C. Alcaraz, R. Roman, P. Najera, and J. Lopez, "Acceso seguro a redes de sensores en SCADA a través de Internet", *XI Reunión Española sobre Criptología y Seguridad de la Información (RECSI 2010)*, pp. 337-342, 2010.
NICS Lab. Publications: `https://www.nics.uma.es/publications`

Acceso seguro a redes de sensores en SCADA a través de Internet

Cristina Alcaraz, Rodrigo Roman, Pablo Najera, Javier Lopez
Escuela Técnica Superior de Ingeniería Informática
Universidad de Málaga
Email: alcaraz, roman, najera, jlm@lcc.uma.es

***Resumen*—Las Infraestructuras Críticas (ICs) son monitorizadas por sistemas altamente complejos, conocidos como sistemas SCADA (Sistemas de Control y Adquisición de Datos), cuyo principal soporte se encuentra en las subestaciones, las cuales miden de primera instancia el estado real de tales ICs. Para mejorar este control, la industria está actualmente demandando la integración en el modelo tradicional de dos avances tecnológicos: Internet y las redes de sensores inalámbricas. Sin embargo, su incorporación requiere analizar los requisitos de seguridad que surgen en dicho contexto, así como diversos aspectos correlacionados (ej. mantenimiento, rendimiento, seguridad y optimización) y, en base a estos, la estrategia de integración más adecuada para satisfacer dichos requisitos. Este artículo proporciona dicho análisis en profundidad con el fin de ofrecer un modelo de integración seguro adecuado para entornos críticos.**

***Index Terms*—Sistemas Críticos de Control, Sistemas SCADA, Redes Mesh Inalámbrica de Sensores, el Internet, Internet of Things.**

I. Introducción

La introducción de nuevas tecnologías y diferentes tipos de sistemas de comunicación en las redes de control industriales está impulsando nuevos e importantes avances en los procesos de automatización y control. Un caso particular son los SCADA que emplean nuevas tecnologías para monitorizar en tiempo real muchas de las infraestructuras críticas (ICs) desplegadas en nuestra sociedad, tales como los sistemas de energía, de transporte o distribución de agua/aceite. Específicamente, en estos momentos dos de las tecnologías más demandadas son las redes inalámbricas e Internet. El primero, dado que proporciona los mismos servicios de control que una infraestructura cableada, pero con un bajo coste de instalación y mantenimiento. El segundo, al ofrecer conectividad global independientemente de la posición física de los dispositivos, tales como nodos sensores configurados en las subestaciones para controlar las infraestructuras críticas.

La imagen 1 muestra un sistema SCADA actual [1], donde los operadores autenticados y autorizados gestionan los flujos de datos transmitidos por las subestaciones. Una subestación remota se compone de dispositivos de campo, conocidos como Unidades Terminales Remotas (RTUs), capaces de recolectar, gestionar y transmitir los flujos de datos recibidos de sus sensores. Por otra parte, la imagen muestra también nuevas tecnologías adoptadas recientemente por las subestaciones, tales como redes de sensores inalámbricas (Wireless Sensor Networks o WSNs). Este tipo de red es una de las tecnologías

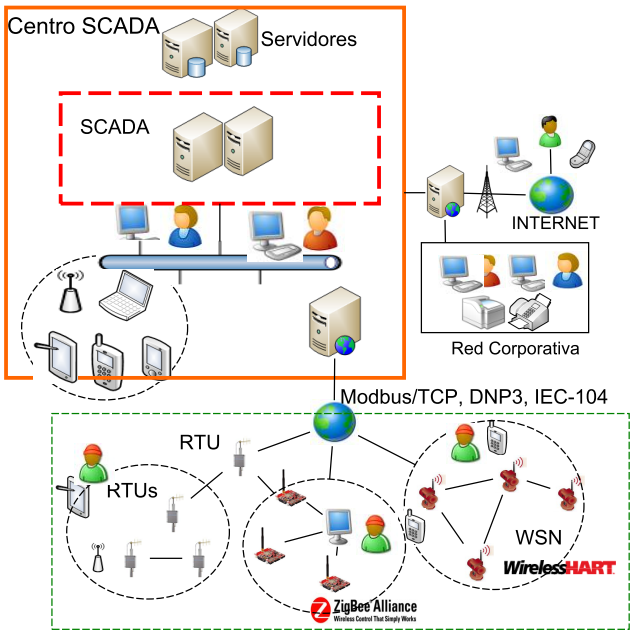

Figura 1. A current SCADA network architecture

más demandadas por los ingenieros industriales, dado que ofrece servicios de control similares a una RTU, pero con un bajo coste de instalación. Sin embargo, tales servicios no están siendo todavía explotados apropiadamente, dado que los estándares de comunicación únicamente contemplan conectividad local. Debido a esto, tanto la industria como la comunidad científica están tratando de maximizar esfuerzos para ofrecer tales servicios a través de Internet. Como resultado, un nuevo paradigma comienza a emerger en el contexto de las infraestructuras críticas, la Internet de los Objetos (IoT).

La IoT está formada de diversas infraestructuras heterogéneas de comunicación interconectadas, donde Internet, los servicios y objetos físicos juegan un importante rol en los procesos de control y automatización. El interés por abrir los procesos de comunicación en ICs a la red de redes y la inminente expansión de los nuevos paradigmas de comunicación ha motivado el desarrollo de diversos trabajos de investigación. Así, Li et. al propusieron en [2] un sistema basado en web para RTUs inteligentes con capacidad para

interpretar HTTP, Jain et. al presentó en [3] un sistema experto basado en web para diagnóstico y control de sistemas de energía e incluso algunas compañías comerciales tales como Yokogawa [4] o WebSCADA [5] están ya proporcionando soluciones de control utilizando Internet.

En particular, las WSNs, como parte de los objetos de la IoT, pueden crear una capa virtual, autónoma e inteligente sobre el entorno físico de subestaciones remotas, proporcionando información sobre el estado del mundo real que puede ser accedido en cualquier momento y lugar. De hecho, los gobiernos de alrededor del mundo han previsto el potencial de las WSNs en infraestructuras críticas y las han incluido en sus planes nacionales para investigación y desarrollo, tal como el gobierno australiano, a través de su Research Network for a Secure Australia (RNSA) [6], o el gobierno de los Estados Unidos en sus planes de protección para ICs [7],[8]. La comunidad científica e industrial está realizando diversas investigaciones para la adopción de las WSN en CIP. Por ejemplo, Bai et al. [9] ha implementado las WSN en un sistema SCADA para la monitorización de la energía generada por una planta de energía eólica. Carlsen et. al. introdujeron en [10] una WSN capaz de predecir la pérdida de aceite/gas en una planta submarina en el Mar del Norte.

La interacción de las WSN en las ICs a través de Internet se puede lograr empleando múltiples estrategias de integración: desde nodos sensores que implementen la pila TCP/IP y se conviertan en miembros completos de la IoT, a redes capilares que mantengan su independencia, pero empleen los servidores de Internet como interfaz hacia las entidades externas. Sin embargo, este camino presenta diferentes problemas que no han sido aún estudiados en profundidad en la literatura, tales como qué estrategia de integración debería emplearse en la integración de las WSN industriales en IoT, qué problemática de seguridad surgirá debido a esta evolución de la arquitectura de red y cómo asegurar que los requisitos de seguridad de los sistemas críticos se satisfacen en este paradigma de red. El objetivo de este artículo es proporcionar una base para la respuesta a estas cuestiones, analizando los requisitos de seguridad e infrastructurales de las WSN industriales conectadas a Internet y discutiendo la adecuación de las estrategias de integración que harán realidad la visión de gestión ubicua en el área de las redes industriales.

El artículo se organiza de la siguiente manera. La sección II describe los requisitos que deben ser considerados para alcanzar una integración segura. La sección III presenta las estrategias de integración susceptibles de ser adoptadas. La sección IV proporciona una análisis de la integración entre WSN e Internet en el contexto de las redes de control dados los requisitos mencionados previamente. La sección V concluye el artículo y muestra las líneas de trabajo futuro.

II. Requisitos de WSN industriales

Con objeto de proporcionar sus servicios, los sensores industriales inalámbricos podría beneficiarse sustancialmente de su integración en la IoT. La colaboración y agregación de datos críticos entre sensores geográficamente dispersos se vería mejorada, proporcionando información más fiable y precisa. Más allá, tanto los operadores de sistemas como los usuarios finales (con privilegios restringidos) podrían beneficiarse del acceso en tiempo real desde cualquier lugar a la infraestructura reduciendo costes. Sin embargo, a pesar de que es posible utilizar diferentes estrategias para conectar las WSNs a Internet, es necesario conocer cuál es más adecuada para los requisitos de cada escenario. El objetivo de esta sección es introducir tanto los requisitos específicos de las WSN industriales antes de presentar las diferentes estrategias de integración.

II-A. Requisitos de Control y Automatización

Para estudiar la seguridad de las WSN industriales en el contexto de Internet, es esencial considerar no sólo los requisitos de seguridad, sino también los requisitos que tales redes de control deben satisfacer, tales como mantenimiento, rendimiento del sistema y fiabilidad de los recursos y servicios. El motivo es simple: algunos de estos requisitos tienen una influencia directa sobre los requisitos de seguridad y viceversa, tales como la sobrecarga en memoria o tiempo de respuesta del nodo debido a los mecanismos de seguridad empleados. Debido a ello, esta subsección introduce los requisitos básicos (incluyendo los de seguridad) que deben considerar tanto sistemas de control como industriales .

II-A1. Mantenimiento: Es necesario realizar el mantenimiento del software y hardware de las subestaciones. Para prevenir la aparición de errores, cada dispositivo debe ser debidamente configurado, y deben realizarse tests periódicos de su estado. Además, los componentes software deben estar actualizados con las revisiones críticas, así como añadirse nuevo hardware a la subestación cuando éste es necesario. Por tanto, las propiedades asociadas al mantenimiento son:

- *Direccionamiento*. Es necesario especificar un tipo de identificación única para cada elemento presente en la subestación de forma que sea posible acceder al flujo de datos que éste produce. Esta propiedad se relaciona con cómo se accede a los diferentes identificadores de los dispositivos y quién se encarga de almacenar dichas identidades.
- *Acceso Interno*. Los servicios ofrecidos por los dispositivos que se encuentran en la subestación deben se accecidos de forma local por los operadores de las subestaciones, ya sea por motivos de testeo o de redundancia. Esta propiedad se relaciona con la complejidad actual de acceder a los dispositivos de la subestación de forma local.
- *Mantenibilidad*. Como con cualquier dispositivo, el software de las RTUs deberá ser actualizado debido a optimizaciones o parches de seguridad entre otros. Esta propiedad se refiere al número de dispositivos que deben cambiar con objeto de actualizar la funcionalidad de la subestación.
- *Extensibilidad*. El número de RTUs que puede encontrarse en una subestación concreta cambia a lo largo del tiempo de vida de la infraestructura. Esta propiedad se

relaciona con los cambios totales que deben realizarse en la subestación para incluir nuevo hardware.

II-A2. Fiabilidad: La funcionalidad proporcionada por la subestación debe ser suficientemente fiable para ofrecer sus servicios con unos niveles de calidad concretos. Los flujos de datos provistos por las RTUs deben estar disponibles en todo momento, y cualquier consulta relativa al contenido actual de dichos flujos de datos debe llegar al sistema central tan rápido como sea posible. Consecuentemente, las propiedad asociadas a la fiabilidad son:

- *Disponibilidad*[1]. Los datos producidos por las RTUs deben estar disponibles en todo momento con objeto de reaccionar a situaciones problemáticas y asegurar la integridad del sistema completo. Como propiedad, se dan dos dimensiones de la misma: la fiabilidad (empleando la redundancia del sistema para evitar los puntos únicos de fallo) y la seguridad (existencia de ataques de denegación de servicio y el empleo de mecanismos de sanado para proporcionar los servicios incluso en el caso de ataques/fallos en el sistema).
- *Rendimiento*. La información debe ser recuperada de las RTUs a velocidad suficiente. Como propiedad, el rendimiento se relaciona con las capacidades hardware de los dispositivos de la subestación, además de la velocidad actual de la infraestructura de la red de la subestación, y el número de saltos entre la RTU y el repositorio de datos.

II-A3. Sobrecarga: Es necesario lograr un balance entre el número de recursos disponibles al dispositivo y su coste global. Los dispositivos no deberían recibir una sobrecarga de trabajo, pero tampoco deberían de dedicarse recursos innecesarios. Más allá, aquellos recursos deberían optimizarase para funcionar en el entorno de la subestación. Consecuentemente, las propiedades asociadas con la sobrecarga son:

- *Recursos del Dispositivo*. Con objeto de implementar los diferentes protocolos que proporcionan la funcionalidad central de las subestaciones, tales como DNP3 o WirelessHART, los dispositivos deben usar parte de sus recursos HW y SW. Esta propiedad referencia la cantidad de recursos que se necesitan dentro de un nodo para implementar dichos protocolos.
- *Optimización*. Hay algunos protocolos específicos que se han optimizado para proporcionar la mejor funcionalidad posible en un entorno particular. Esta propiedad se relaciona con la existencia de protocolos específicos de red (tales como WirelessHART), que son conscientes de las características específicas del entorno de red y utilizarlos para proporcionar mejores servicios (por ej. redundancia de red y robustez del enlace).

II-A4. Seguridad: La seguridad de los diferentes procesos de una subestación es materia de máxima importancia. Cualquier problema que afecte a la integridad de los elementos de una subestación tendrá potencialmente una influencia sobre el mundo real, afectando no sólo a las infraestructuras físicas, sino a los seres humanos. Por lo tanto, sólo usuarios autorizados deben de disponer de privilegios para modificar el estado de los elementos de las subestaciones, y únicamente los usuarios fiables deben poder acceder a los flujos de datos producidos por las subestaciones. De manera adicional, deben existir mecanismos que almacenen las interaciones entre los diferentes elementos, para facilitar no sólo el análisis del comportamiento del sistema, sino también la detección de posibles brechas de seguridad. Por lo tanto, las propiedades asociadas a la seguridad son:

- *Canal Seguro*. Allá donde dos dispositivos que pertenezcan al mismo sistema SCADA (por ej. una máquina del sistema central y una RTU de una subestación)se comuniquen, es importante establecer un canal seguro que soporte servicios de integridad y confidencialidad extremo-a-extremo. La integridad del flujo de datos evitará la introducción de información falsa en el sistema. Además, la confidencialidad del flujo de información evitará el acceso de adversarios a información sensible. Como propiedad, referencia al tipo de máquinas y mecanismos que se ven envueltas en la creación de un canal de comunicación que soporte confidencialidad e integridad.
- *Autenticación*. En lo que se refiere a la autenticación de usuario, los dispositivos deben asegurarse de la identidad de un usuario que solicite una operación concreta. Como propiedad, la autenticación se refiere a la localización y la naturaleza de los mecanismos y elementos que pueden emplearse para proporcionar la identidad de un ser humano.
- *Autorización*. Una vez que cualquier usuario de la red (sea un humano o una máquina) proporciona su identidad, puede ser necesario comprobar si tal usuario tiene los derechos para acceder a la información. No sólo se debe controlar el acceso a la información, sino también la granularidad de la información. Es también necesario monitorizar las operaciones de control (por ej. los dispositivos deben ser sólo reprogramados por los usuarios autorizados). Como propiedad, la autorización referencia a los tipos de mecanismos, credenciales y herramientas que pueden emplearse para comprobar si una cierta entidad está autorizada a realizar una operación.
- *Registro y detección*. Es necesario mantener un registro de las interaciones de los heterogéneos usuarios que acceden a los servicios de una subestación. Tal registro permitirá recrear los incidentes de seguridad y las situaciones anormales. Además, podemos detectar ataques específicos en tiempo real. Como propiedad, el registro y la detección referencian a la estructura de los sistemas de registro y los mecanismos que pueden emplearse para analizarlos.

[1]La disponibilidad puede considerarse como un requisito de seguridad, pero ha sido clasificada como un requisito de fiabilidad debido a su relación cercana a la dimensión funcional de la subestación.

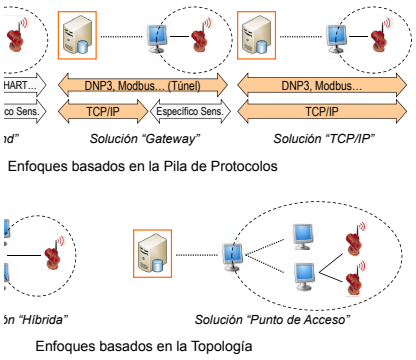

Figura 2. Estrategias de integración

III. Estrategias de Integración

Actualmente existen dos formas de integrar las WSNs industriales en Internet, las cuales van a depender de la (i) *pila de protocolo* o de la (ii) *topología* de la red. Para la primera clasificación, es necesario comprender las similitudes existentes entre ambas tecnologías, obteniéndose tres posibles soluciones/modelos (ver Figura 2): **Front-end** (la WSN es independiente del Internet), **Gateway** (intercambio de información a través de nodos especiales de Internet), y **TCP/IP** (los nodos implementan la pila TCP/IP). Para entrar en más detalle, comentaremos cada uno de estos casos. Por ejemplo, para una solución Front-end, tanto el centro SCADA como las WSNs en las subestaciones remotas no establecen comunicaciones directas, permitiendo a las WSNs tener implementada su propias pilas de protocolos (ZigBee, WirelessHART, ISA100.11.a). En este caso, las interacciones entre ambos extremos deben residir en una interfaz capaz de traducir los respectivos protocolos (ej. una RTU), facilitando la consulta y el control de las subestaciones.

En una solución Gateway, también se considera la existencia de un nodo especial capaz de actuar como un gateway a nivel de aplicación (ej. una RTU), con el fin de traducir los protocolos de las capas inferiores provenientes de ambas redes (ej. TCP/IP y Modbus), además de enrutar la información de un punto a otro (como hace el front-end), sin necesidad de conexión directa con el Internet y sin requerir que la propia pila de WSN cambie. Finalmente, en la solución TCP/IP, los nodos sensores ya forman parte del Internet, al tener implementado dentro de su lógica el estándar TCP/IP o un conjunto de protocolos compatibles (como 6LowPAN [11] en redes 802.15.4 [12]). Esta solución es precisamente la que podría integrar las WSNs industriales en el contexto de IoT (*Internet of Things*).

Por el contrario, en la segunda clasificación, el nivel de integración va a depender de la localización física de aquellos nodos responsables de proveer acceso a Internet, como pueden ser: (i) estaciones bases localizadas en la raíz de un diseño de WSN híbrida (solución **Híbrida**) o (ii) nodos backbone dedicados a proveer puntos de accesos a Internet en un salto (solución **Punto de Acceso**). Las WSNs del primer caso, se caracterizan por ofrecer redundancia cuya información debe pasar a través de ellas. Por el contrario, las redes diseñadas bajo una solución de Punto de Acceso presentan una topología de red en forma de árbol cuyas hojas corresponden a nodos sensores y el resto son considerados puntos de accesos a Internet. Ambas clasificaciones pueden funcionar conjuntamente, permitiendo que nodos backbones o estaciones bases, puedan funcionar como front-ends/gateways, favoreciendo los accesos directos entre los nodos y el centro SCADA. Sin embargo, combinar un modelo de red TCP/IP con soluciones Híbridas/Punto de Acceso puede no tener mucho sentido, al existir en los nodos sensores una vía de acceso directa hacia el Internet.

IV. Análisis de Mecanismos de Integración

Una vez conocidas las diferentes estrategias de integración, es necesario discutir las (des)/ventajas de cada una de ellas en un contexto industrial. Para ello, es necesario considerar las propiedades de la **Sección** II

1) ***Mantenimiento***: En términos de *direccionamiento*, tanto las soluciones Front-end como el Gateway requieren de una tarea de de traducción de identidades a una dirección de un nodo de la red, por lo que el nodo responsable (es decir, la RTU) deberá mantener una tabla de direcciones. En cambio, si la solución es TCP/IP, dicha tabla de direcciones debe ser localizada en el centro SCADA para transmitir directamente hacia el Internet. Luego, existen dos tipos de redes: **descentralizados** o **centralizados**. Obviamente, la gestión en una red centralizada, como una red Híbrida o de Punto de Acceso, será mucho más costosa que la descentralizada al requerirse una replicación de tablas de direcciones en las estaciones bases o backbones o una interfaz intermediaria que permita realizar las traducciones.

Por otro lado, e independientemente de la solución, los operadores tienen que llevar a cabo tareas de mantenimiento mediante conexiones TCP/IP (*acceso interno*) a la propia subestación, con el fin de acceder a los servicios de recuperación de datos. También cabe la posibilidad de que los operadores en campo puedan acceder directamente a servicios locales del propio protocolo de WSN (p. ej. ISA100.11a), tal como ocurre en soluciones Front-end y Gateway. En cambio, en modelos TCP/IP se requiere conocer de antemano la dirección de red del sensor. Por último, esta propiedad puede ser un poco más compleja en soluciones de Punto de Acceso, ya que se necesita que los operadores estén físicamente cercanos a los nodos que deseen acceder.

El *mantenimiento* SW de los nodos sensores va a depender del número de dispositivos a ser actualizados (nuevos servicios SCADA). En soluciones Front-end, el proceso afecta únicamente a un dispositivo de la red (la RTU), el cual requiera parar los procesos de control y la disponibilidad de la WSN momentáneamente con el fin de llevar a cabo las tareas de mantenimiento. En cambio, las soluciones Gateway

y TCP/IP ofrecen actualizaciones graduales en todos los nodos sensores implicados, asegurando continuidad y funcionalidad. Igualmente, la solución Híbrida es también capaz de ofrecer tales actualizaciones graduales al proveer redundancia de elementos, mientras que la solución de Punto de Acceso puede no ofrecerla, ya que los nodos están conectados de alguna forma a un determinado nodo backbone. En lo que respecta a la *extensibilidad*, tanto el Front-end como el Gateway requieren incluir una nueva entrada en la tabla de traducciones para hacer funcionar los servicios específicos de las WSNs, mientras que en soluciones TCP/IP son precisamente los nodos sensores los encargados de añadir nuevas entradas (de manera individual). Igualmente, esta propiedad también podría afectar a tanto soluciones Híbridas como de Punto de Acceso, excepto en el caso particular que dichas tablas sean gestionadas de manera distribuida.

3) ***Sobrecarga***: *Recursos de los dispositivos* están relacionados con todas aquellas soluciones (Híbrida, Punto de Acceso y TCP/IP) que requieran ciertas capacidades SW y HW en los nodos para implementar protocolos de aplicación y servicios de seguridad. Sin embargo, aunque los nodos sensores industriales aparentemente provean ciertas capacidades computacionales y recursos, estos siguen presentando ciertas complejidades (como los nodos convencionales). Con lo que respecta a la *optimización*, todos aquellos modelos (como el Front-end, Gateway, Híbrida y Punto de Acceso) que hacen uso de protocolos específicos de WSN (p. ej. WirelessHART o ISA100.11a), pueden beneficiarse de los servicios ofrecidos por ellos (p. ej. sincronización mediante una determinada TDMA, mecanismos de control de interferencias y coexistencia con otras tecnologías, mecanismos de diagnósticos, gestión de prioridades y gestión de rutas redundantes). La mayoría de estos servicios propios no están contemplados por la pila TCP/IP.

3) ***Seguridad***: Para conseguir un *canal seguro* se requiere mecanismos que aseguren confidencialidad e integridad en todas las comunicaciones, es decir, desde el centro SCADA hasta las WSNs. En el modelo TCP/IP es posible proveer tales servicios, ya que cada nodo final tiene implementado de alguna forma la pila TCP/IP. Incluso, aunque no sea posible hacer uso de las ventajas de IPSec debido a la naturaleza restrictiva de los sensores [13], es posible hacer uso de SSL/TLS implementados en la capa de transporte o WS-ConversacionSegura en la capa de aplicación para aquellas redes que hacen uso de servicios Web. Estos mismos mecanismos de aplicación podrían ser también viables en un modelo Gateway, ya que sus capacidades se centran en reenviar la información. Por el contrario, una solución Front-end necesita proteger el canal de dos formas: (i) con mecanismos de seguridad TCP/IP y (ii) con mecanismos de protección específicos de las WSNs (ej. claves simétricas de WirelessHART). Finalmente, es importante comentar que tanto el modelo Front-end como el Gateway permite implementar una red privada virtual (VPN) entre el centro SCADA y el front-end/gateway, asegurando la confidencialidad y la integridad de los mensajes de control.

Uno de los principales desafíos en lo que respecta a la *autentificación* es determinar la localización de los servicios de autentificación de usuario y el almacenamiento de las credenciales de seguridad, como usuario/contraseña. El modelo más simple es el Front-end, ya que es justo el nodo quién tiene que almacenarlos y gestionarlos. En cambio, estos servicios de seguridad son distribuidos en disversos puntos de la red en las demás soluciones. Una posible solución sería aplicar protocolos y mecanismos de seguridad de manera centralizada con el fin de gestionar en un mismo punto toda la información relativa a la autentificación (ej. Kerberos [14]). No obstante, estas soluciones podrían añadir ciertas complejidades a los nodos sensores al requerir el uso de servicios adicionales para validar las credenciales. Para evitar este hecho, una posible solución sería replicar las bases de datos de credenciales, con el problema añadido de que se podría dificultar los procesos de mantenimiento del sistema completo. Con respecto al modelo Gateway, una medida de seguridad sería configurar canales dedicados y seguros entre el usuario y el gateway justo después de realizarse un proceso de autentificación.

La propiedad de *autorización* es similar a la de autentificación, con la excepción de que es necesario conocer dónde almacenar los servicios asociados a la autorización y los permisos de usuarios. Por consiguiente, las mismas soluciones para la autentificación son efectivas para la autorización. Sin embargo, el uso de bases de datos distribuidas podría incluir una importante complejidad al sistema, ya que los permisos de usuarios tienden a cambiar con mayor frecuencia.

En cuanto al *registro*, es necesario almacenar todas las interacciones entre el sistema central y los nodos sensores. Una medida óptima sería diseñar un modelo de red totalmente centralizado, como podría ser un modelo Front-end y un Gateway, e incluso, si existe mecanismos de seguridad implementados punto a punto, la solución Gateway podría filtrar cierta información manteniendo dicha naturaleza centralizada. En cambio, un modelo descentralizado, como el TCP/IP, podría suponer ciertas complejidades de almacenamiento en los sensores, ya que serían ellos los que deberían registrar todas las interacciones ocurridas en el sistema. Igualmente, la *detección* debería implementarse en soluciones centralizadas, ya que supondría incrementar la inteligencia del nodo con nuevas reglas de detección, reduciendo sus capacidades lógicas para procesar otros tipos de tareas. Este mecanismo se hace prácticamente esencial para ayudar a detectar posibles malfuncionamientos y ataques internos, por lo que se recomienda seguir investigando en la elaboración de reglas y patrones sencillos (no complejos) para WSNs.

IV-A. Discusiones

Considerando los análisis realizados anteriormente, nuestro principal objetivo ahora es determinar la validez de tales estrategias en un contexto industrial. Por ejemplo, en una solución TCP/IP, las WSNs localizadas en subestaciones remotas son consideradas partes del Internet, pero sin embargo, este hecho podría no ser tan ventajoso. En términos de seguridad es necesario proteger la WSN desde cualquier tipo de intruso, ya que un incremento en el tráfico de red podría suponer una

reducción de funcionalidad en los nodos sensores debido a sus limitadas capacidades. La autenticación y la autorización pueden ser resueltas, en un principio, mediante soluciones centralizadas como kerberos. Por otro lado, los nodos que tienen implementado la pila TCP/IP y no tienen suficientes recursos para implementar protocolos específicos WSNs (WirelessHART o ISA100.11a), no llegan a beneficiarse de los servicios de optimización ofrecidos por éstos, e incluso, no pueden implementar mecanismos de almacenamiento y reenvío para ganar redundancia de datos, así como la gestión de datos en caché. No obstante, este modelo podría ofrecer ciertas ventajas en lo que respecta el mantenimiento SW gradual y resistencia a fallos, sin aislar la funcionalidad total del sistema/subsistema.

Por otro lado, los nodos sensores de un modelo Front-end pueden hacer uso de los estándares existentes para implementar mecanismos de seguridad cuya funcionalidad reside en un único punto. Sin embargo, este hecho podría suponer riesgos de aislamiento al tratarse de un punto vulnerable a ataques de denegación de servicios. Una posible solución sería implementar un modelo de red Híbrida o Punto de Acceso, aunque ésto podría suponer nuevos problemas asociados a la replicación de recursos. Otra ventaja de usar Front-end es el uso de servicios óptimos ofrecidos por los estándares específicos de WSNs y la posibilidad de configurar mecanismos de seguridad que ayuden a mejorar la resistencia (p. ej. rutas redundantes). Por último, aunque el mantenimiento SW de la red es simple (actualización en un nodo), existe el riesgo de aislar la funcionalidad de la red durante un periodo de tiempo crucial. Para ello, se recomienda replicar nodos, tal como hace los modelos Híbridos y Punto de Acceso.

En lo que respecta al modelo Gateway, éste puede ser considerado una mezcla entre las dos primeros. En particular, ésta ofrece algunas implementaciones dadas por el Front-end, como puede ser el uso de servicios óptimos específicos de WSN e implementaciones de almacenamiento y reenvío, permitiendo a su vez realizar consultas directas al centro SCADA. No obstante, la funcionalidad del Gateway podría añadir complejidades a los nodos, además de considerar detalles de seguridad como la autentificación y la autorización. Además, el gateway debería filtrar las entradas para analizar las consultas y evitar ataques específicos de aplicación y considerar aspectos como la complejidad añadida en los procesos de mantenimiento SW. Por último, esta solución puede ser combinada con modelos de red Híbridas y de Punto de Acceso para configurar redundancia, aunque es también esencial considerar los problemas relativos a estos modelos, como pueden ser la distribución de tablas y recursos.

Por consiguiente, *parece interesante usar una solución puramente TCP/IP en subestaciones remotas, sin embargo, esta solución podría no ser suficiente para una integración total de WSNs en Internet bajo un contexto industrial*. Además, como los sistemas de control simplemente acceden a flujos de datos y realizan tareas de control bajo comandos, otras soluciones, como el Front-end combinadas con modelos que provean redundancia, podrían ser a priori suficientes para las necesidades actuales de la industria. No obstante, es importante comentar que una integración segura y completa de una WSN en el Internet podría brindar al sistema con nuevos e interesantes mecanismos de control, algunos de los cuales harían uso de servicios Web.

V. Conclusion

Desde que los nodos sensores son parte del IoT e Internet de la Energía, nuevos desafíos de investigación están comenzado a emerger, los cuales están resumidos en este artículo bajo un análisis de integración (segura) de nodos sensores en Internet bajo un contexto industrial. Como conclusión de este análisis vemos que actualmente no es necesario integrar totalmente las redes de sensores industriales dentro de Internet y que una simple red basada en redundancia podría ser, por ahora, suficiente para ofrecer la funcionalidad deseada. Sin embargo, queda pendiente para un futuro investigar cómo explotar el potencial y funcionalidad ofrecido por Internet junto al uso de nodos sensores industriales para así garantizar nuevas e interesantes aplicaciones de control.

Agradecimientos

Este trabajo ha sido parcialmente financiado por ARES (CSD2007-00004), PROTECT-IC (TSI-020302-2009-10) y SPRINT (TIN2009-09237), siendo este último co-financiado por FEDER.

Referencias

[1] C. Alcaraz, G. Fernandez, R. Roman, A. Balastegui, J. Lopez. *Secure Management of SCADA Networks*. New Trends in Network Management, CEPIS, vol. IX, no. 6, 2008, pp.22–28.

[2] D. Li, Y. Serizawa and M. Kiuchi, *Concept design for a Web-based supervisory control and data-acquisition (SCADA) system*, Transmission and Distribution Conference and Exhibition, Asia Pacific. IEEE/PES , vol. 1 , pp. 32-36, 2002.

[3] M. Jain, A. Jain and M. Srinivas, *A web based expert system shell for fault diagnosis and control of power system equipment*, Condition Monitoring and Diagnosis, pp.1310-1313, ISBN: 978-1-4244-1621-9, 2008.

[4] Yokogawa, http://yokogawa.com/scd/fasttools/scd-scada-websuper-en.htm, accessed on Aplil, 2010.

[5] WebSCADA, http://www.webscada.com/, accessed on April, 2010.

[6] D. Bopping, *CIIP in Australia*, 1st CI2RCO Critical Information Infrastructure Protection conference, Rome, 2006.

[7] The Department of Homeland Security, Science and Technology Directorate, *The National Plan for Research and Development in Support of Critical Infrastructure Protection*, Washington, D.C., 2005.

[8] The Department of Homeland Security, *National Infrastructure Protection Plan Partnering to enhace protection and resilence*, 2009.

[9] X. Bai, X. Meng, Z. Du, M. Gong and Z. Hu, *Design of Wireless Sensor Network in SCADA system for wind power plant*. Automation and Logistics (ICAL), pp. 3023-3027, 2008.

[10] S. Carlsen, A. Skavhaug, S. Petersen and P. Doyle, *Using wireless sensor networks to enable increased oil recovery*, IEEE International Conference on Emerging Technologies and Factory Automation, pp. 1039-1048, 2008.

[11] G. Montenegro, N. Kushalnagar, J. Hui and D. Culler, "RFC 4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks", 2007.

[12] IEEE Standard, 802.15.4-2006, "Wireless medium access control and physical layer specifications for low-rate wireless personal area networks", 2006.

[13] N. Kushalnagar, G. Montenegro and C. Schumacher, "RFC 4919: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", 2007.

[14] C. Neuman, T. Yu, S. Hartman, and K. Raeburn, "RFC 4129: The Kerberos Network Authentication Service (V5)", Request for Comments, 2005.