las velocidades correspondientes (s_a, s_b) de dos posiciones consecutivas. Dependiendo de la distancia a la intersección, los conductores de carretillas elevadoras serán advertidos o no, en caso de que estén en riesgo. Esto se denota por $x_R(s_a)$ y $y_R(s_b)$, respectivamente, y está representado por las líneas discontinuas rojas en la Figura 88. Si las dos carretillas elevadoras a y b ya han traspasado las líneas rojas, entonces hay un riesgo real de colisión que se debe evitar. Tenga en cuenta que $x_R(s_a)$ y $y_R(s_b)$ dependen de la velocidad de cada carretilla elevadora, y por tanto, se ajusta a las normas tradicionales de tráfico para calcular el tiempo de frenado de los vehículos. Así, el sistema tiene que alertar a los dos conductores sólo cuando ambas carretillas elevadoras han cruzado sus líneas rojas (riesgo). De lo contrario no habrá colisión, tal como se representa en la Figura 88 en la línea de tiempo.

Con el fin de controlar esta situación, el Centro de Control debe realizar un seguimiento de la posición de cada carretilla elevadora y actuar en consecuencia. En la Figura 89, se representa el escenario para un solo vehículo, el cual inserta su posición en el SOS cada T_a segundos. Desde el Centro de Control se accede a los datos del SOS cada T_{read} segundos y evalúa si debe alertar a la carretilla elevadora a (y también al vehículo b). Alertar a ambos vehículos lleva un tiempo (T_{send}) y una respuesta (T_{ack}) de cada vehículo. Para la fábrica en cuestión, se han realizado varias pruebas y el tiempo medio (T_{send} + T_{ack}) es 200 ms, con una variabilidad de 50 ms. Si el CC considera que hay riesgo, el conductor es alertado Δx metros antes de cruzar la línea de riesgo (representado como una carretilla elevadora verde en la Figura 89). Tenga en cuenta que el conductor puede ser alertado tras cruzar la línea de riesgo (representado como una carretilla elevadora en color rojo) y por lo tanto existe un riesgo potencial. Sin embargo, dado que se alerta a ambos vehículos es posible que sea alertado a tiempo el otro conductor (b) y el riesgo de colisión disminuye significativamente.

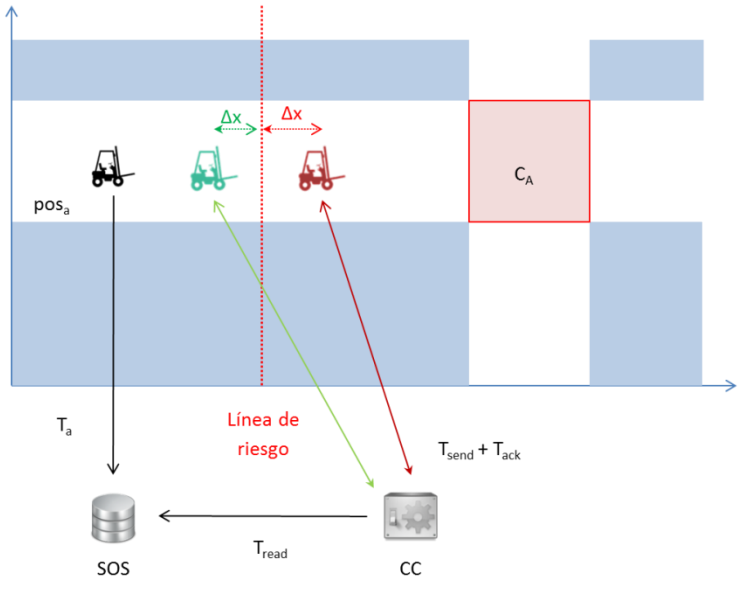

Figura 89. Seguimiento de carretillas elevadoras

Para que este hecho no se produzca y evitar alertar a los conductores a y b demasiado tarde, hay una distancia de seguridad (x_s e y_s). El CC controla si los vehículos a y b cruzan la distancia de seguridad (en vez de la línea de riesgo) con el fin de poder alertarlos antes de que crucen la línea de riesgo y tengan suficiente tiempo para frenar (las líneas de seguridad se representan en la Figura 88).

La prueba realizada para evaluar el funcionamiento del sistema FASyS consiste en comprobar si la colisión entre carretillas elevadoras puede ser evitado o no. Se ha utilizado el simulador con diferentes velocidades (s_a y s_b) con el fin de comprobar la velocidad máxima a la que se detecta con éxito el riesgo de colisión.

Los resultados se presentan en la Tabla 4 para diferentes valores de velocidad. Como puede verse, si ambas carretillas elevadoras se desplazan a una velocidad inferior a los 42 km/h (filas 1-7), ambos conductores son alertados antes de llegar al umbral definido (línea de riesgo) y podrán detenerse sin ningún peligro. Incluso si uno de los conductores se mueve con una velocidad superior (filas 8, 9), el otro conductor es alertado antes de la línea de riesgo y puede evitarse el accidente (éxito parcial). Para velocidades superiores en ambos vehículos (fila 10), los conductores son alertados tras la línea de riesgo y existe la posibilidad de que se produzca un accidente si ambas carretillas elevadoras entran en la zona de colisión (C_A).

La pérdida de datos se ha establecido en 5%. Sin embargo, para movimientos lineales y una tasa de pérdida baja, no es relevante si algún paquete (updateSensor) no llega al SOS, ya que los valores pueden ser estimados.

Tabla 4. Resultados de la simulación para el escenario de pruebas

	Speed (s_a)	**Δx (m)**	**Speed (s_b)**	**Δy (m)**	**Result**
1	18.96	0.65	22.92	1.82	Success
2	18.96	0.73	24.45	0.62	Success
3	18.96	0.67	29.03	1.09	Success
4	21.33	0.35	33.62	0.47	Success
5	24.38	1.15	33.62	0.61	Success
6	28.44	1.48	39.74	0.71	Success
7	34.13	0.88	33.62	0.36	Success
8	34.13	0.29	50.44	-2.46	Partially Success
9	42.67	-6.28	39.73	0.23	Partially Success
10	42.67	-4.06	50.44	-0.28	Failure

7.2.3. Prevención de colisiones con smart objects

Para esta situación, el escenario de prueba utilizado es el mismo que el diseñado en el primer caso. Hay dos carretillas elevadoras que se mueven a través de dos pasillos de la fábrica en la que existe un área de colisión.

Cada WSN tendrá su propio objeto inteligente que le permite gestionar y procesar toda la información. Por lo tanto, la WSN tiene dos interfaces: una interfaz real al SOS para enviar medidas, y una interfaz virtual a una unidad de proceso virtual interno modelado por un SO, para ampliar la capacidad de procesamiento interno (ver Figura 90). En este

caso, cada una de las carretillas está representada por una WSN que envía su posición y velocidad.

Hay varias maneras de calcular o estimar el riesgo potencial para un SO. En primer lugar, el SO debe conocer la ubicación de todos los posibles cruces que entrañan algún riesgo. Para ello, el SO tiene la capacidad de consultar un Repositorio de Recursos Común (CRR, por sus siglas en inglés) para obtener el mapa de la fábrica incluyendo todas las intersecciones. A continuación, el SO obtiene la posición y la velocidad de las carretillas elevadoras accediendo al SOS. Hay que tener en cuenta que esta información también puede obtenerse directamente de la WSN (de hecho sería más eficiente), pero se ha desarrollado de esta forma para poder obtener datos (posición y velocidad) del SOS de cualquier carretilla en caso de ser necesario.

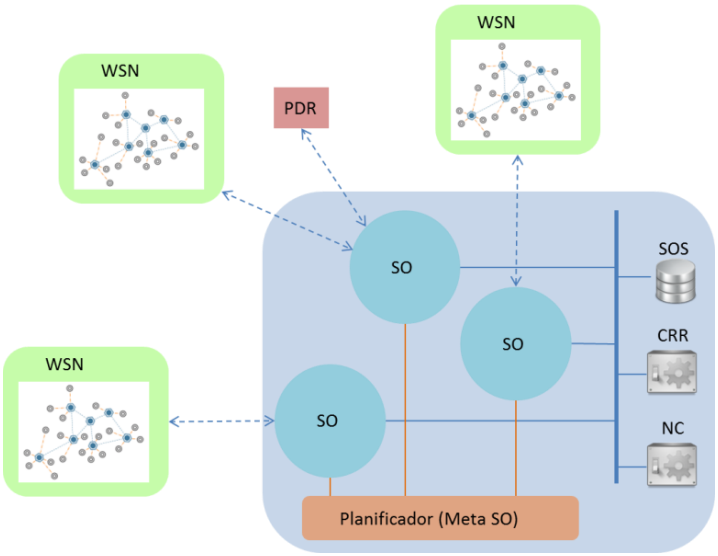

Figura 90. Arquitectura de alto nivel del sistema con smart objects

A partir de dicha información (posición, velocidad y mapa) el SO puede estimar en tiempo real, si se está entrando en una zona de riesgo, en este caso la intersección. En caso de riesgo de colisión, el SO notifica el evento al centro de notificaciones (NC). Si otra carretilla elevadora entra en la zona de riesgo de la misma intersección, su SO correspondiente recibe la notificación a través de la NC, que sirve como canal de comunicación entre los SOs. Las acciones a tomar para evitar el riesgo pueden variar en función de la situación, por ejemplo, reducir la velocidad o parar completamente.

Además del sistema de notificación de eventos también existe una interacción cooperativa entre SOs. Con el fin de evitar colisiones antes de que sucedan, los SOs pueden cooperar formando un metaobjeto llamado planificador. El planificador permite obtener la ruta inicial óptima para cada SO antes de iniciar la conducción. De esta manera, se puede evitar colisiones antes de que ocurran.

Otra característica relevante del SO, consiste en la encapsulación de los datos personales y privados (por ejemplo, datos médicos). El SO es capaz de cotejar los datos personales con datos ambientales y extraer conclusiones (por ejemplo, un trabajador asociado a una WSN no debería estar expuesto a aminas más de una cierta cantidad de

tiempo) sin revelar información sensible. El SO es la única entidad del sistema que tiene acceso a los datos personales (PDR, Personal Data Records) o registros médicos, y por lo tanto, conoce los riesgos de un trabajador específico. Es totalmente privado y confidencial, porque el único que lee la información es el SO y luego obtiene la información necesaria desde el SOS o CRR para realizar algún proceso de razonamiento.

Inicialización

Inicialmente todos los relojes de los distintos SO se sincronizan con un servidor de tiempo (a través de NTP, Network Time Protocol) para permitir un cálculo preciso de las colisiones y establecer rutas. Cada SO sabe de ante mano cual será la próxima ruta que su vehículo correspondiente. Esto permite detectar con antelación los cruces donde existe alguna posibilidad de riesgo, y suscribirse en el NC a aquellos eventos (cruces correspondientes) que interesan a cada vehículo. Por su parte, cada vehículo inserta su posición en el SOS periódicamente, que en el caso de los vehículos a y b emplean un tiempo $T_{InsertData}$ (ver Figura 92).

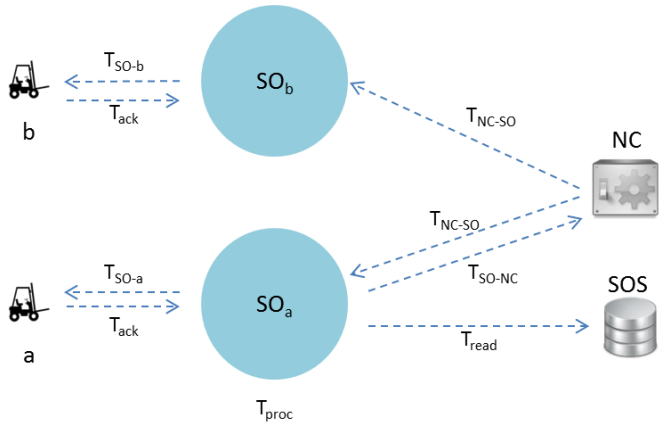

Figura 91. Esquema de los eventos

Eventos

El primer vehículo (en este caso el vehículo b) entra en la zona de riesgo de un cruce, lo que genera que su SO asociado envíe una alerta al centro de notificaciones. Esta acción no se representa explícitamente en la Figura 92, ya que incluir todas las acciones puede dificultar la comprensión. El SO de la segunda carretilla (vehículo a) monitoriza en tiempo real los movimientos del vehículo, mediante solicitudes al SOS (T_{read}) y el procesado de dicha información (T_{proc}). Cuando detecta que ha entrado en la misma zona de riesgo, envía una alerta al NC ($T_{SO \rightarrow NC}$). Inmediatamente el NC se comunica con todos los SOs suscritos al evento (en el mismo cruce) para evitar una colisión ($T_{NC \rightarrow SO}$). Por último, cada SO notifica a su vehículo correspondiente la orden para detenerse o reducir la velocidad ($T_{SO\text{-}a}$, $T_{SO\text{-}b}$) y espera una respuesta (T_{ack}). Por tanto, el tiempo total para el vehículo a, puede estimarse de la siguiente manera (ver Figura 92):

$$T = T_{read} + T_{proc} + T_{SO \rightarrow NC} + T_{NC \rightarrow SO} + T_{SO\text{-}a} + T_{ack} \quad (1)$$

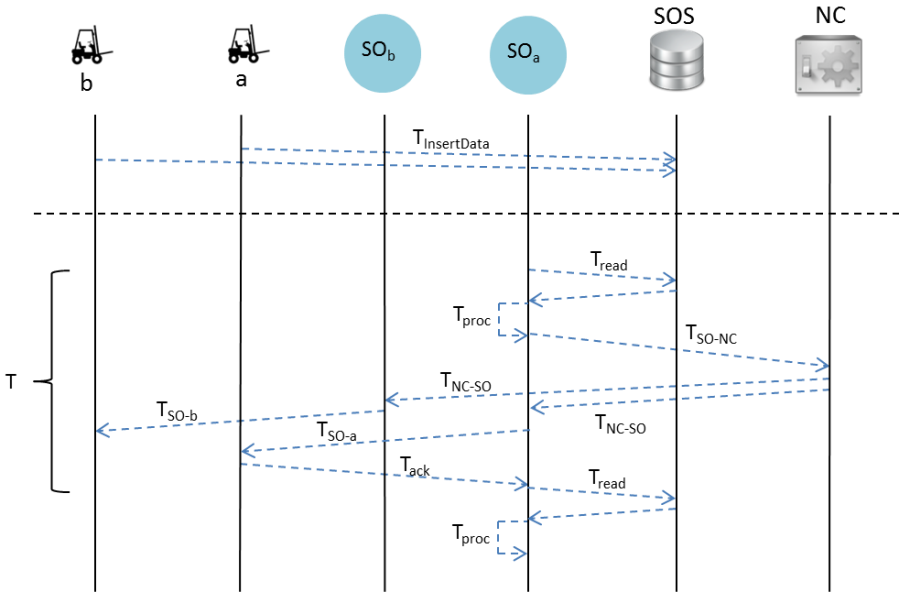

Figura 92. Diagrama de secuencia del escenario

Tras recibir la respuesta del vehículo, se realiza una nueva solicitud de la posición final del vehículo al SOS para evaluar el resultado y conocer si se ha detenido a tiempo de evitar la colisión.

Resultados

Para obtener estos resultados se ha simulado una fábrica con 25 vehículos y una superficie de 2.500 m^2, y se han establecido rutas aleatorias para los vehículos a través de los pasillos de la fábrica. Se han establecido tres valores fijos de RC (riesgo de colisión) por hora: 5, 10 y 20 durante todo un día (24 horas). El número de vehículos (25) y la variabilidad de RC (entre 5 y 20 por hora) parecen realistas para la fábrica en cuestión.

Tabla 5. Resultados de la simulación en el escenario SO

RC (ph)	Maximum speed (km/h)
5	44
10	35
20	27

Como se puede ver en la Tabla 5, cuando el número de RC aumenta, la velocidad máxima a la que pueden circular las carretillas elevadoras para detectar de forma segura la colisión, disminuye. Esto se produce principalmente por el aumento en el número de mensajes intercambiados (a/desde el SOS y a/desde el NC), y por tanto, aumenta el tiempo de detección resultante. Para pequeños valores de RC, los vehículos pueden ir a una velocidad más alta.

Aunque es difícil comparar ambos escenarios, ya que en el primero el CEP está físicamente en un solo equipo y en el segundo los smart objects están distribuidos, se

puede estimar cualitativamente que el tiempo final es ligeramente superior en el primer caso. El tiempo de procesamiento en el SO es significativamente más bajo en comparación con un CEP, ya que el SO sólo se preocupa de un solo vehículo, mientras que el CEP evalúa toda la fábrica.

Sin embargo, el CEP no requiere un NC, ya que interactúa directamente con los WSNs. Los SO, por el contrario, requiere el NC para intercambiar notificaciones. Por otra parte, el CEP puede consultar al SOS múltiples vehículos o sensores en un solo mensaje, mientras que cada SO requiere mensajes individuales (aunque más simples). Esto aumenta la cantidad total de mensajes intercambiados, y por lo tanto, el tiempo resultante.

Como los SOs son objetos independientes, el sistema es descentralizado, por lo que si uno de ellos se cae, no implica el caída de todo el sistema. El uso de mecanismos de computación en la nube también ayuda en la detección de fallos y recuperación inmediata. Sin embargo, el uso de varios objetos virtuales implica la necesidad de ordenadores más potentes en la fábrica.

7.3. UniverSEC

Se ha llevado a cabo el desarrollo de un demostrador de escenario para la validación de las herramientas, métodos, arquitectura y modelos técnicos que se han diseñado en UniverSEC. El escenario integra las diferentes tecnologías, enfoques y algunos de los dispositivos reales que forman el smart grid. A partir de la monitorización continua de sus elementos se puede evaluar el valor de SA en tiempo real.

Con este prototipo, se quiere demostrar que el sistema es capaz de mantener en todo momento todos los elementos que componen el smart grid asegurados. En el momento que se detecta alguna vulnerabilidad es capaz de detectarlo y actuar en consecuencia, ya sea resolviéndolo de forma automática o avisando a quien corresponda.

7.3.1. Escenario de la prueba

La versión reducida del smart grid, la cual disponemos como escenario de prueba, está compuesta por algunos de los componentes reales que utilizan los operadores para la gestión de la energía, como se puede ver en la Figura 93.

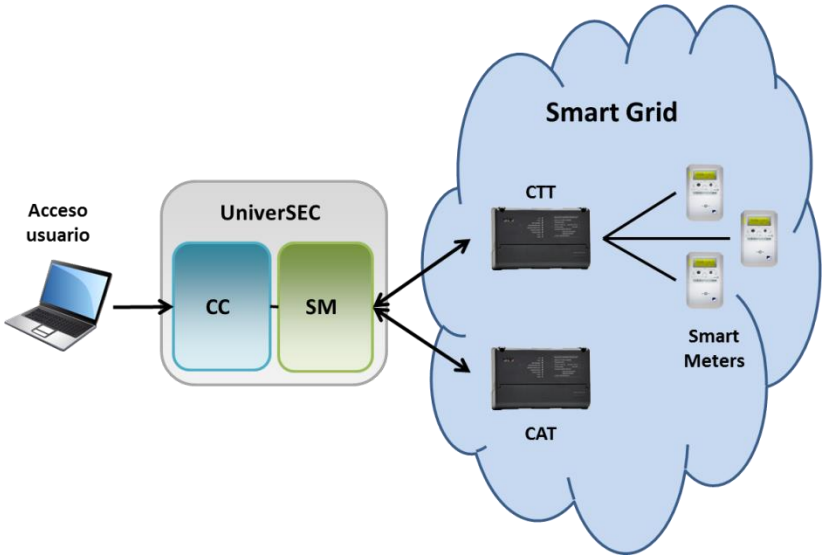

Figura 93. Arquitectura de la prueba

El más conocido de ellos es el smart meter (contador inteligente), el cual se está empezando a implantar en España, para medir el consumo de energía en tiempo real. Los datos que provienen de varios smart meter se concentran mediante un CTT, de forma que se optimizan los mensajes de datos enviados. El CAT se utiliza para gestionar y configurar de forma remota todos los smart meters que dependen de un CTT. Además, a la hora de enviar los datos se utiliza un router específico llamado DRA que realiza un túnel IPSEC. Todos estos dispositivos han sido proporcionados por ZIV, miembro del consorcio UniverSEC (ver Figura 94).

Figura 94. Smart meter, CTT y CAT

Una vez conectados todos los dispositivos y montado el escenario, el resultado es el de la Figura 95, donde además se ha añadido una fuente de alimentación para alimentar todos los dispositivos y un servidor en que está instalado el sistema UniverSEC.

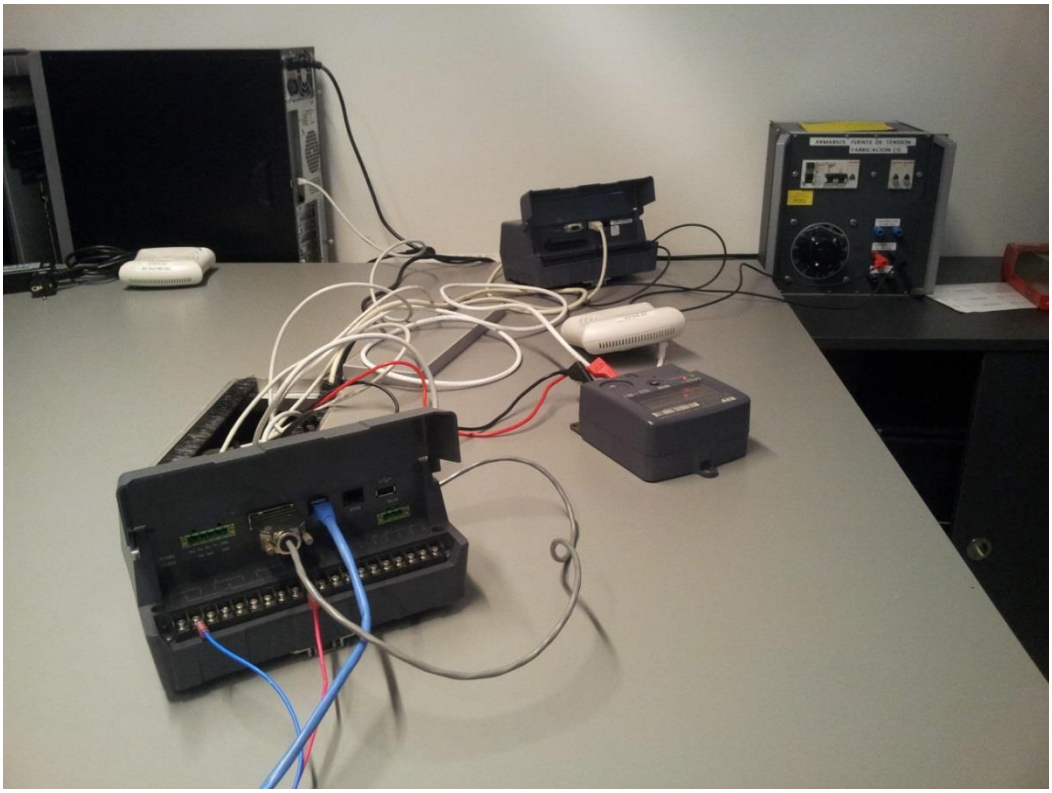

Figura 95. Escenario de prueba

El siguiente paso, previo a la puesta en marcha de la prueba, es registrar en la base de datos todos los dispositivos que van a ser monitorizados, insertar todas las medidas base que van a ser evaluadas, así como todos los elementos que componen el SA. En la Figura 96, se puede ver el resultado después de registrar los cuatro dispositivos.

Figura 96. Menú de dispositivos

Para una visualización y comprensión más sencilla, se ha planteado evaluar la garantía de seguridad de un único servicio, el acceso remoto a los cuatro dispositivos, en particular sobre SSH y Telnet. En cualquier caso, esto se podría extender a todos los servicios que tienen estos aparatos, como podría ser el envío periódico de los datos medidos por el contador.

7.3.2. Ejecución de la prueba

El primer paso a realizar, es la activación de los tres servicios que lleva a cabo el sistema (evaluación remota, cálculo de DMs y CEP) por parte del administrador del smart grid, como se ha visto en la sección 5.5.4.

Tras unos segundos de espera, en el menú de BMs las medidas base pasan de estar en color gris (sin datos), a verde o rojo en función de su vulnerabilidad. Como se puede ver en la Figura 97, se están monitorizando 7 medidas base, dos por cada dispositivo, salvo el smart meter que solo dispone de acceso a través de Telnet. En un principio todas ellas estaban aseguradas (verde), pero se forzado una de ellas a vulnerable (rojo), para percibir mejor el funcionamiento.

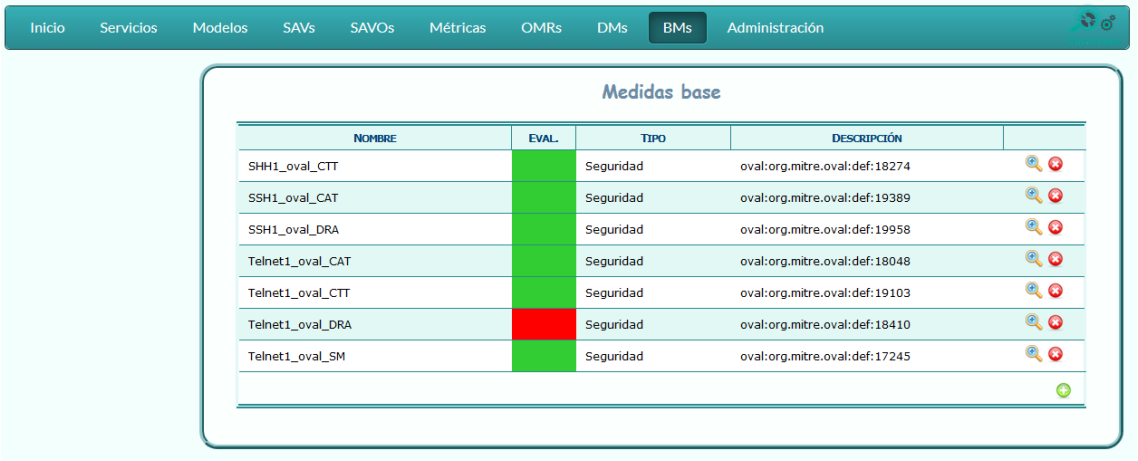

Figura 97. Menú de BMs

A partir de las medidas base se calculan las medidas derivadas. En este caso la relación entre ambas es uno a uno, ya que por cada uno de los protocolos (SSH y Telnet) solo se evalúa una vulnerabilidad. Por tanto, la Figura 98, es muy similar a la anterior.

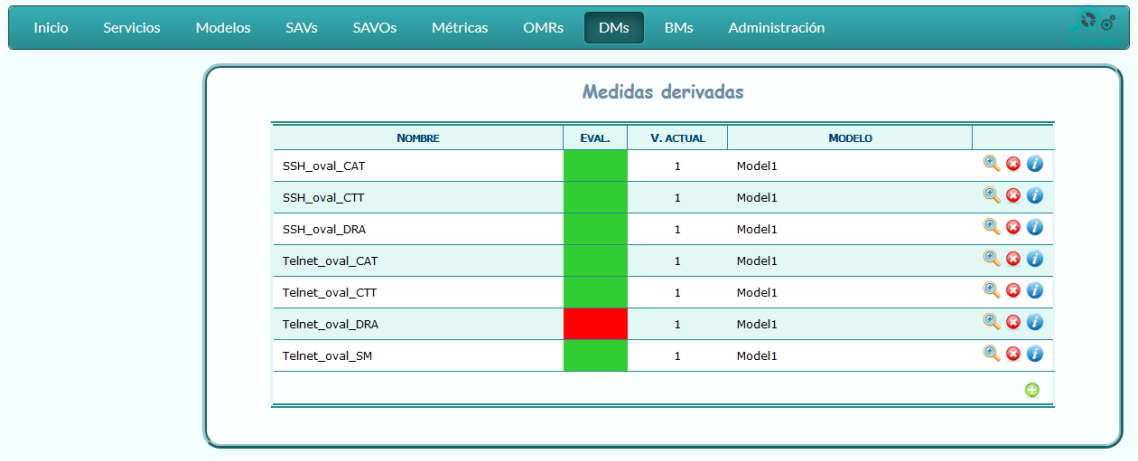

Figura 98. Menú de DMs

A continuación, con las medidas derivadas se calculan los requisitos de medición de objetos. En este caso se agrega para cada OMR el servicio de acceso remoto de cada dispositivo (SSH y Telnet). Por tanto hay cuatro OMRs con dos DMs cada uno, salvo en el caso del smart meter que solo tenía Telnet (ver Figura 99).

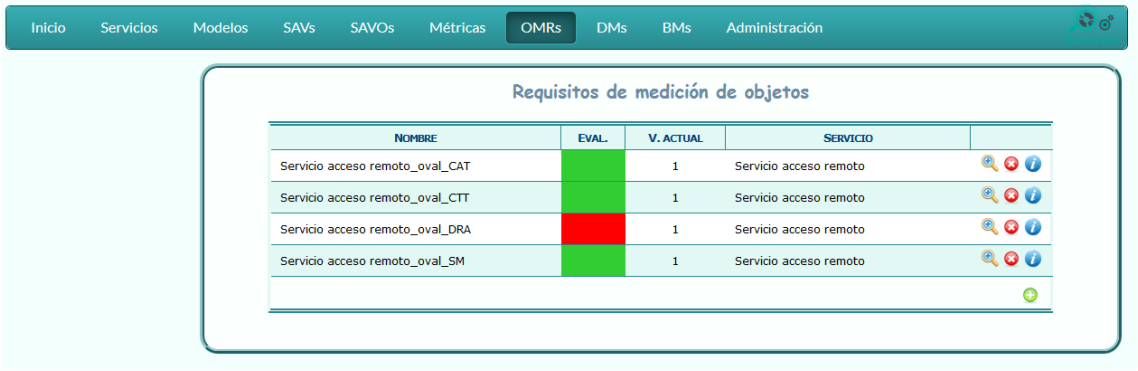

Figura 99. Menú de OMRs

Para conocer en detalle por qué el servicio de acceso remoto del DRA evaluado a través de oval es vulnerable, se puede hacer clic en el icono de información, y ver con exactitud cuál es su estado.

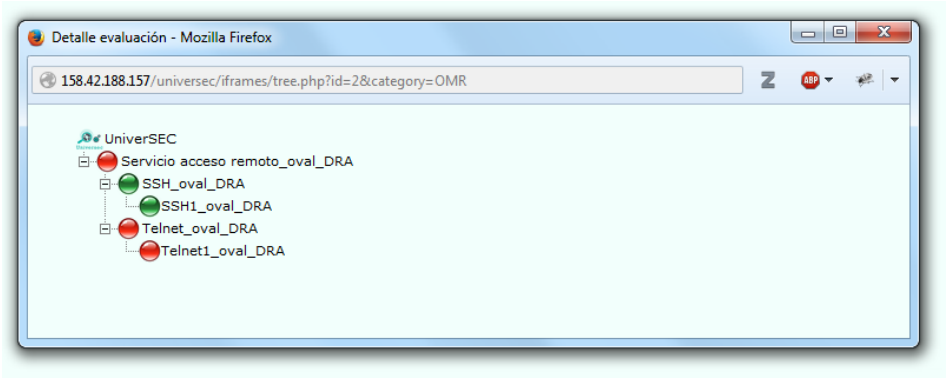

Figura 100. Detalle de OMR

El cálculo de las métricas se realiza agregando los OMR de todos los dispositivos para cada uno de los servicios. Es este caso solo se está evaluando el servicio de acceso remoto, de modo que se tiene una única métrica. Debido a que uno de los OMR que lo compone es vulnerable, la evaluación de la métrica resulta ser también vulnerable.

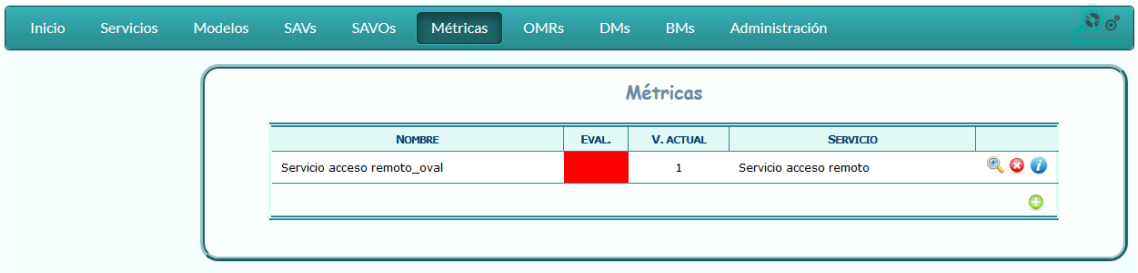

Figura 101. Menú de métricas

Por último, el cálculo de los servicios se lleva a cabo agregando aquellas métricas que pertenecen a un mismo servicio medido a través de diferentes estándares. De momento, solo se están evaluando las vulnerabilidades a través de OVAL, y por tanto, solo se dispone de una métrica para el servicio de acceso remoto (ver Figura 102).

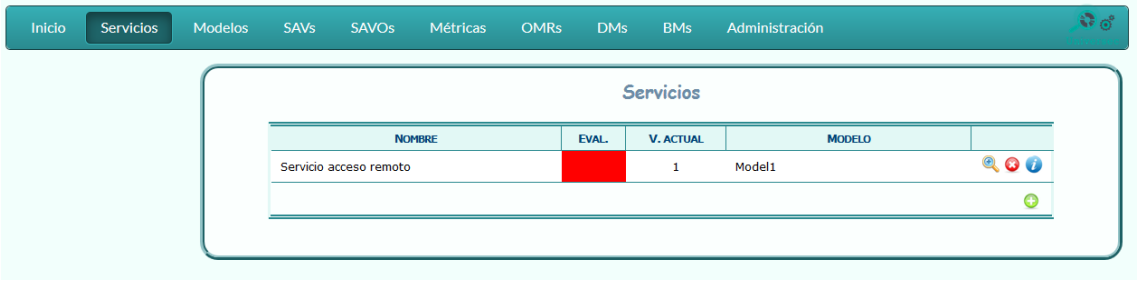

Figura 102. Menú de servicios

Igual que en todos los menús anteriores, se puede visualizar por qué un servicio es vulnerable, con el fin de poder subsanar el problema. En la Figura 103, se puede ver fácilmente todo el proceso que se acaba de seguir y determinar de forma inmediata cual es el problema.

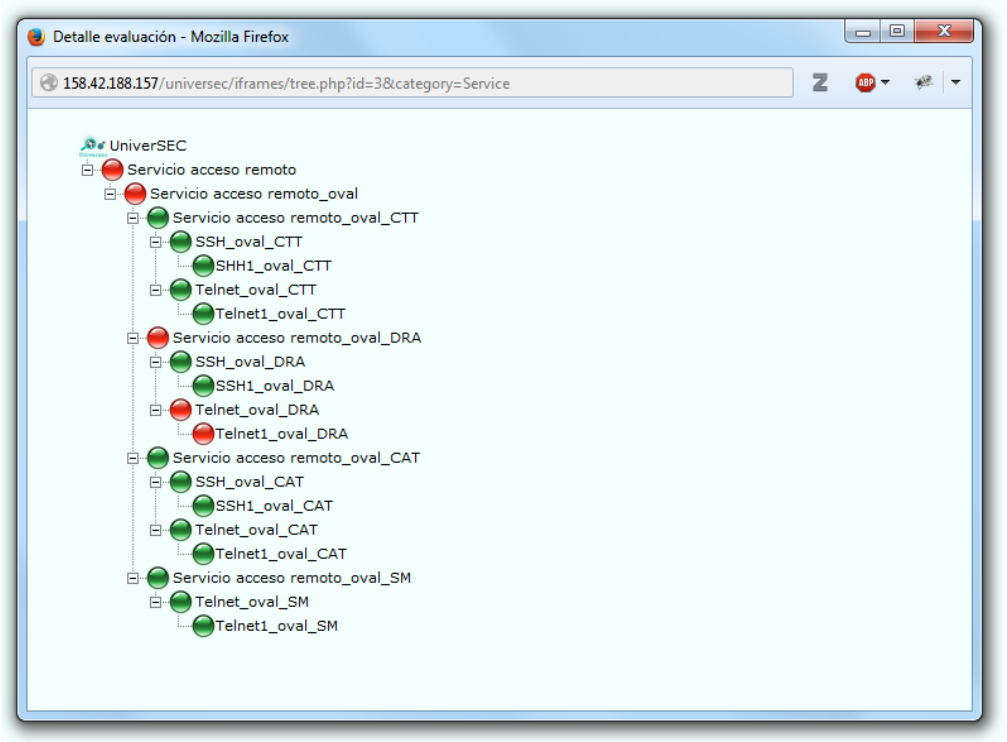

Figura 103. Estado del servicio

Desde el menú principal, también se puede ver el estado general de todos los dispositivos desplegados en el smart grid de forma inmediata. En la Figura 104, se pueden ver los cuatro dispositivos georeferenciados, en este caso en las oficinas de Nextel. Además, el color del icono de cada dispositivo varía en función del resultado de la evaluación de todos sus OMRs. Para conocer con detalle el porqué de su estado, se puede hacer clic sobre el icono y se despliega una tabla con un listado de sus OMRs y su evaluación, como en la Figura 105.

En las gráficas del lateral se puede ver que el 100% de los servicios son vulnerables, ya que solo hay registrado un servicio y en todo momento su estado ha sido vulnerable.

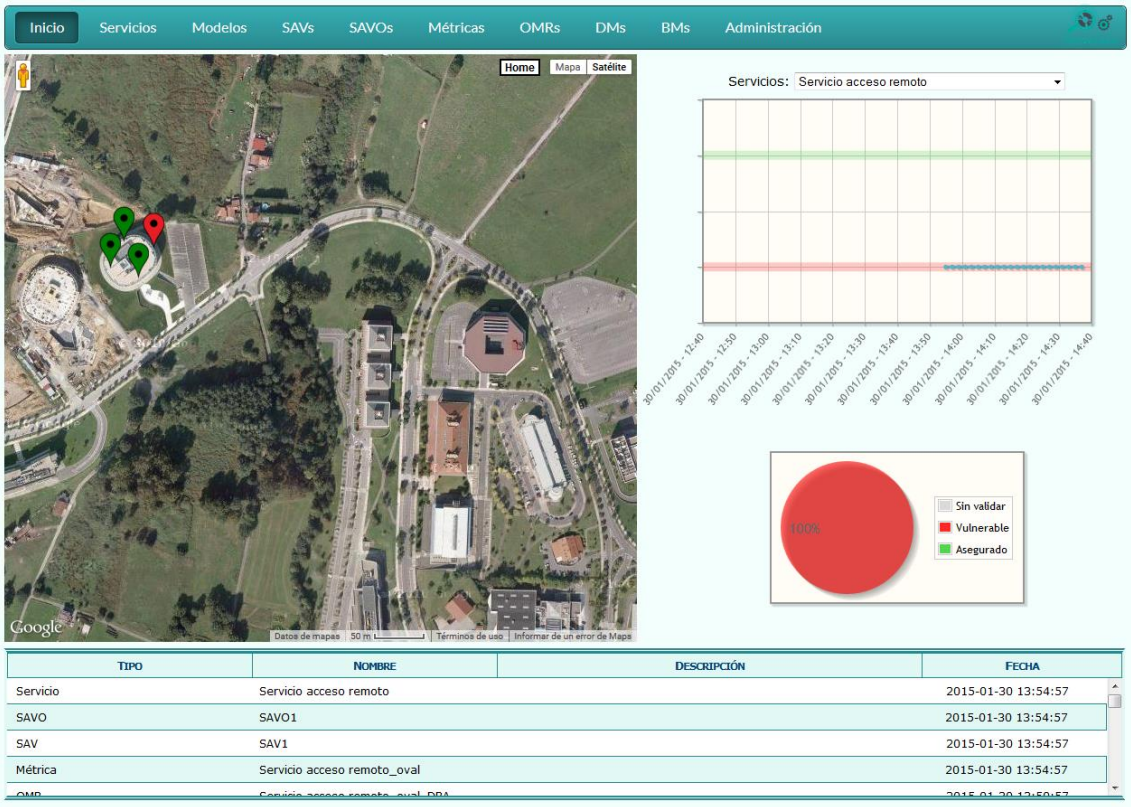

Figura 104. Pantalla principal

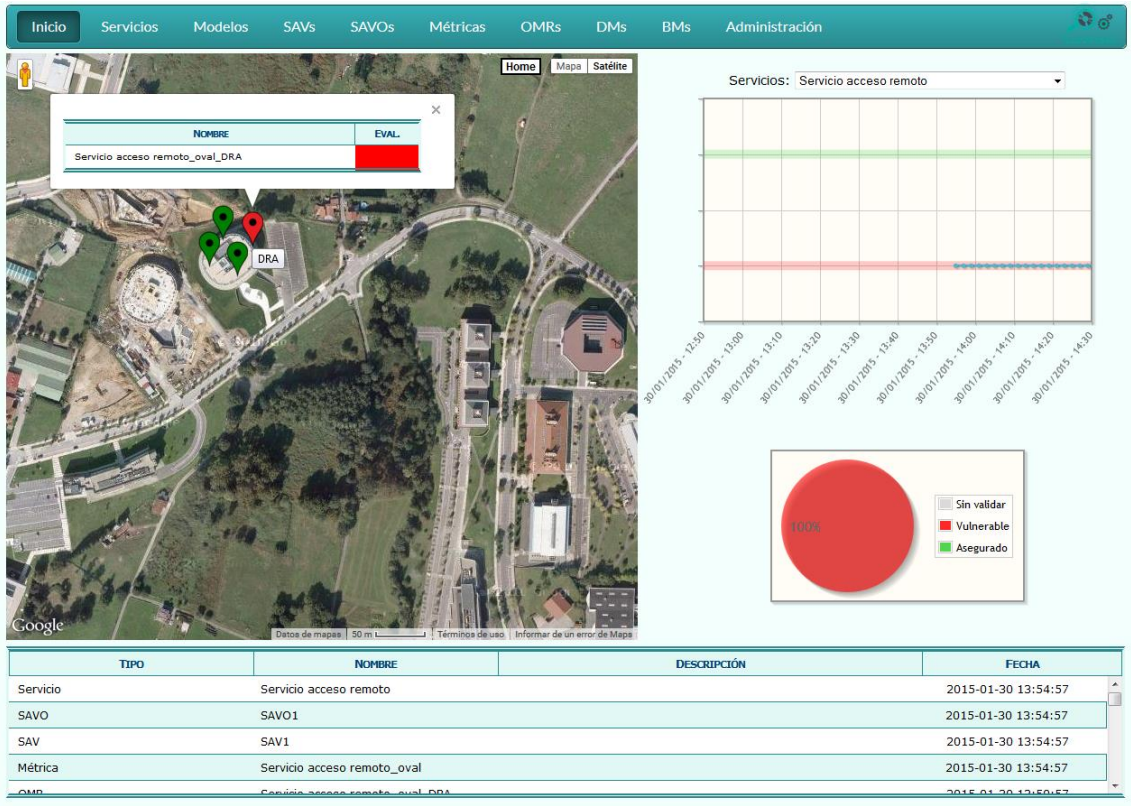

Figura 105. Pantalla principal con información de dispositivo

7.4. STIMULO

Para realizar la evaluación del sistema STIMULO, se ha planificado una prueba, en la que un vehículo real lleva a cabo una Orden de Transporte del puerto de Valencia. Esta tarea engloba el desplazamiento hasta el puerto para la recogida del contenedor, y el transporte hasta el destino designado para la descarga.

7.4.1. Escenario de la prueba

La ruta inicialmente planteada para la prueba (aunque puede variar en función de las decisiones del sistema), es la que va desde el puerto de Valencia hasta el depósito de la empresa de transporte. Al tratarse de camiones, normalmente circularán por las vías principales y prácticamente nunca entrarán en la ciudad. Por tanto, el camión sale del depositó y va hasta el puerto en primer lugar. Y tras realizar la carga del contenedor regresa al depósito.

La mayoría de cámaras utilizadas para el cálculo del IMT se muestran en la Figura 106, donde la V-30 es la vía principalmente afectada (en blanco), y luego tenemos cámaras para otras vías que conectan con la V-30 (en gris).

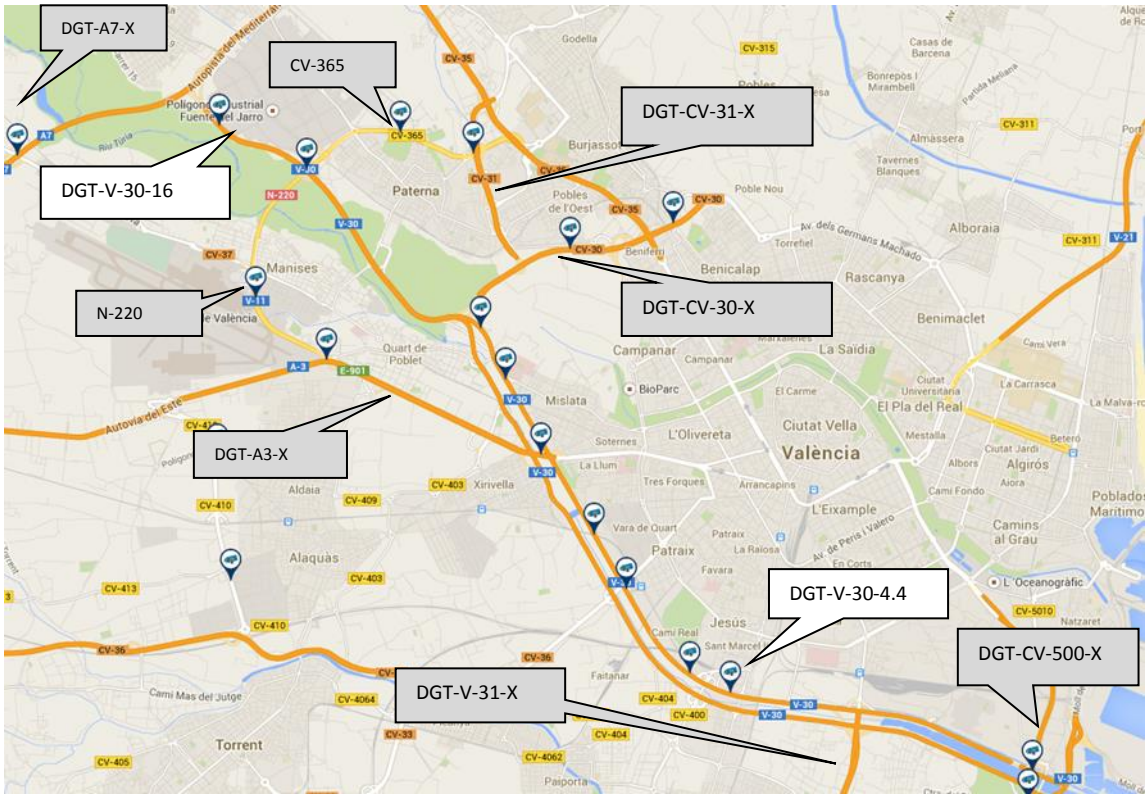

Figura 106. Cámaras en la zona de prueba [235]

7.4.2. Ejecución de la prueba

Obtención del IMT

En primer lugar, el sistema calcula la intensidad de tráfico a partir de las fuentes de datos disponibles. Para el trayecto desde el puerto al depósito, se va a circular por la V-30 en dirección oeste, por lo que se obtienen todas las imágenes de dicha carretera y las posibles alternativas, para evaluar el estado del tráfico.

En la Figura 107, se pueden ver las imágenes de tráfico de tres de las cámaras registradas (DGT-V-30-4.4, DGT-V-30-6.8, DGT-V-30-10.2), en dos instantes de tiempo distintos. Estas imágenes obtenidas se envían al módulo de Visión Artificial para que, a partir de ellas, calcule el valor de IMT.

Figura 107. Imágenes obtenidas de las cámaras de la V-30 [236]

El módulo de Visión Artificial evalúa todas las imágenes (por cada cámara se evalúan todas las imágenes disponibles) y determina el valor de IMT. Para las tres cámaras mencionadas, el valor de IMT es 396, 423 y 502, respectivamente. Estos valores son introducidos en el SOS para su posterior acceso.

Inteligencia colectiva

El módulo de Inteligencia Colectiva obtiene todos los datos del SOS y de la orden de transporte correspondiente, y realiza 3 simulaciones en SUMO, hasta establecer que la ruta óptima es la mostrada en la Figura 108.

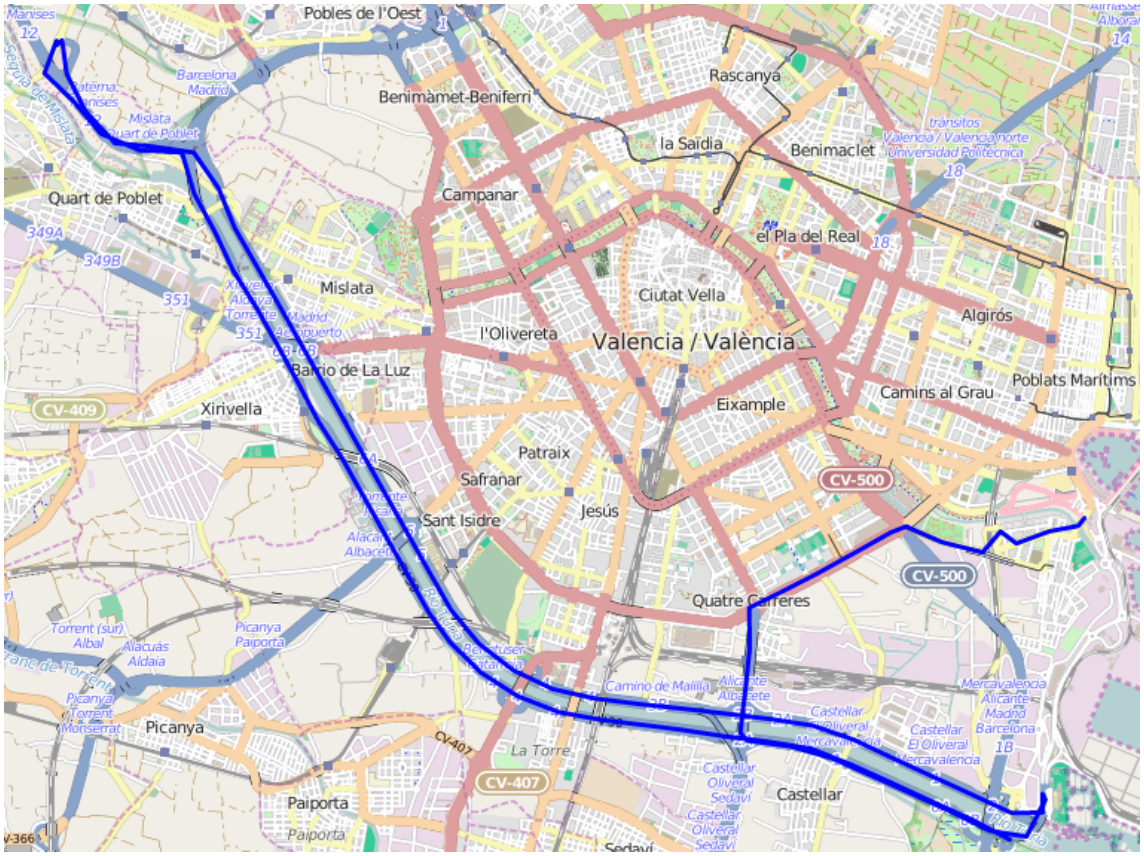

Figura 108. Ruta designada por la IC

Aplicación móvil

El conductor del camión está informado en todo momento de cuál es la ruta que debe tomar a través de la aplicación móvil. Además, si hubiera alguna incidencia alertaría al conductor y cambiaría la ruta en caso de ser necesario. Como se trata de un trayecto corto no se ha planificado ninguna parada para que descanse el conductor.

Después de introducir la matrícula y la orden del transporte, el conductor accede a la pantalla principal de la aplicación (ver Figura 109), desde la cual puede acceder a las distintas opciones. Tras establecerse la comunicación entre el móvil y el sistema STIMULO, se enviará, las incidencias, las alarmas, los eventos y la ruta a seguir, que se dibuja automáticamente en el mapa.

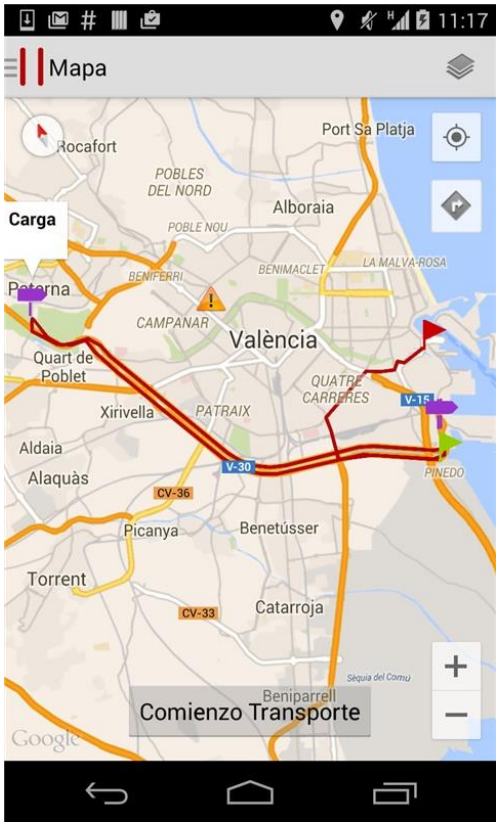

Figura 109. Ruta en la aplicación móvil

Desde el menú general (Figura 110), el conductor puede acceder a toda la información adicional, como el estado de la orden de transporte. En ella, se informa la fecha y hora prevista para la recogida del contenedor, la carga y la entrega. Al llegar a cada uno de estos destinos, el conductor debe presionar un botón para indicar que se ha realizado la tarea. También puede acceder al listado de incidencias y alarmas, o introducir una nueva incidencia.

Figura 110. Menú general

8. Conclusiones y líneas de trabajo futuras

8.1. Conclusiones finales

En esta tesis se ha presentado, estudiado y evaluado el estándar abierto para mejorar la interoperabilidad SWE. Para ello, se ha diseñado e implementado una arquitectura que se integra con dicho estándar, y se ha puesto a prueba en distintos casos de uso. Las conclusiones que se pueden extraer son las siguientes.

8.1.1. Conclusiones generales

Estado del arte

- La evolución de los sensores a *sensor web,* supuso un gran avance en los sistemas de monitorización ambientales, de forma que se pueden agrupar varios sensores en un solo nodo y acceder a ellos como una única entidad de forma asíncrona. Incluso el nodo, puede ser capaz de realizar un pre procesado o fusión de datos. Además, todos los nodos son iguales entre ellos, así que cualquiera de ellos puede actuar como pasarela o como reloj.
- En la actualidad, el término *sensor web* se utiliza principalmente cuando se habla de sensores conectados a Internet y con capacidad de integración en entornos WWW. El principal uso hoy por hoy, es en la integración de datos de sensores en aplicaciones web.
- Entre los estándares de interoperabilidad entre sensores, los más utilizados son UPnP y DLNA, para implementar una arquitectura de red distribuida de dispositivos, de forma que sea automático entrar o dejar la red. También podemos encontrar DPWS, aunque en este caso, está más relacionado con servicios web. Otra alternativa para dispositivos electrónicos pequeños como los sensores, es CoAP, el cual permite controlarlos a través de Internet.
- SWE se creó con el fin de desarrollar estándares que permitan acceder y controlar sensores a través de Internet. Está compuesto de varias especificaciones, entre ellas SensorML y O&M, que permiten descubrir sensores, acceder a sus propiedades y capacidades, configurar un sensor, acceder en tiempo real a sus medidas, etc. El servicio más importante que dispone es el SOS, para proporcionar almacenamiento y acceso a las medidas de los sensores.
- Debido al auge de las redes de sensores, en los últimos años, se han desarrollado múltiples aplicaciones que utilizan alguna implementación de SWE. Existen aplicaciones para evaluar la relación entre el cambio climático y el impacto en la salud humana (EO2HEAVEN), para monitorizar la calidad del agua en ríos y lagos (GENESIS), para datos oceanográficos, para calcular el efecto de la conducción en el consumo de combustible (enviroCAR), etc.
- Se ha mejorado *sensor web* mediante la incorporación de tecnologías semánticas y la incorporación de metadatos semánticos. De este modo se incrementan la interoperabilidad entre sistemas y facilita las tareas de razonamiento y

clasificación. Entre los lenguajes más usados para hacer más explícito el significado de los datos y crear ontologías están RDF y OWL.

- Para la detección de vulnerabilidades en un sistema de monitorización y control es posible utilizar diversos sistemas, como firewalls de nueva generación, IDP o IPS. Por otra parte, es necesario evitar que los nodos de la red de sensores sean comprometidos, para lo cual, es necesario utilizar técnicas como INSENS o SPINS, que realizan autenticación con claves compartidas o la prohibición de usar broadcast.
- Entre los principales estándares en seguridad industrial, se encuentran: NISTIR 7628, que proporciona un marco para desarrollar estrategias de seguridad cibernética en el smart grid; ISO 27000, para la gestión de la seguridad informática en un SGSI; el Common Criteria, un marco para especificar requisitos de seguridad en sistemas informáticos y que por tanto garantiza la seguridad del producto; y el SA, que es un proceso que permite mantener la integridad y la disponibilidad de la información en sistemas TIC.
- Los ITS son sistemas que utilizan las TIC e IoT para mejorar la seguridad y la gestión del transporte terrestre. Consigue reducir la congestión, mejorar la seguridad y aumentar la productividad. Utiliza técnicas de monitorización del estado del tráfico mediante visión por computador, detección de vehículos y su clase, inteligencia artificial para la gestión del tráfico, etc.
- El concepto de IoT hace referencia a la interconexión digital de objetos a Internet, para poder interactuar y obtener información. A partir de la multitud de datos obtenidos, se pueden crear aplicaciones para cuatro dominios de aplicación: personal y del hogar, empresa, servicios públicos, y móvil.

Especificación de la arquitectura

- La aportación más importante de esta tesis ha sido la arquitectura I3WSN propuesta, integrada con el estándar SWE, de modo que garantice la interoperabilidad entre sensores y sistemas.
- La arquitectura es suficientemente genérica como para aplicarse en distintos entornos, adaptándose a las necesidades de los sistemas IoT.
- La arquitectura es escalable, ya que su organización jerárquica permite una fácil expansión. Sus dos bloques principales son independientes entre sí, lo que permite ser flexibles a los diferentes sistemas e infraestructuras.
- Sus dos componentes principales son: el bloque de obtención de datos, para la recogida continua y almacenamiento de los datos; y el centro de control, que ofrece al usuario final una visión global del sistema y le permite configurar y supervisar todos los parámetros.

- La comunicación entre el bloque de obtención de datos y el centro de control permite el intercambio de datos y ordenes en el sistema. Además de los datos de los sensores, también permite obtener los sensores disponibles, configurar los sensores, etc.
- Todos los elementos situados dentro del área de supervisión son tratados como sensores, ya sean trabajadores, equipo informático, sensores, vehículos, cámaras, etc. Cada uno de ellos envía sus datos al SOS de forma automática. En este caso, se ha seleccionado la implementación del SOS del 52north.
- Se pueden utilizar distintas topologías a la hora de diseñar el sistema, con el fin de adaptarse a la distribución de la infraestructura. Se puede optar por una arquitectura centralizada, con un centro de control de alto nivel que concentra la información; una arquitectura distribuida, donde varios centros de control colaboran a la hora de tomar decisiones; o una arquitectura híbrida.

8.1.2. FASyS

- El objetivo final en las fábricas del futuro, no es una fábrica sin riesgo, sino una fábrica que dispone de los recursos técnicos, humanos y de organización para identificar, detectar, monitorizar y gestionar de forma continua los riesgos relativos a la salud y la seguridad de los trabajadores, en todo el ciclo de vida de la fábrica.
- Es preciso fortalecer las plataformas de comunicación y aplicaciones en red para mejorar el rendimiento y la competitividad. El sistema FASyS trata de mitigar los riesgos laborales potenciales, mediante la detección precoz de los factores ambientales que pueden llevar a tales riesgos o accidentes. Todos estos factores son monitorizados a través de redes inalámbricas de sensores, que se despliegan a lo largo de la fábrica y pueden comunicarse con un centro de control remoto, incluso en condiciones adversas, gracias al despliegue de una red troncal inalámbrica heterogénea.
- Se ha presentado un nuevo enfoque para el uso de tecnologías Sensor Web Enablement en entornos industriales, con el fin de monitorizar el comportamiento de los trabajadores y asegurar tanto su seguridad como su salud, de acuerdo con el paradigma FoF. A fin de lograr este objetivo, se han desplegado diversos sensores inalámbricos heterogéneos dentro de la fábrica, incluso sensores llevados por los trabajadores en forma de una red de área personal (PAN). La información detectada se envía a un servidor SOS, donde se almacena y está disponible para que cualquier aplicación o usuario que la necesite, acceda a ella de forma estándar. Este es un aspecto fundamental para el éxito del sistema, ya que normalmente las WSNs tienen su propia interfaz de comunicación y rara vez interoperar con otras redes, lo que representa un serio inconveniente para un despliegue escalable y modular de los sistemas de sensores en una fábrica.

- La red de comunicaciones heterogénea abarca diferentes tecnologías inalámbricas. En particular, se utiliza IEEE 802.15.4 (ZigBee) para comunicaciones de corto alcance y baja potencia. Para las comunicaciones de alcance medio, se utiliza IEEE 802.11 (Wi-Fi) para proporcionar conectividad a los coordinadores WSN y sensores de alta capacidad (por ejemplo, cámaras de vídeo). Para las comunicaciones de largo alcance con el Centro de Control, se ha utilizado IEEE 802.16 (WiMAX) debido a su ancho de banda disponible.
- Para la implementación de la arquitectura se ha utilizado la arquitectura I3WSN, ya que está totalmente integrada con el estándar SWE y al ser modular y escalable se puede adaptar al tamaño y forma de la fábrica. Cada sección en la que hay una o varias WSNs forman un área, y a su vez varias áreas junto con su correspondiente SOS y Centro de Control Local, forman una zona. Las zonas disponen de una conexión con el Centro de Control Global donde está situado el CEP, el HMI.
- El sistema FASyS, es una herramienta que permite evaluar todo tipo de escenarios de seguridad para los trabajadores y máquinas en entornos industriales. Se ha demostrado con un escenario de colisión entre carretillas elevadoras, pero es fácilmente extensible a otros entornos y escenarios. Para lograr este objetivo se han utilizado varios componentes: (i) WSNs para detectar las condiciones ambientales (ii) un SOS para permitir la interoperabilidad entre los datos de WSN, (iii) un simulador de sensores para replicar comportamientos específicos de diferentes sensores, (iv) un entorno de computación en la nube, virtualizar para smart objets y proporcionar capacidad de procesamiento e inteligencia a las WSN, (vi) un CEP para centralizar algunos procesos y comparar con smart objets y (vii) un HMI para proporcionar una plataforma gráfica de monitorización.
- Los smart objets proporcionan una plataforma de gestión distribuida, en comparación con un CEP centralizado (proporciona más potencia de procesamiento para los WSNs), y se pueden encapsular mejor algunos problemas de seguridad (por ejemplo, datos personales). Sin embargo, las infraestructuras de computación en la nube dentro de una fábrica, requieren una importante inversión económica inicial que tiene que ser considerada. Los SO pueden calcular en tiempo real cuando una carretilla elevadora incurre en un riesgo de tener un accidente (colisión) y alertar automáticamente.
- Se ha desarrollado un interfaz gráfico de usuario con el fin de controlar fácilmente todas las acciones que ocurren dentro de la fábrica, ubicado en el centro de control. Permite visualizar y controlar los sensores de la fábrica georeferenciados, además de ver representadas en tiempo real todas las alarmas asociadas a un sensor. El HMI está desarrollado como una aplicación web, lo que facilita la visualización en cualquier dispositivo de usuario (ordenadores, tabletas y móviles), y mejora la interacción y la comunicación con el trabajador a través de su teléfono móvil.
- El simulador implementado, es una herramienta útil para facilitar la planificación y evaluación de escenarios de seguridad para los trabajadores en entornos industriales, ya que evita el despliegue de numerosos sensores reales dentro de una

fábrica para identificar situaciones de riesgo. El simulador, es capaz de generar datos en tiempo real de sensores móviles y fijos, y enviar todas las mediciones simuladas al SOS, que actúa como repositorio común. Mediante el interfaz de SOS se actualiza, no sólo las mediciones, sino también la ubicación del sensor en el caso de sensores móviles. Ya que el SOS presenta una interfaz web con los sensores, cualquier sensor real conectado a una red IP puede interactuar fácilmente con el SOS.

8.1.3. UniverSEC

- La aplicación del smart grid al sistema de red eléctrica, es esencial para mejorar la calidad del servicio y reducir los altos costos que tiene actualmente. Mediante la integración de los desarrollos de la ingeniería eléctrica y los avances en TIC, se puede lograr una mejora en la eficiencia, fiabilidad, sostenibilidad de la producción y distribución de la energía.
- La combinación de una red de comunicaciones y la interconexión de todos los elementos con el smart grid, aumenta significativamente la vulnerabilidad de todo el sistema, por lo que es necesario que el nuevo sistema sea totalmente seguro en todas sus etapas: generación, transmisión, distribución y consumo.
- Para garantizar la seguridad de la red de una infraestructura crítica, como el caso del smart grid, es necesario un sistema similar a un SGSI, capaz de conocer, gestionar y minimizar los riesgos que atenten contra la seguridad de la información, mediante la monitorización continua de los elementos del smart grid en todas sus etapas.
- Se ha utilizado como parámetro de evaluación de la seguridad, tanto del conjunto del smart grid, como de cada uno de sus componentes, el parámetro Security Assurance (SA), que mide la confianza objetivo para cumplir los requerimientos de seguridad fijados para realizar sus actividades y mantener la confidencialidad, integridad y disponibilidad de la información.
- La estructura jerárquica del SA permite diseñar todos los servicios necesarios, a partir de las vulnerabilidades detectadas por SCAP. Gracias a la posibilidad de definir nuestros propios BMs, DMs, OMR, etc. y combinarlos, se logra un alto nivel de garantía de seguridad.
- La utilización de la arquitectura I3WSN para el sistema propuesto facilita la adaptación a cualquier tipo de red, ya que tiene dos bloques independientes, el sistema de medida para la recogida de datos en tiempo real y el centro de control para el procesamiento y visualización.
- El sistema propuesto utiliza protocolos y estándares internacionales. El SOS de SWE, permite almacenar los datos de todos los sensores en una forma estándar y acceder a ellos de forma sencilla, tanto para los sensores como las aplicaciones. Por otra parte, el uso de SCAP automatiza el acceso a las vulnerabilidades de los

dispositivos del smart grid. Tanto el SOS, como SCAP, permiten una fácil integración de nuevas funcionalidades al sistema y la adaptación a otros entornos.

- A través de la HMI, el supervisor de la red, puede ver el estado real del SA de todos los dispositivos y servicios, así como estadísticas, gráficas o alarmas correspondientes. En caso de ser necesario puede también revisar todos los datos almacenados en el SOS y los procesados posteriormente.

8.1.4. STIMULO

- Los sistemas de transporte inteligente, son aquellos que utilizan las tecnologías TIC para mejorar la gestión y la seguridad en el transporte terrestre. En la actualidad, están siendo implantados en muchos lugares, ya que permite por ejemplo, mejorar la movilidad en el transporte público y mantener informados a los usuarios, o también, mejorar la comunicación entre vehículos para elevar el nivel de seguridad.
- En particular, el proyecto STIMULO ha creado un sistema ITS capaz de mejorar la eficiencia en el transporte de contenedores de mercancías con información en tiempo real de sensores y cámaras. Para ello, utiliza modelos de simulación basados en los datos de tráfico obtenidos, y procesos de inteligencia colectiva para evaluar las distintas opciones (rutas, paradas, etc.). Su objetivo es predecir y gestionar el tiempo real de llegada de los camiones de transporte de mercancías al puerto, de manera que se optimice el tiempo de carga y descarga.
- Los sistemas ITS están muy relacionado con el término smart city, el cual, engloba todos aquellos sistemas que utilizan las TIC para mejorar el desarrollo sostenible de la ciudad. Se centra principalmente en la gestión de la energía, la movilidad inteligente, la logística, etc.
- El bloque central del sistema STIMULO debe comunicarse con múltiples actores para poder operar correctamente. En primer lugar, debe recibir información de todas las fuentes disponibles. Después, debe comunicarse con el sistema que va a gestionar, en este caso el PCS del puerto de Valencia, para recibir las órdenes de transporte. Por último, debe estar en contacto continuo con los transportistas para indicarles la ruta inicial prevista y los posibles cambios en función del tráfico.
- La principal fuente de datos del sistema es el estado del tráfico obtenido a partir de las imágenes de la DGT, AYV, GV y GC. Pero además del IMT, son necesarios otros datos para el funcionamiento. Debe conocer el mapa de todas las carreteras en la zona de evaluación, representadas estructuralmente y con información detallada como la que ofrece OSM. Necesita también un modelo de tráfico que modele el comportamiento real de los vehículos, calculado a partir de datos históricos y en tiempo real. Son necesarias las órdenes de transporte del puerto de Valencia donde se indica la matrícula del camión, tipo de operación, origen y

destino de los contenedores. Por último, necesita las posiciones reales de los camiones que se están monitorizando.

- El despliegue de cámaras, con acceso abierto a sus imágenes, da la oportunidad de crear sistemas de monitorización del tráfico en las carreteras en tiempo real, para modelar y verificar un modelo de tráfico con el que poder predecir rutas.
- La arquitectura de los bloques de adquisición de cámaras (SAC) y módulo de visión artificial (VA) del sistema STIMULO, se basa en la arquitectura I3WSN. El SAC es el encargado de la obtención de imágenes, primero mediante la descarga de las imágenes o vídeo y después realizando la validación de cada una de ellas. Por otra parte, la VA realiza un procesado de las imágenes para después poder obtener el valor de IMT de cada una y almacenarlo en el SOS.
- La Inteligencia Colectiva (IC) es el núcleo del sistema de gestión de rutas, el cual, permite planificar todas las rutas teniendo en cuenta las restricciones temporales, las de tráfico y las que imponga cada vehículo. Para poder tomar este tipo de decisiones, es necesario un sistema de simulación de tráfico que permita simular en tiempo real un escenario verídico con el tráfico real correspondiente. Para ello, se utiliza el simulador SUMO, el cual, permite estimar los tipos de llegada al puerto de Valencia óptimos, en función del tráfico que se extrae del modelo de tráfico.
- STIMULO dispone de un interfaz gráfico, a través del cual, es posible llevar a cabo la configuración del sistema. Se deben introducir todas las fuentes de datos de las que se va a extraer información (cámaras, espiras, etc.). Tras el registro se puede activar el servicio para que empiece a monitorizar todos los dispositivos. También da acceso al usuario a todas las medidas en tiempo real del valor de IMT, obtenido de las distintas fuentes.
- Para dar acceso al sistema STIMULO a los conductores de los vehículos mientras están en la carretera, se ha creado una aplicación móvil, en la cual, se le indica al conductor la ruta, la hora de llegada prevista, o las paradas que debe realizar. El conductor también informa al sistema cuando llega a su destino, o cuando advierte una incidencia en la carretera.

8.2. Líneas futuras de investigación

Si bien es posible ampliar el estudio realizado en esta tesis en múltiples direcciones, en esta sección se ofrecen algunas opciones, tanto en el ámbito de SWE, como en los casos de uso presentados.

- SWE ha demostrado su eficacia para una amplia variedad de proyectos y aplicaciones, aunque no es todavía ampliamente utilizado en aplicaciones comerciales. Uno de los motivos, es el carácter genérico de los estándares que se requieren para ser aplicado en una amplia gama de dominios. La flexibilidad requerida permite, por una parte, la integración de sensores heterogéneos, pero por otro lado, deja ciertos elementos genéricos para cumplir el requisito de

flexibilidad. Esto hace que sea difícil la implementación de clientes genéricos e interoperables capaces de tratar con diferentes implementaciones SOS. Un enfoque útil para hacer frente a este problema, es definir perfiles específicos de dominio.

- La última versión de SWE, mejora significativamente las especificaciones de alerta y notificación de eventos, aumentando la funcionalidad de filtrado de eventos. Pero los últimos desarrollos indican un aumento de la necesidad de una arquitectura común de eventos, no solo para *sensor web*, sino para SDI. El SES y SPS son los primeros pasos hacia esta funcionalidad común, pero deben ser mejorados.
- El conocimiento de la procedencia, la calidad y la incertidumbre de los datos de los sensores, es esencial a la hora de tomar decisiones acertadas. En la actualidad, esta información no suele estar incorporada en la implementación de los mensajes y no existe una manera única de hacerlo.
- Desde hace tiempo, se han creado nuevas aplicaciones (las llamadas aplicaciones web 2.0), en las que los usuarios se interconectan a través de sus redes sociales y son proveedores y consumidores de datos al mismo tiempo. Esto permite aprovechar la inteligencia colectiva para aplicaciones innovadoras. Por tanto, analizar y utilizar las conexiones sociales entre usuarios de plataformas de redes sociales, para mejorar la red de sensores, es otra línea de investigación emergente.
- Como se ha visto en el capítulo 2, la investigación sobre semántic sensor web, estudia el papel de las anotaciones semánticas, ontologías, y el razonamiento para mejorar la funcionalidad de sensor web, tales como el descubrimiento de sensores o la integración entre ellos. Existen muchos estudios sobre el tema e incluso alguna implementación, pero todavía no se utiliza habitualmente.
- Dentro del caso de uso FASyS, sería interesante analizar e incorporar nuevos escenarios de riesgo dentro de la fábrica, para intentar englobar todas las situaciones de riesgo posible, susceptible de ocurrir en cualquier tipo de fábrica de mecanizado y montaje.
- Es importante introducir nuevas tecnologías inalámbricas y abiertas que se utilicen en entornos industriales, a medida que aparezcan. También, añadir nuevos sensores capaces de medir aquellas propiedades físicas necesarias, especialmente en las redes de área personal inalámbrica (WPAN), para la recopilación de información de los trabajadores.
- En el caso de optar por la utilización de Smart Objects para la virtualización de los trabajadores, se debe tener precaución con la gestión de los SOs a medida que aumentan. Es también un tema de investigación en el ámbito de las técnicas de computación en nube.
- El trabajo futuro en el caso de uso de UniverSEC, está orientado a añadir nuevos elementos al smart grid para hacer el sistema más completo, de forma que se incorporen todos los dispositivos, ya sean de la red de gestión del smart grid, o de

la propia red energética. De esta forma todos los elementos que lo componen serán controlados y supervisados por el sistema.

- Otra línea de investigación, puede ser definir nuevos servicios para mejorar la definición del security assurance y corregir posibles nuevas vulnerabilidades.
- También sería interesante, aplicar la metodología y la tecnología propuesta, para monitorizar y garantizar la seguridad en otras infraestructuras críticas.
- En el caso de uso de STIMULO, es imprescindible el conocimiento del estado real del tráfico de las carreteras y las incidencias ocurridas, por lo tanto, hay que añadir nuevas fuentes de información, que sean útiles a la hora de determinar el estado del tráfico, como son radares, puntos negros, redes sociales, etc.
- A la hora de detectar y contar vehículos a partir de las imágenes de las cámaras de tráfico, se necesita que la cámara sea estática y las condiciones sean buenas. Hay que mejorar la detección para que se incluya las cámaras móviles, condiciones meteorológicas adversas, o intensidad lumínica. Además, las cámaras de una misma vía, podrían estar correladas para poder identificar flujos de tráfico.

9. Referencias

9.1. Bibliografía

[1] Y. Demchenko, C. de Laat y P. Membrey, «Defining architecture components of the Big Data Ecosystem,» de *International Conference on Collaboration Technologies and Systems (CTS), pp. 104-112*, Minneapolis, May 2014.

[2] T. Repantis, X. Gu y V. Kalogeraki, «QoS-Aware Shared Component Composition for Distributed Stream Processing Systems,» *IEEE Transactions on Parallel and Distributed Systems,* vol. 20, nº 7, pp. 968-982, Sep 2008.

[3] K. Delin, S. Jackson y R.R., «Sensor Webs,» Some NASA Tech Briefs, 1999.

[4] W. S. Ahn, K. H. Kim y S. W. Yoo, «Study on robustness middleware using integrating Sensor Observation Service in Sensor Web Enablement,» de *The 12th International Conference on Advanced Communication Technology (ICACT), Vol. 1, pp. 476-479*, Feb 2010.

[5] M. Grothe y J. Kooijman, «Sensor Web Enablement».

[6] L. Tan y N. Wang, «Future internet: The Internet of Things,» de *3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), pp. 376-380*, Aug 2010.

[7] L. Coetzee y J. Eksteen, «The Internet of Things - promise for the future? An introduction,» de *IST-Africa Conference Proceedings, pp. 1-9*, May 2011.

[8] «Proyecto FASyS,» [En línea]. Available: www.fasys.es.

[9] «Proyecto UniverSEC,» [En línea]. Available: http://www.satrd.upv.es/proyectos/universec.htm.

[10] «Proyecto STIMULO,» [En línea]. Available: http://innpacto-stimulo.org/proyecto.php.

[11] J. Fraden, Handbook of Modern Sensors, Springer, 2010.

[12] C. Stasch, K. Janowicz, A. Bröring, I. Reis y W. Kuhn, «A Stimulus-Centric Algebraic Approach to Sensors and Observations,» de *GeoSensor Networks*, vol. 5659, Springer, July 2009, pp. vol. 5659, 169–179.

[13] I. Simonis, «OGC Best Practices 06021r4: OGC Sensor Web Enablement Architecture,» Open Geospatial Consortium, Wayland, MA, USA, 2008.

[14] S. Lan, M. Qilong y J. Du, «Architecture of Wireless Sensor Networks for Environmental Monitoring,» de *International Workshop on Geoscience and Remote Sensing*, Dec 2008.

[15] Z. Zhang y X. Hu, «ZigBee based wireless sensor networks and their use in medical and health care domain,» de *Seventh International Conference on Sensing Technology (ICST), pp 756-761*, Dec 2013.

[16] K. A. Delin y E. Small, «The Sensor Web: Advanced Technology for Situational Awareness,» *Wiley Handbook of Science and Technology for Homeland Security,* Mar 2009.

[17] K. A. Delin, «The Sensor Web: Distributed Sensing for Collective Action,» *Sensors online,* July 2006.

[18] Y. Tian, J. Geiger, H. Su, S. Kumar y P. Houser, «Middleware-Based Sensor Web Integration,» *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing,* vol. 3, nº 4, pp. 467-472, Jun 2010.

[19] «NASA sensor web,» [En línea]. Available: sensorwebs.jpl.nasa.gov.

[20] C. Koch y G. Laurent, «Complexity and the Nervous System,» *Science,* vol. 284, nº 5411, pp. 96-98, Apr 1999.

[21] S. H. Liang, A. Croitoru y C. V. Tao, «A distributed geospatial infrastructure for Sensor Web,» *Computers & Geosciences,* vol. 31, nº 2, p. 221–231, Mar 2005.

[22] P. Gibbons, B. Karp, Y. Ke, S. Nath y S. Seshan, «IrisNet: an architecture for a worldwide sensor Web,» *IEEE Pervasive Computing,* vol. 2, nº 4, pp. 1536-1268, Dec 2003.

[23] Y. Tian, J. Geiger, H. Su, S. Kumar y P. Houser, «Middleware-Based Sensor Web Integration,» *IEEE Journal of Applied Earth Observations and Remote Sensing,* vol. 3, nº 4, pp. 467-472, Jun 2010.

[24] «Web de OGC,» [En línea]. Available: http://www.opengeospatial.org/.

[25] «ISO/IEC 74981:Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model,» ISO/IEC, Geneva, Switzerland, 1996.

[26] J. d. Rio, D. M. Toma, T. C. O'Reilly, A. Bröring, D. R. Dana, F. Bache y K. L. Headley, «Standards-based Plug & Work for Instruments in Ocean Observing Systems,» *IEEE Journal of Oceanic Engineering,* vol. 39, nº 3, pp. 430-443, July 2014.

[27] J.-S. Lee, Y.-W. Su y C.-C. Shen, «A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi,» de *33rd Annual Conference of the IEEE Industrial Electronics Society (IECON), pp. 46-51*, Nov 2007.

[28] Z. S. Organization, «ZigBee Specification, Document 053474r17,» ZigBee Alliance, Jan 2008.

[29] J. Song, S. Han, A. Mok, D. Chen, M. Lucas y M. Nixon, «WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control,» de *Proceedings of the IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS'08), pp. 377 - 386*, St. Louis, April 2008.

[30] «Wireless Systems for Industrial Automation: Process Control and Related Applications, Standard 100.11a, Draft 2a,» International Society of Automation (ISA), 2009.

[31] «Bluetooth SIG. Bluetooth Specification Version 3.0,» Bluetooth Special Interest Group, 2009.

[32] ISO/IEC, «ISO/IEC 2934111: 2011: Information technology – UPnP Device Architecture – Part 11: UPnP Device Architecture Version 1.1,» ISO, Geneva, Switzerland, 2011.

[33] S. Motegi, K. Tasaka, A. Idoue y H. Horiuchi, «Proposal on Wide Area DLNA Communication System,» de *5th IEEE Consumer Communications and Networking Conference, pp. 233-237*, Jan 2008.

[34] D. Driscoll y A. Mensch, «OASIS Devices Profile for Web Services (DPWS) Version 1.1,» OASIS, 2009.

[35] G. Alonso, F. Casati, H. Kuno y V. Machiraju, Web Services: Concepts, Architectures and Applications, Springer, 2004.

[36] E. Zeeb, G. Moritz, D. Timmermann y F. Golatowski, «WS4D: Toolkits for Networked Embedded Systems Based on the Devices Profile for Web Services,» de *39th International Conference on Parallel Processing Workshops (ICPPW)*, San Diego, CA, Sept 2010.

[37] O. Bergmann, K. Hillmann y S. Gerdes, «A CoAP-gateway for smart homes,» de *International Conference on Computing, Networking and Communications (ICNC), pp. 446-450*, Feb 2012.

[38] A. Abd El-Aziz y A. Kannan, «JSON encryption,» de *International Conference on Computer Communication and Informatics (ICCCI), pp. 1-6*, Jan 2014.

[39] «Extensible Markup Language (XML) 1.0 (Third Edition),» W3C Recommendation, 2004. [En línea]. Available: http://www.w3.org/TR/2004/REC-xml-20040204.

[40] V. Sinha, F. Doucet, C. Siska, R. Gupta, S. Liao y A. Ghosh, «YAML: a tool for hardware design visualization and capture,» de *13th International Symposium on System Synthesis, pp. 9-14*, Sep 2000.

[41] K. Lee, «IEEE 1451: A Standard in Support of Smart Transducer Networking,» *Proceedings of the 17th IEEE Instrumentation and Measurement Technology Conference,* vol. 2, nº 525-528, May 2000.

[42] K. Lee y E. Song, «Object-oriented application framework for IEEE 1451.1 standard [smart sensors],» de *Proceedings of the 21st IEEE Instrumentation and Measurement Technology Conference (IMTC 04), vol. 2, pp. 1182-1187*, May 2004.

[43] C. Granell, M. Gould, M. Á. Manso y M. Á. Bernabé, «Handbook of Research on Geoinformatics,» de *Spatial Data Infrastructures*, IGI Global, 2009, pp. 36-41.

[44] J. De La Beaujardiere, «OpenGIS® Web Map Server Implementation Specification,» Version 1.3.0. (=OGC, 06-042), 2006.

[45] A. Whiteside y J. D. Evans, «Web Coverage Service (WCS) Implementation Specification,» Version 1.1.0. (=OGC, 06-083r8), 2006.

[46] P. A. Vretanos, «Web Feature Service Implementation Specification,» Version 1.1.0. (=OGC, 04-094), 2004.

[47] S. Cox, P. Daisey, R. Lake, C. Portele y A. Whiteside, «OpenGIS® Geography Markup Language (GML) Implementation Specification,» Version 3.1 RP.(=OGC, 03-105r1), 2004.

[48] S. Havens, «Transducer Markup Language Implementation Specification,» Version 1.0.0. (=OGC, 06-010r6), 2006.

[49] H. Conover, G. Berthiau, M. Botts, H. M. Goodman y X. Li, «Using sensor web protocols for environmental data acquisition and management,» *Ecological Informatics,* vol. 5, nº 1, pp. 32-41, Jan 2010.

[50] M. Botts, «Sensor Model Language (SensorML) Implementation Specification,» Version 1.0. (=OGC, 07-000), 2007.

[51] S. Cox, «Observations and Measurements - Part 1 - Observation schema,» Version 1.0. (=OGC, 07-022r1), 2007.

[52] A. Na y M. Priest, «Sensor Observation Service - Implementation Specification,» Version 1.0. (=OGC, 06-009r6), 2007.

[53] «52 North. Sensor Web Community,» [En línea]. Available: http://52north.org/communities/sensorweb/index.html.

[54] I. Simonis, «Sensor Alert Service,» Version 0.9. (=OGC, 06-028r3), 2006.

[55] I. Simonis, «Sensor Planning Service Implementation Specification,» Version 1.0. (=OGC, 07-014r3), 2007.

[56] I. Simonis y Echterhoff, «Draft OpenGIS® Web Notification Service Implementation Specification,» Version 0.0.9. (=OGC, 06-095), 2006.

[57] D. Nebert y A. Whiteside, «OpenGIS Catalog Services Specification,» Version 2.0.0 with Corrigendum (=OGC, 04-021r3), 2005.

[58] J. Nogueras-Iso, F. Zarazaga-Soria, R. Béjar, P. Álvarez y P. Muro-Medrano, «OGC Catalog Services: a key element for the development of Spatial Data Infrastructures,» *Computers & Geosciences,* vol. 31, nº 2, pp. 199-209, Mar 2005.

[59] N. Chen, L. Di, G. Yu, J. Gong y Y. Wei, «Use of ebRIM-based CSW with sensor observation services for registry and discovery of remote-sensing observations,» *Computers & Geosciences,* vol. 35, nº 2, pp. 360-372, Feb 2009.

[60] O. G. C. Inc., «OpenGIS® Catalogue Services Specification 2.0 - ISO19115/ISO19119 Application Profile for CSW 2.0,» OGC 04-038r1, Jul 2004.

[61] K. Senkler, U. Voges y A. Remke, «An ISO 19115/19119 profile for OGC catalogue services CSW 2.0,» de *10th EC GI & GIS Workshop*, Jun 2004.

[62] H. Kopetz, «Internet of Things,» de *Real-Time Systems*, Springer, Feb 2011, pp. 307-323.

[63] V. Cronin y K. Sverdrup, «Defining static correction for jointly relocated earthquakes along the Blanco Transform Fault Zone based on SOSUS hydrophone data,» de *Proceedings OCEANS, vol 5, pp. 2721-2726*, San Diego, CA, USA, Sept 2003.

[64] P. Marshall, «Extending the Reach of Cognitive Radio,» *Proceedings of the IEEE,* vol. 97, nº 4, pp. 612-625, April 2009.

[65] K. Martinez, R. Ong y J. Hart, «Glacsweb: a sensor network for hostile environments,» de *First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, pp. 81-87*, Oct 2004.

[66] J. Zhou y D. De Roure, «FloodNet: Coupling Adaptive Sampling with Energy Aware Routing in a Flood Warning System,» *Journal of Computer Science and Technology,* vol. 22, nº 1, pp. 121-130, Sept 2006.

[67] S. Islam, A. Fathy, Y. Wang, M. Kuhn y M. Mahfouz, «Hassle-Free Vitals: BioWireleSS for a Patient-Centric Health-Care Paradigm,» *IEEE Microwave Magazine,* vol. 15, nº 7, pp. S25-S33, Dec 2014.

[68] R. Paradiso, T. Faetti y S. Werner, «Wearable monitoring systems for psychological and physiological state assessment in a naturalistic environment,» de *Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp. 2250-2253*, Sep 2011.

[69] M. Baig, H. GholamHosseini, M. Connolly y G. Kashfi, «Real-time vital signs monitoring and interpretation system for early detection of multiple physical signs in older adults,» de *IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI), 355-*

358, Jun 2014.

[70] D. Kelly, S. McLoone y R. Farrell, «Minimal hardware Bluetooth tracking for long-term at-home elder supervision,» de *Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp. 2136 - 2140*, Buenos Aires, Sep 2010.

[71] N. Chen, Z. Zheng y Z. Chen, «An Efficient Sensor Observation Data Registration based on Asynchronous Service Middleware,» de *IFIP International Conference on Network and Parallel Computing Workshops*, Liaoning, Sep 2007.

[72] G. McFerren, D. Hohls, G. Fleming y T. Sutton, «Evaluating Sensor Observation Service implementations,» de *IEEE International Geoscience and Remote Sensing Symposium (IGARSS 2009)*, Cape Town, July 2009.

[73] J.-C. Liu y K.-Y. Chuang, «WASP: An innovative sensor observation service with web-/GIS-based architecture,» de *17th International Conference on Geoinformatics*, Fairfax VA, Aug 2009.

[74] C. Henson, J. Pschorr, A. Sheth y K. Thirunarayan, «SemSOS: Semantic Sensor Observation Service,» de *Proceedings of International Symposium on Collaborative Technologies and Systems (CTS 2009)*, Baltimore, May 2009.

[75] I. Simonis y M. Van Der Merwe, «Earth Observation and Environmental Modelling for the Mitigation of Health Risks such as cholera, cardio-vascular and respiratory diseases,» de *IST-Africa Conference Proceedings, pp 1-8*, May 2011.

[76] M. Pulido-Velazquez, J. Sauer, P. Koundouri y A. Allan, «The EU FP7 GENESIS project on groundwater systems. Contributions to the analysis of economic, legal and institutional issues of groundwater management with selected case studies,» Mar 2013.

[77] L. Bermudez, T. Cook, D. Forrest y P. Bogden, «Web feature service (WFS) and sensor observation service (SOS) comparison to publish time series data,» de *Proceedings of International Symposium on Collaborative Technologies and Systems (CTS '09)*, Baltimore, May 2009.

[78] P. Yue, C. Guo y L. Jiang, «Using Google Fusion Tables for Cloud-based sensor observation services,» de *Second International Conference on Agro-Geoinformatics*, Fairfax VA, Aug 2013.

[79] H. Wang, L. Di, G. Yu y B. Zhang, «Implementation of Sensor Observation Service for Satellite Imagery Sensors,» de *17th International Conference on Geoinformatics*, Fairfax VA, Aug 2009.

[80] A. Witayangkurn, M. Nagai, K. Honda, M. Dailey y R. Shibasaki, «Real-time Monitoring System Using Unmanned Aerial Vehicle Integrated With Sensor Observation Service,» de *Conference on Unmanned Aerial Vehicle in Geomatics*, Zurich, Switzerland, Sep 2011.

[81] E. Pebesma, D. Cornford, G. Dubois, G. B. Heuvelink y D. Hristopulos, «INTAMAP: The design and implementation of an interoperable automated interpolation web service,» *Computers & Geosciences,* vol. 37, nº 3, pp. 343-352, Mar 2011.

[82] «Web de MapServer SOS,» [En línea]. Available: http://mapserver.org/ogc/sos_server.html.

[83] «Web de Deegree SOS,» [En línea]. Available: http://wiki.deegree.org/deegreeWiki/deegree3/SensorObservationService.

[84] T. Berners-Lee, J. Hendler y O. Lassila, «The Semantic Web,» *Scientific American,* p. 34–43, May 2001.

[85] G. Klyne y J. J. Carroll, «Resource Description Framework (RDF): Concepts and Abstract Syntax,» W3C Recommendations, 2004.

[86] D. L. McGuinness y F. v. Harmelen, «OWL Web Ontology Language - Overview,» W3C Recommendations, 2004.

[87] C. Ji, J. Liu y X. Wang, «Associating Semantic Sensor Web with Domain Ontology: The Way to Obtain Meaningful Sensor Data,» *International Journal of u-and e-Service, Science and Technology,* vol. 7, nº 5, pp. 271-282, 2014.

[88] A. Sheth, C. Henson y S. Sahoo, «Semantic Sensor Web,» *IEEE Internet Computing,* vol. 12, nº 4, pp. 78-83, Aug 2008.

[89] O. Corcho y R. Garcia-Castro, «Five challenges for the Semantic Sensor Web,» *Semantic Web,* vol. 1, nº 1,2, pp. 121-125, Apr 2010.

[90] V. Podgorelec y L. Pavlic, «Managing Diagnostic Process Data Using Semantic Web,» de *IEEE International Symposium on Computer-Based Medical Systems (CBMS '07), 127-134*, Jun 2007.

[91] R. Stevens, S. Jupp, J. Klein y J. Schanstra, «Using semantic web technologies to manage complexity and change in biomedical data,» de *Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp. 3708-3711*, Aug 2011.

[92] S. Ilarri, A. lllarramendi, E. Mena y A. Sheth, «Semantics in Location-Based Services,» *IEEE Internet Computing,* vol. 15, nº 6, pp. 10-14, Dec 2011.

[93] K. Ganesh, M. Sekar y V. Vaidehi, «Semantic Intrusion Detection System using pattern matching and state transition analysis,» de *International Conference on Recent Trends in Information Technology (ICRTIT), pp. 607-612*, Jun 2011.

[94] M. Tan, W. Zhou, L. Zheng y S. Wang, «A Scalable Distributed Syntactic, Semantic, and Lexical Language Model,» *Computational Linguistics,* vol. 38, nº 3, pp. 631-671, Nov

2011.

[95] H.-S. Choi y W.-S. Rhee, «Distributed semantic sensor web architecture,» de *IEEE Conference TENCON, pp.1-6*, Nov 2012.

[96] B. Wang y D. Liu, «Basic Theory System of Knowledge Engineering in Product Design Domain,» de *International Conference on System Science, Engineering Design and Manufacturing Informatization (ICSEM), vol. 2, pp. 292-295*, Nov 2010.

[97] D.-J. Kang, J.-J. Lee, S.-J. Kim y J.-H. Park, «Analysis on cyber threats to SCADA systems,» de *Transmission & Distribution Conference & Exposition: Asia and Pacific*, Oct 2009.

[98] S. Shyne, D. Kidston y P. George, «Distributed multi-national network operation centres,» de *Military Communications Conference (MILCOM), vol. 2, pp. 598-602*, Nov 2004.

[99] M. Younus, C. Peiyong, L. Hu y F. Yuqing, «MES development and significant applications in manufacturing -A review,» de *2nd International Conference on Education Technology and Computer (ICETC), vol. 5, pp. 97-101*, Jun 2010.

[100] I. Bell, «The future of control [programmable automation controllers],» *Manufacturing Engineer,* vol. 84, nº 4, pp. 36-39, Aug 2005.

[101] «IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related system. Parts 1 to 7,» de *Geneva: International Electrotechnical Commission*, 1998-2000.

[102] «Web del NIST,» [En línea]. Available: http://csrc.nist.gov/publications/PubsNISTIRs.html.

[103] R. K. Abercrombie y F. T. Sheldon, «Risk Assessment Methodology Based on the NISTIR 7628 Guidelines,» de *46th Hawaii International Conference on System Sciences (HICSS)*, HI, USA, Jan 2013.

[104] A. C. Chan y J. Zhou, «On Smart Grid Cybersecurity Standardization: Issues of Designing with the NISTIR 7628,» *Communications Magazine, IEEE,* vol. 51, nº 1, pp. 58 - 65, Jan 2013.

[105] «Web del British Standards Institution,» [En línea]. Available: http://www.bsigroup.com/.

[106] «Web esándar 27000,» [En línea]. Available: http://www.27000.org/.

[107] «Web oficial del proyecto Common Criteria,» [En línea]. Available: http://www.commoncriteriaportal.org/.

[108] M. Vetterling, G. Wimmel y A. Wisspeintner, «Secure Systems Development Based on the Common Criteria: The PalME Project,» *ACM SIGSOFT,* vol. 27, nº 6, pp. 129-138, Nov 2002.

[109] S. Houmb, S. Islam, E. Knauss, J. Jürjens y K. Schneider, «Eliciting Security Requirements and Tracing them to Design: An Integration of Common Criteria, Heuristics, and UMLsec,» *Requirements Engineering,* vol. 15, nº 1, pp. 63-93, March 2010.

[110] M. Bartsch, «German Smart Metering and European Privacy Needs,» de *Proceedings of International ETG-Congress 2013. Symposium 1: Security in Critical Infrastructures Today*, Berlin, Germany, Nov 2013.

[111] K. Clark, S. Tyree, J. Dawkins y J. Hale, «Qualitative and Quantitative Analytical Techniques for Network Security Assessment,» de *Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, pp. 321-328*, New York, June 2004.

[112] K. Taguchi, N. Yoshioka, T. Tobita y H. Kaneko, «Aligning Security Requirements and Security Assurance Using the Common Criteria,» de *Fourth International Conference on Secure Software Integration and Reliability Improvement (SSIRI)*, Singapore, June 2010.

[113] M. Ouedraogo, H. Mouratidis, D. Khadraoui y E. Dubois, «Security Assurance Metrics and Aggregation Techniques for IT Systems,» de *Fourth International Conference on Internet Monitoring and Protection (ICIMP '09), pp. 98-102*, Venice, May 2009.

[114] J. Lokoč, J. Moško, P. Čech y T. Skopal, «On indexing metric spaces using cut-regions," , vol. 43, p. 1–19, 2014,» *Information Systems,* vol. 43, pp. 1-19, Jan 2014.

[115] N. Seddigh, P. Pieda, A. Mattrawy, B. Nandy, J. Lambardis y A. Hatfield, «Current Trends and Advances in Information Assurance Metrics,» de *Proceeding of the Second Annual Conference on Privacy, Security and Trust*, New Brunswic, Canada, Oct 2004.

[116] T. Klevinsky, S. Laliberte y A. Gupta, Hack I.T. - Security Through Penetration Testing, Addison-Wesley Professional, Feb 2002.

[117] E. Bulut, D. Khadraoui y B. Marquet, «Multi-Agent based Security Assurance Monitoring System for Telecommunication Infrastructures,» de *Proceedings of the Fourth International Conference on Communication, Network and Information Security (CNIS '07), pp. 90-95*, Berkeley, California, Sept 2007.

[118] T. Kanstrén, R. Savola, A. Evesti, H. Pentikäinen, A. Hecker, M. Ouedraogo, K. Hätönen, P. Halonen, C. Blad, O. López y S. Ros, «Towards an abstraction layer for security assurance measurements,» de *Proceedings of the Fourth European Conference on Software Architecture (ECSA '10)*, Copenhagen, Denmark, Aug 2010.

[119] Y. Mu y C. Shen, «Building up active-defending security assurance framework for e-commerce,» de *IET International Conference on Wireless, Mobile and Multimedia*

Networks, China, Nov 2006.

[120] R. Chandrasekaran, «Security Assurance Using Face Recognition & Detection System Based On Neural Networks,» de *International Conference on Neural Networks and Brain (ICNN&B '05), pp. 1100-1106*, Oct 2005.

[121] P. Giménez, B. Molina, C. E. Palau y M. Esteve, «Security assurance en Smart Grid,» de *URSI*, 2014.

[122] O. Al-Jarrah y A. Arafat, «Network Intrusion Detection System using attack behavior classification,» de *5th International Conference on Information and Communication Systems (ICICS), pp. 1-6*, Apr 2014.

[123] D. Stiawan, A. Abdullah y M. Idris, «The trends of Intrusion Prevention System network,» de *2nd International Conference on Education Technology and Computer (ICETC), vol. 4, pp. V4-217 - V4-221*, Jun 2010.

[124] K. Saghar, D. Kendall y A. Bouridane, «Vulnerability of insens to denial of service attacks,» de *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 1896-1899*, Prague, May 2011.

[125] A. Perrig, R. Szewczyk, V. Wen, D. Culler y J. D. Tygar, «SPINS: Security Protocols for Sensor Networks,» de *Mobile Computing and Networking*, Rome, 2001.

[126] H. Xiangdong y F. Rui, «Message Broadcast Authentication in uTESLA Based on Double Filtering Mechanism,» de *International Conference on Internet Technology and Applications (iTAP), pp. 1-4*, Aug 2011.

[127] L. Tobarra, D. Cazorla y F. Cuartero, «Formal Analysis of Sensor Network Encryption Protocol (SNEP),» de *IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), pp. 1-6*, Pisa, Oct 2007.

[128] M. Enzweiler y D. M. Gavrila, «Monocular Pedestrian Detection:Survey and Experiments,» *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 31, nº 12, pp. 2179-2195, oct 2009.

[129] M. Cracknell, «Image Detection in the Real World-A Progress Update,» de *Proceedings ITS World Congress*, Nov 2008.

[130] Citilog, «Paving Intelligence into Safety, Security and Mobility,» 2011.

[131] S. Kantawong y T. Phanprasit, «Intelligent traffic cone based on vehicle accident detection and identification using image compression analysis and RFID system,» de *International Conference on Electrical Engineering/Electronics Computer Telecommunications and Information Technology (ECTI-CON)*, May 2010.

[132] P. Guha, A. Mukerjee y K. S. Venkatesh, «Appearance-Based Multiple-Agent Tracking under Complex Occlusions,» de *PRICAI 2006: Trends in Artificial Intelligence*, Springer, 2006, pp. 593-602.

[133] N. K. Kanhere y S. T. Birchfield, «Real-Time Incremental Segmentation and Tracking of Vehicles at Low Camera Angles using Stable Features,» *IEEE Transactions on Intelligence Transportation Systems,* vol. 9, nº 1, pp. 148-160, Mar 2008.

[134] S. Messelodi, C. M. Modena y M. Zanin, «A Computer Vision System for the Detection and Classification of Vehicles at Urban Road Intersections,» de *Pattern Analysis and Applications, vol. 8, nº 1-2*, Springer, Sep 2005, pp. 17-31.

[135] C.-L. Huang y W.-C. Liao, «A Vision-Based Vehicle Identification System,» de *Proceedings of the 17th International Conference on Pattern Recognition (ICPR), vol. 4, pp. 364-367*, Aug 2004.

[136] N. Buch, J. Orwell y S. Velastin, «Urban Road User Detection and Classification using 3-D Wireframe Models,» *IET Computer Vision,* vol. 4, nº 2, pp. 105-116, Jun 2010.

[137] S. Agarwal, A. Awan y D. Roth, «Learning to Detect Objects in Images Via a Sparse Part-Based Representation,» *IEEE Transactions on Pattern Analysis and Machine,* vol. 26, nº 11, pp. 1475-1490, Sep 2004.

[138] D. G. Lowe, «Object recognition from local scale-invariant features,» de *Proceedings of the Seventh IEEE International Conference on Computer Vision, vol. 2, pp. 1150-1157*, 1999.

[139] H. Bay, T. Tuytelaars y L. V. Gool, «SURF: Speeded-Up Robust Features,» de *Computer Vision - ECCV 2006, vol.* , Springer, 2006, pp. 404-417.

[140] W. T. Freeman y M. Roth, «Orientation Histograms for Hand Gesture Recognition,» de *IEEE International Workshop on Automatic Face and Gesture-Recognition, pp. 296-301*, 1995.

[141] N. Dalal y B. Triggs, «Histograms of oriented gradients for human detection,» de *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), vol. 1, pp. 1063-6919* , 2005.

[142] N. Buch, J. Orwell y S. A. Velastin, «3D Extended Histogram of Oriented Gradients (3DHOG) for Classification of Road Users in Urban Scenes,» de *Proceedings of British Machine Conference*, 2009.

[143] A. Opelt, A. Pinz y A. Zisserman, «A Boundary-Fragment-Model for Object Detection,» de *Computer Vision – ECCV 2006*, Springer, 2006, pp. 575-588.

[144] Y. F. y. R. E. Schapire, «A Short Introduction to Boosting. TheJapanese Society for Artificial Intelligence,» *Journal of Japanese Society for Artificial Intelligence,* vol. 14, nº 5,

pp. 771-780, Sep 1999.

[145] N. Buch, S. A. Velastin y J. Orwell, «A Review of Computer Vision Techniques for the Analysis of Urban Traffic,» *IEEE Transactions on Intelligent Transportation Systems,* vol. 12, nº 3, pp. 920-939, Mar 2011.

[146] P. Viola y M. J. Jones, «Robust Real-Time Face Detection,» *International Journal of Computer Vision,* vol. 57, nº 2, pp. 137-154, May 2004.

[147] D. Beimer, P. MacLauchlan, B. Coifman y J. Malik, «A real-time computer vision system for measuring traffic parameters,» de *Proceedings of IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pp. 495-501*, Jun 1997.

[148] N. S. y. T. Sayed, «A feature-based tracking algorithm for vehicles in intersections,» de *Proceedings of the 3th Canadian Conference on Computer and Robot Vision, pp. 59*, Jun 2009.

[149] D. Bloisi y L. Iocchi, «Argos-A video surveillance system for boat traffic monitoring in Venice,» de *Proceedings of International Journal of Pattern Recognition and Artificial Intelligence, pp. 1477-1502*, 2009.

[150] Z. Kim y J. Malik, «Fast vehicle detection with probabilistic feature grouping and its application to vehicle tracking,» de *Proceedings of the 9th International Conference of Computer Vision, vol. 1, pp. 524-531*, Oct 2003.

[151] S. Gupte, O. Masoud, R. F. K. Martin y N. P. Papanikolopoulos, «Detection and Classification of Vehicles.,» *IEEE Transactions on Intelligent Transportation Systems,* vol. 3, nº 1, pp. 37-47, Aug 2002.

[152] R. Rad y M. Jamzad, «Real time classification and tracking of multiple vehicles in highways,» *Pattern Recognition Letters,* vol. 26, nº 10, pp. 1597-1607, Jul 2005.

[153] R. Claes, T. Holvoet y D. Weyns, «A Decentralized Approach for Anticipatory Vehicle Routing Using Delegate Multiagent Systems,» *IEEE Transactions on Intelligent Transportation Systems,* vol. 12, nº 2, pp. 364-373, Mar 2011.

[154] K. Wunderlich, D. Kaufman y R. Smith, «Link travel time prediction for decentralized route guidance architectures,» *IEEE Transactions on Intelligent Transportation Systems,* vol. 1, nº 1, pp. 4-14, Mar 2000.

[155] T. Yamashita, K. Izumi, K. Kurumatani y H. Nakashima, «Smooth traffic flow with a cooperative car navigation system,» de *Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems (AAMAS '05), pp. 478-485*, 2005.

[156] Y. Ando, Y. Fukazawa, O. Masutani, H. Iwasaki y S. Honiden, «Performance of pheromone model for predicting traffic congestion,» de *Proceedings of the fifth international joint*

conference on Autonomous agents and multiagent systems (AAMAS '06), pp. 73-80, May 2006.

[157] T. Ito, R. Kanamori, J. Takahashi, I. M. Maestre y E. d. l. Hoz, «The Comparison of Stigmergy Strategies for Decentralized Traffic Congestion Control: Preliminary Results,» de *PRICAI 2012: Trends in Artificial Intelligence, vol. 7458, pp. 146-156*, Springer, 2012.

[158] B. Tatomir y L. Rothkrantz, «Hierarchical Routing in Traffic Using Swarm-Intelligence,» de *IEEE Intelligent Transportation Systems Conference (ITSC '06), pp.230-235*, Sep 2006.

[159] K. Dresner y P. Stone, «Multiagent traffic management: a reservation-based intersection control mechanism,» de *Proceedings of the Third International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS), pp. 530 - 537*, Jul 2004.

[160] M. Vasirani y S. Ossowsky, «A Computational Market for Distributed Control of Urban Road Traffic Systems,» *IEEE Transactions on Intelligent Transportation Systems,* vol. 12, nº 2, pp. 313-321, Feb 2011.

[161] H. V. D. Parunak y S. Brueckner, «Modeling uncertain domains with polyagents,» de *Proceedings of the fifth international joint conference on Autonomous agents and multiagent systems (AAMAS '06), pp. 111–113*, May 2006.

[162] R. Junges y A. Bazzan, «Evaluating the performance of DCOP algorithms in a real world dynamic problem,» de *Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems (AAMAS '08), vol. 2, pp. 599-606*, May 2008.

[163] L. Kuyer, S. Whiteson, B. Bakker y N. Vlassis, «Multiagent Reinforcement Learning for Urban Traffic Control Using Coordination Graphs,» de *Machine Learning and Knowledge Discovery in Databases, vol. 5211*, Springer, 2008, pp. 656-671.

[164] S. Lämmer y D. Helbing, «Self-Control of Traffic Lights and Vehicle Flows in Urban Road Networks,» *Journal of Statistical Mechanics: Theory and Experiment,* vol. 4, Feb 2008.

[165] M. Abdel-Aty y M. Abdalla, «Examination of multiple mode/route-choice paradigms under ATIS,» *IEEE Transactions on Intelligent Transportation Systems,* vol. 7, nº 3, pp. 332-248, Sep 2006.

[166] R. Rossetti, S. Bampi, L. Ronghui, D. V. Vliet y H. Cybis, «An agent-based framework for the assessment of drivers' decision-making,» de *Proceedings of the IEEE International Conference on Intelligent Transportation Systems, pp.387-392*, Oct 2000.

[167] R. Prud'homme y J. P. Bocarejo, «The London congestion charge: a tentative economic appraisal,» *Transport Policy,* vol. 12, nº 3, pp. 279-287, May 2005.

[168] J. Eliasson y L.-G. Mattsson, «Equity effects of congestion pricing. Quantitative methodology and a case study for Stockholm,» *Transportation Research Part A: Policy*

and Practice, vol. 40, nº 7, pp. 602-620, Aug 2006.

[169] P. Olszewski y L. Xie, «Modelling the effects of road pricing on traffic in Singapore,» *Transportation Research Part A: Policy and Practice,* vol. 39, nº 7-9, pp. 755-772, Nov 2005.

[170] L. B. d. Oliveira y E. Camponogara, «Multi-agent model predictive control of signaling split in urban traffic networks,» *Transportation Research Part C: Emerging Technologies,* vol. 18, nº 1, pp. 120-139, Feb 2010.

[171] A. Hegyi, B. D. Schutter y H. Hellendoorn, «Model predictive control for optimal coordination of ramp metering and variable speed limits,» *Tramsportation Research Part C: Emerging Technologies,* vol. 13, nº 3, pp. 185-209, Jun 2005.

[172] M. Papageorgiou, I. Papamichail, A. Messmer y Y. Wang, «Traffic Simulation with METANET,» de *Fundamentals of Traffic Simulation. International Series in Operations Research & Management Science, vol. 145*, Springer, Jun 2010, pp. 399-430.

[173] H. Ezawa y N. Mukai, «Adaptive traffic signal control based on vehicle route sharing by wireless communication,» de *Knowledge-based and intelligent information and engineering systems, vol. 6279*, Springer, 2010, pp. 280-289.

[174] J.-P. Vasseur y A. Dunkels, Interconnecting Smart Objects with IP: The Next Internet, Morgan Kaufmann Publishers, Jul 2010.

[175] «Web de ThingWorx,» [En línea]. Available: http://www.thingworx.com/.

[176] «Web de EVRYTHNG,» [En línea]. Available: https://evrythng.com/.

[177] «Web de Sense,» [En línea]. Available: http://open.sen.se/.

[178] S. Lee, S.-S. Lim, M. Yoon, S.-M. Yoon y J. Kim, «SNS of Things: Concept, issues, and challenges for globe scale interoperability of IoT applications,» de *Sixth International Conf on Ubiquitous and Future Networks (ICUFN), pp. 315-316*, Jul 2014.

[179] A. Gluhak, S. Krco, M. Nati, D. Pfisterer y N. Mitton, «A survey on facilities for experimental Internet of Things research,» *IEEE Communications Magazine,* vol. 49, nº 11, pp. 58-67, Nov 2011.

[180] L. Atzori, A. Iera y G. Morabito, «The Internet of Things: a survey,» *Computer Networks,* vol. 54, nº 15, p. 2787–2805, Oct 2010.

[181] L. Haiyan, C. Song, W. Dalei, N. Stergiou y S. Ka-Chun, «A remote markerless human gait tracking for e-healthcare based on content-aware wireless multimedia communications,» *IEEE Wireless Communications,* vol. 17, nº 1, p. 44–50, Feb 2010.

[182] G. Nussbaum, «People with disabilities: assistive homes and environments,» *Computers Helping People with Special Needs,* pp. 457-460, 2006.

[183] A. Alkar y U. Buhur, «An Internet based wireless home automation system for multifunctional devices,» *IEEE Transactions on Consumer Electronics,* vol. 51, nº 4, pp. 1169-1174, Dic 2005.

[184] M. Darianian y M. Michael, «Smart home mobile RFID-based Internet-of-Things systems and services,» de *International Conference on Advanced Computer Theory and Engineering (ICACTE '08), pp. 116-120*, Dec 2008.

[185] X. Li, R. Lu, X. Liang y X. Shen, «Smart community: an Internet of Things application,» *IEEE Communications Magazine,* vol. 49, nº 11, pp. 68-75, Nov 2011.

[186] M. Yun y B. Yuxin, «Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid,» de *International Conference on Advances in Energy Engineering (ICAEE), pp. 69–72.*, 2010.

[187] F. Cao, F. Jiang y Z. Liu, «Application of ISFET Microsensors with Mobile Network to Build IoT for Water Environment Monitoring,» de *International Conference on Intelligent Environments (IE), pp. 207 - 210*, July 2014.

[188] Z. Liqiang, Y. Shouyi, L. Leibo, Z. Zhen y W. Shaojun, «A crop monitoring system based on wireless sensor network,» *Procedia Environmental Sciences,* vol. 11B, p. 558–565, Dec 2011.

[189] P. Kumar, S. Ranganath, W. Huang y K. Sengupta, «Framework for real-time behavior interpretation from traffic video,» *IEEE Transactions on Intelligent Transportation Systems,* vol. 6, nº 1, pp. 43-53, Mar 2005.

[190] H. Lin, R. Zito y M. Taylor, «A review of travel-time prediction in transport and logistics,» de *Proceedings of the Eastern Asia Society for Transportation Studies, vol. 5, pp. 1433–1448*, 2005.

[191] P. Giménez, B. Molina, J. Calvo-Gallego, C. E. Palau y M. Esteve, «I3WSN: Industrial Intelligent Wireless Sensor Networks for Indoor Environments,» *Computers in industry,* vol. 65, nº 1, pp. 187-199, Jan 2014.

[192] I. Ungurean, N.-C. Gaitan y V. Gaitan, «An IoT architecture for things from industrial environment,» de *10th International Conference on Communications (COMM), pp. 1-4*, May 2014.

[193] A. Daidone, S. Chiaradonna, A. Bondavalli y P. Veríssimo, «Analysis of a Redundant Architecture for Critical Infrastructure Protection,» de *Architecting Dependable Systems V*, Springer Berlin Heidelberg, 2008, pp. 78-100.

[194] M. Berning, T. Riedel, D. Karl, F. Schandinat, M. Beigl y N. Fantana, «Augmented service in the factory of the future,» de *Ninth International Conference on Networked Sensing Systems (INSS)*, Antwerp, June 2012.

[195] M. Sepulcre, J. A. Palazón, J. Gozalvez y J. Orozco, «Wireless Connectivity for Mobile Sensing Applications in Industrial Environments,» de *Proceedings of the 6th IEEE International Symposium on Industrial Embedded Systems (SIES'11), pp 111 - 114*, Vasteras, June 2011.

[196] A. Willig, K. Matheus y A. Wolisz, «Wireless Technology in Industrial Networks,» *Proceedings of the IEEE,* vol. 93, nº 6, p. 1130–1151, June 2005.

[197] J. Li, X. Zhu, N. Tang y J. Sui, «Study on ZigBee network architecture and routing algorithm,» de *July 2010*, Dalian, Proceedings of the 2nd International Conference on Signal Processing Systems (ICSPS'10), pp. 389-393.

[198] J. A. Palazón, M. Sepulcre, J. Gozalvez, J. Orozco y O. López, «Heterogeneous Wireless Connectivity for Fixed and Mobile Sensing Applications in Industrial Environments,» de *Proceedings of the 16th IEEE International Conference on Emerging Technologies & Factory Automation (ETFA), pp. 1 - 8*, Toulouse, Sept. 2011.

[199] K. Koumpis, L. Hanna, M. Andersson y M. Johansson, «Wireless Industrial Control and Monitoring beyond Cable Replacement,» de *Proceedings of the 2nd PROFIBUS International Conference*, Binley, Jun 2005.

[200] Z. Huaji, W. Huarui y S. Xiang, «Research on the Ontology-Based Complex Event Processing Engine of RFID Technology for Agricultural Products,» de *International Conference on Artificial Intelligence and Computational Intelligence (AICI '09), pp. 328-333*, Nov 2009.

[201] «Web oficial de drupal,» [En línea]. Available: http://www.drupal.org.

[202] J. Clark, «The importance of simulation techniques in its research and analysis,» de *Proceedings of the 29th conference on Winter simulation (WSC '97), pp. 1236-1243*, Savannah, GA, 1997.

[203] E. Mielants y H. Mielants, «The Importance of Simulation as a Mode of Analysis: Theoretical and Practical Implications and Considerations,» *Revue Belge d'Histoire Contemporaine,* vol. XXVII, nº 3-4, pp. 293-322, 1997.

[204] P. Levis, N. Lee, M. Welsh y D. Culler, «TOSSIM: accurate and scalable simulation of entire TinyOS applications,» de *Proceedings of the 1st international conference on Embedded networked sensor systems (SenSys '03), p. 126 - 137* , Los Angeles, Oct 2003.

[205] I. Downard, «Simulating Sensor Networks in NS-2,» Naval Research Laboratory, may 2004.

[206] A. Varga, «The OMNeT++ Discrete Event Simulation System,» de *Proceedings of the 15th European Simulation Multiconference (ESM'2001)*, Prague, june 2001.

[207] V. Gungor, D. Sahin, T. Kocak y S. Ergut, «Smart Grid Technologies: Communication Technologies and Standards,» *IEEE Transactions on Industrial Informatics,* vol. 4, nº 7, pp. 529 - 539, Nov 2011.

[208] E. Brezhnev y V. Kharchenko, «BBN-based approach for assessment of Smart Grid and nuclear power plant interaction,» de *East-West Design & Test Symposium, pp. 1-7*, Sept 2013.

[209] A. Sinha, M. Goswami, A. Lahiri y M. Debnath, «Mininizing the cost of generation for future Smart Grids,» de *2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT), pp. 87-92*, Nagercoil, India, March 2013.

[210] L. Vanfretti, D. V. Hertem, L. Nordstrom y J. Gjerde, «A smart transmission grid for Europe: Research challenges in developing grid enabling technologies,» de *IEEE Power and Energy Society General Meeting, pp. 1-8*, San Diego, CA, July 2011.

[211] Q. Ou, Y. Zhen, X. Li y Y. Zhang, «Application of Internet of Things in Smart Grid Power Transmission,» de *Third FTRA International Conference on Mobile Ubiquitous, and Intelligent Computing (MUSIC), pp.96-100*, Vancouver, BC, June 2012.

[212] J. DongLi, M. XiaoLi y S. XiaoHui, «Study on technology system of self-healing control in smart distribution grid,» de *International Conference on Advanced Power System Automation and Protection (APAP), pp. 26-30*, Beijing, Oct 2011.

[213] E. Bou-Harb, C. Fachkha, M. Pourzandi y M. Debbabi, «Communication security for smart grid distribution networks,» *IEEE Communications Magazine,* vol. 51, nº 1, pp. 42-49, Jan 2013.

[214] J. Naus, G. Spaargaren, B. v. Vliet y H. v. d. Horst, «Smart grids, information flows and emerging domestic energy practices,» *Energy Policy,* vol. 68, p. 436–446, May 2014.

[215] M. Vural y G. Kurt, «Effect of cooperative communications on power consumption in smart grid,» de *21st Signal Processing and Communications Applications Conference (SIU), pp. 1-4*, Haspolat, April 2013.

[216] «Ley 8/2011 del BOE,» [En línea]. Available: http://www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf.

[217] «Centro Nacional para la Protección de las Infraestructuras Críticas,» [En línea]. Available: http://www.cnpic-es.es/index.html.

[218] K. Kolowrocki y J. Soszynska-Budny, «Introduction to safety analysis of critical infrastructures,» de *International Conference on Quality, Reliability, Risk, Maintenance,*

and Safety Engineering (ICQR2MSE), pp. 1-6, June 2012.

[219] W. Chunlei, F. Lan y D. Yiqi, «National Critical Infrastructure Modeling and Analysis Based on Complex System Theory,» de *First International Conference on Instrumentation, Measurement, Computer, Communication and Control, pp. 832-836*, Oct 2011.

[220] S. Yasakethu, J. Jiang y A. Graziano, «Intelligent risk detection and analysis tools for critical infrastructure protection,» de *2013 IEEE EUROCON, pp. 52-59*, Zagreb, July 2013.

[221] R. Kozik y M. Choras, «Current cyber security threats and challenges in critical infrastructures protection,» de *Second International Conference on Informatics and Applications (ICIA), pp. 93-97*, Sept 2013.

[222] L. Coppolino, S. D'Antonio, L. Romano y G. Spagnuolo, «An Intrusion Detection System for Critical Information Infrastructures using Wireless Sensor Network technologies,» de *5th International Conference on Critical Infrastructure (CRIS), pp. 1-8*, Beijing, Sept 2010.

[223] E. Kyriakides y M. Polycarpou, Intelligent Monitoring, Control and Security of Critical Infrastructure Systems, Springer, Mar 2009.

[224] «Web del proyecto Bugyo Beyond,» [En línea]. Available: http://projects.celtic-initiative.org/bugyo-beyond/.

[225] M. M. Polycarpou, «Intelligent Monitoring, Control and Security of Critical Infrastructure Systems,» ICT COST Action IC0806, Mar 2009.

[226] S. Radack y R. Kuhn, «Managing Security: The Security Content Automation Protocol,» *IEEE. IT Professional,* vol. 13, nº 1, pp. 9-11, Feb 2011.

[227] «Web oficial de OpenSCAP,» [En línea]. Available: http://www.open-scap.org/page/Main_Page.

[228] N. Ziring y S. D. Quinn, «Specification for the Extensible Configuration Checklist Description Format (XCCDF),» NIST, 2008.

[229] J. Zhang, F.-Y. Wang, K. Wang, W.-H. Lin, X. Xu y C. Chen, «Data-Driven Intelligent Transportation Systems: A Survey,» *IEEE Transactions on Intelligent Transportation Systems,* vol. 12, nº 4, pp. 1624-1639, Jun 2011.

[230] A. Caragliu, C. Del Bo y P. Nijkamp, «Smart cities in Europe,» de *3rd Central European Conference in Regional Science (CERS)*, 2009.

[231] T. y. C. Ministerio de Industria, «Mapa tecnológico ciudades inteligentes,» Observatorio Tecnológico de la Energía, Apr 2012.

[232] R. Achaerandio, R. Bigliani, J. Curto y G. Gallotti, «Análisis de las Ciudades Inteligentes en

España 2012 – El Viaje a la Ciudad Inteligente,» IDC, Sep 2012.

[233] «Web de OSM,» [En línea]. Available: http://www.openstreetmap.org/.

[234] D. Krajzewicz, J. Erdmann, M. Behrisch y L. Bieker, «Recent Development and Applications of SUMO - Simulation of Urban MObility,» *International Journal on Advances in Systems and Measurements,* vol. 5, nº 3-4, pp. 128-138, 2012.

[235] «Maas de Race,» [En línea]. Available: mapas.race.es.

[236] «Servicio de cámaras de tráfico de la DGT,» [En línea]. Available: http://infocar.dgt.es/etraffic/.

10. Anexo 1. Glosario

10.1. Términos y acrónimos

WSN	Wireless Sensor Network
SWE	Sensor Web Enablement
OGC	Open Geospatial Consortium
IoT	Internet of Things
FASyS	Fábrica Absolutamente Segura y Sostenible
SGSI	Sistema de Gestión de la Seguridad de la Información
ITS	Intelligent Transport Systems,
TIC	Tecnologías de la Información y las comunicaciones
FoF	Factories of the Future
SO	Smart Object
UPnP	Universal Plug and Play
DLNA	Digital Living Network Alliance
DPWS	Devices Profile for Web Services
M2M	Machine to Machine
CoAP	Constrained Application Protocol
SDI	Spatial Data Infrastructures
SML	Sensor Model Language
O&M	Observation & Measurements
SOS	Sensor Observation Service
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
CC	Common Criteria
TI	Tecnología de la Información
SA	Security Assurance
CEP	Complex Event Processing
SCAP	Security Content Automation Protocol
XCCDF	Extensible Configuration Checklist Description Format
OVAL	Open Vulnerability and Assessment Language
PCS	Port Community System
IMT	Índice Medio de Tráfico
SO	Smart Objects