Implementación de un sistema de seguridad en medidores inteligentes (Smart Grids)*

Implementation of a Security System for Smart Meters (Smart Grids)

Recibido: 10 de agosto de 2014- Aprobado: 17 de septiembre de 2014

Para citar este artículo: C. Camargo, J. Sáenz, N. Rosas, « Implementación de un sistema de seguridad en medidores inteligentes (Smart Grids) », *Ingenium*, vol. 15, n.° 30, pp. 28-38, octubre, 2014.

Carlos Camargo**
Javier Sáenz***
Nelson Rosas****

Resumen

La Integración de la red eléctrica y las tecnologías de la información y las comunicaciones (TIC) es el futuro de la energía, el mundo moderno no puede ser concebido sin electricidad y la infraestructura actual está mal adaptada a las necesidades actuales, cada día la demanda de energía es mayor y el medio ambiente sufre debido a la generación de CO2, necesitamos una red inteligente con mejor administración de la energía; implementando estas tecnologías se esperan reducir significativamente los

* Artículo de investigación, producto derivado del proyecto realizado en el Grupo de Microelectrónica de la Universidad Nacional (GMUN), de una investigación en curso. El proyecto de investigación es la tesis de maestría titulada: Implementación de un sistema de seguridad para medidores inteligentes (Smart Grids), la cual se inició en enero del 2013, esta tesis está enmarcada dentro del proyecto de extensión «Desarrollo e implementación de un Smart Grid en el Campus de la Universidad Nacional» liderado por el ingeniero Carlos Iván Camargo, desde el Departamento de Ingeniería Eléctrica y Electrónica, el cual consiste en un sistema de medición inteligente que permite monitorear diferentes nodos del sistema de distribución eléctrica. Dentro de los objetivos de este proyecto está el uso de la infraestructura de la Universidad Nacional de Colombia para convertirla en un laboratorio que permita el estudio de arquitecturas, protocolos de comunicación y aplicaciones de Smart Grids.

** Ingeniero Electricista, Universidad Nacional de Colombia, Bogotá - Colombia, Magíster en Ingeniería Eléctrica, Universidad de los Andes, Bogotá - Colombia. Doctor en Ingeniería Eléctrica, Universidad Nacional de Colombia, Bogotá - Colombia. Profesor Asociado, Universidad Nacional de Colombia, sede Bogotá, Facultad de Ingeniería, Departamento de Ingeniería Eléctrica y Electrónica. Grupo de Investigación en Microelectrónica (GMUN). E-mail: cicamargoba@unal.edu.co.

*** Ingeniero Electrónico, Universidad Nacional de Colombia, Bogotá - Colombia, Estudiante de Maestría en Ingeniería de Telecomunicaciones, Universidad Nacional de Colombia, Bogotá, Grupo de Investigación en Microelectrónica(GMUN). E-mail: jasaenz@unal.edu.co.

**** Ingeniero Electrónico, Universidad Nacional de Colombia, Bogotá - Colombia, Magíster en Ingeniería de Telecomunicaciones, Universidad Nacional de Colombia, Bogotá - Colombia. Profesor Asociado, Universidad de San Buenaventura, Bogotá, Facultad de Ingeniería, Director de Ingeniería Electrónica y de Ingeniería de Telecomunicaciones. Grupo de Investigación en Microelectrónica (GMUN). E-mail:nfrosasj@unal.edu.co.

tiempos de lectura en las mediciones, los reportes de fallas y los cambios en la red. En países en desarrollo como Colombia podrán proveer servicios adicionales que ayuden a detectar el robo de energía.

Este artículo presenta una propuesta de implementación para la seguridad en las comunicaciones en medidores inteligentes, aplicando hardware y software libre.

Palabras clave

Red Inteligente, HAN, NAN, AMI, OpenVPN, PKI, SSL, Nagios.

Abstract

The integration of the energy grid and the information communication technologies (ICT) is the future of the energy, the modern world cant be conceived without electricity, and the current infrastructure of the electric grid is ill suited for the actual needs, every day the demand for energy is bigger and the environment is suffering this because the CO2 generation, we need an smarter grid with better energy management. By implementing these technologies are expected to significantly reduce reading times of measurement, the reporting of failures and changes in the grid. In developing countries like Colombia these technologies can provide additional services that help to detect energy theft.

This paper presents an implementation proposal for communications security in smart meters, by applying free hardware and free software.

Keywords

Smart Grid, HAN, NAN, AMI, OpenVPN, PKI, SSL, Nagios.

1. INTRODUCCIÓN

La electricidad es uno de los recursos energéticos fundamentales para el desarrollo de la sociedad [1]. Gran parte de la tecnología funciona con energía eléctrica y por tanto es necesaria para el desarrollo de la civilización. La infraestructura actual se ha mantenido sin cambios significativos en las últimas décadas[2] y debido a esto, hoy en día la red de distribución es muy compleja y poco adaptada a las necesidades del siglo XXI; como consecuencia en Colombia se han presentado apagones masivos como el de abril de 2007 en donde cerca del 98 % de los colombianos se quedaron sin servicio[3], el de diciembre de 2006 que dejó sin servicio parte de los departamentos de Santander y Norte de Santander y una gran parte de la ciudad de Bogotá[4].

Es importante resaltar que los proveedores del servicio desconocen las causas de los apagones de manera inmediata y es necesario realizar labores de investigación para poder llegar al origen de los problemas, pero estas investigaciones en algunos casos no llegan a ninguna conclusión como se puede observar en fig. 1 y fig. 2.

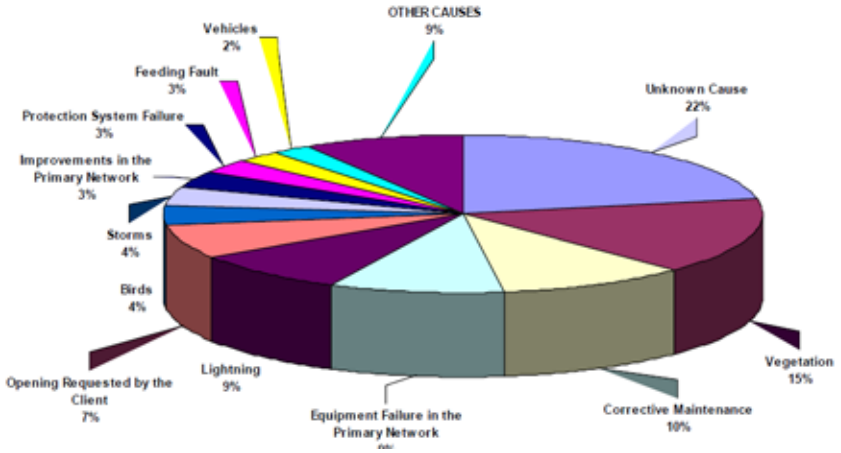

Figura 1. Confiabilidad y calidad del servicio ejemplo fallas por frecuencia (tomado de [5])

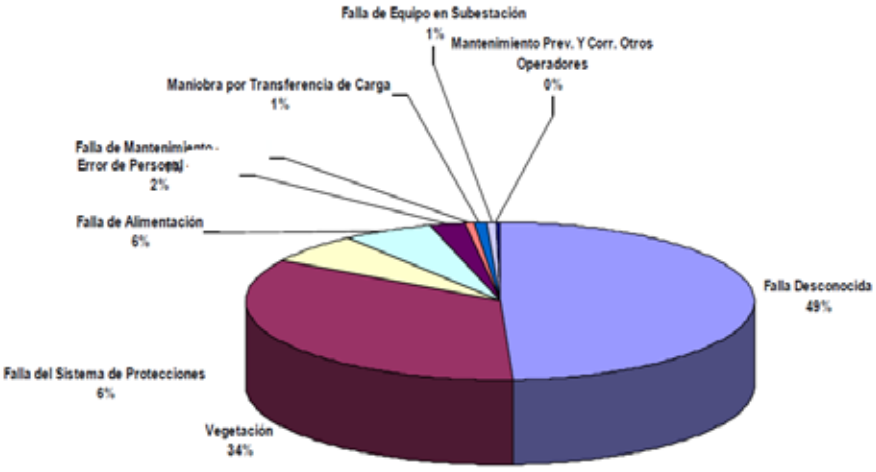

Figura 2. Confiabilidad y calidad del servicio ejemplo fallas por duración (tomado de [5])

Los problemas normalmente se deben a la baja velocidad de respuesta de los interruptores mecánicos, falta de análisis automático, y la poca visibilidad que tienen los operadores acerca del estado de la red [6] [7].

En este momento, la mayor parte de la energía que el mundo desarrollado consume es producida a partir de combustibles fósiles [8], lo cual no es sostenible, además un buen porcentaje se desperdicia durante el proceso de entrega y distribución [1].

Las necesidades mundiales crecientes de generación de energía alternativa plantean nuevos retos como la integración de fuentes renovables a la red eléctrica, almacenamiento y estabilidad del sistema [9] [10]. Las redes inteligentes son una tecnología emergente que tiene como objetivo mejorar la eficiencia, la confiabilidad y seguridad de la red con beneficios adicionales como la integración de vehículos eléctricos, gestión de la demanda a través del control automático y la información y tecnologías de la comunicación [7].

De acuerdo con la Unión Internacional de las Telecomunicaciones (UIT)[1] y con el Instituto Nacional de Estandarización y Tecnología (NIST)[2] , los requisitos de las redes inteligentes se han clasificado en un modelo de tres áreas: servicios y aplicaciones en redes inteligentes, área de comunicaciones y el área de equipo físico, y siete dominios: mercado, clientes, proveedores de servicios, operaciones, generación, transmisión y distribución [11] [12].

La red inteligente es una red de muchos sistemas y subsistemas, es decir, sistemas con varios propietarios están interconectados para proporcionar servicios de extremo a extremo entre las partes interesadas, así como entre dispositivos inteligentes [13] [14].

II. REQUERIMIENTOS DEL ÁREA DE COMUNICACIONES

Debido a que las redes inteligentes incluyen redes de diversas tecnologías de la información, telecomunicaciones y sectores de la energía, es necesario garantizar que un fallo de seguridad en una red no compromete otros sistemas interconectados. Al comprometerse la seguridad en una parte de la red podría afectar la disponibilidad y confiabilidad de la red eléctrica completa. Además, la información dentro de cada sistema específico también necesita ser protegida [12].

La seguridad incluye la confidencialidad, integridad y disponibilidad en todos los sistemas relacionados. Los dispositivos y aplicaciones de cada dominio son los puntos extremos de la red. Ejemplos de aplicaciones y dispositivos en el dominio del cliente incluyen medidores inteligentes, electrodomésticos, termostatos, almacenamiento de energía, vehículos eléctricos, y la generación distribuida [12] Los requisitos adicionales de la red incluyen:

- Capacidad de transporte sobre IP (IPv4 e IPv6)
- Capacidad para transportar la gran cantidad de datos generados por los medidores inteligentes y sensores inteligentes en la red inteligente.
- Funcionalidad de gestión de la red, actividades de la red y dispositivos de red, incluyendo la monitorización del estado, la detección de fallas, el aislamiento y la recuperación.
- Capacidad para identificar y direccionar los elementos de la red y dispositivos conectados.
- Capacidad de enrutamiento a todos los puntos de red.
- Soporte de la calidad de servicio para una amplia gama de aplicaciones con diferentes anchos de banda y latencia y requisitos de pérdidas.
- Estandarización y reglamentación.

1 Unión Internacional de Telecomunicaciones (UIT) - www.itu.int

2 Instituto Nacional de Estandarización y Tecnología - www.nist.gov

A. Redes Basadas en IP

Existe una gran expectativa en cuanto al uso de este protocolo en las comunicaciones de las redes inteligentes debido a que es un protocolo ampliamente conocido, las redes basadas en IP debido a su diseño son fácilmente escalables y como prueba de esto tenemos la Internet, los nuevos dispositivos de redes inteligentes, como medidores inteligentes, electrodomésticos inteligentes para el hogar y los concentradores de datos en los barrios, se podrían agregar a la red. El hecho de que las direcciones IPv4 se han agotado debe ser considerado cuidadosamente [15]. IPv6 ha sido desarrollado específicamente para resolver el problema de espacio de direcciones y proporcionar mejoras para la red IP [16] [17].

III. INFRAESTRUCTURA DE COMUNICACIONES

Tres funcionalidades fundamentales son deseables para la infraestructura de comunicaciones de la red inteligente: detección, transmisión y control [18], en donde, muchas de las tecnologías actualmente usadas para otras aplicaciones como redes inalámbricas, protocolos de seguridad, redes de sensores, etc. serán adaptadas a las redes inteligentes, esto tiene grandes ventajas pues son tecnologías que ya han sido probadas en otras áreas industriales [14].

La red inteligente se concibe normalmente en un ámbito geográfico de dimensiones considerables. Por lo tanto, la infraestructura de comunicaciones de la red inteligente tiene que cubrir toda la región con la intención de conectar un gran conjunto de nodos [19]. En consecuencia, la infraestructura de comunicaciones está prevista para ser una estructura multicapa que se extiende a través de toda la red inteligente desde la red de área para el hogar (HAN) a la red de área de vecindario hasta la red de área extendida (WAN) (fig. 3). En particular, las HAN se comunican con diversos dispositivos inteligentes para ofrecer gestión de la eficiencia energética y respuesta a la demanda. NANs conectan diversas HANs a puntos de acceso locales. WAN provee enlaces de comunicación entre los NANs y los sistemas de servicios públicos para transferir información [18].

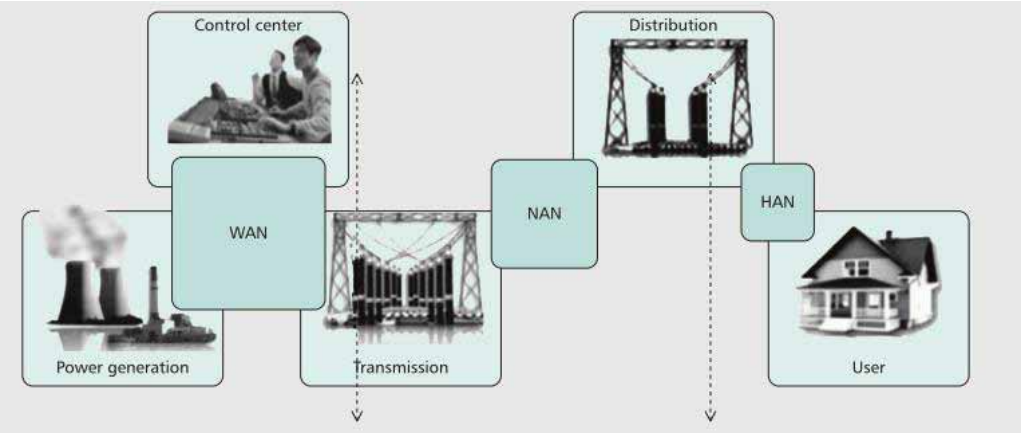

Figura 3 Infraestructura jerárquica de comunicaciones [18].

A. Infraestructura avanzada de medición (AMI)

Un medidor inteligente es un dispositivo que mide y registra variables como electricidad, gas, agua, presión, o calor, que permite comunicación bidireccional para transmitir información, infraestructura de medición avanzada (AMI) es un sistema que mide, recopila y analiza el uso de la energía, y se comunica con los medidores inteligentes para fines de seguimiento y facturación[20].

AMI es un elemento clave en las redes inteligentes, ya que proporciona información exacta en tiempo real a los consumidores informando la cantidad de energía que están utilizando para que puedan controlar su consumo. La industria de la energía tiene gran expectativa en esto debido a que tiene grandes ventajas en la precisión y la mejora de los procesos de lectura y control de los medidores en línea; sin embargo, los beneficios de AMI se ven contrarrestados por la necesidad de implementar sistemas de seguridad cibernética [21].

IV. METODOLOGÍA

Para el desarrollo del proyecto de investigación se abordaron los objetivos de forma secuencial, primero seleccionando la tecnología de telecomunicaciones, luego se determinaron las necesidades de protección con el fin de definir el sistema de seguridad que garantice minimizar los riesgos identificados y por último se implementó el sistema de seguridad en los prototipos anteriormente mencionados, de acuerdo con la metodología CDIO[3] con la cual se han hecho estos desarrollos [24].

V. PROPUESTA DE ARQUITECTURA DE SEGURIDAD - AMI

En esta sección se muestra la propuesta de una arquitectura de seguridad con el fin de cumplir con los requerimientos enunciados anteriormente, es importante mencionar que esta propuesta está enmarcada dentro de la metodología CDIO por tanto se espera que el sistema no sea tan solo una propuesta estrictamente académica sino que trascienda a la operación del mismo. La figura 4 muestra una visión general del sistema entre la red HAN y la red AMI. Hay tres componentes claves: un sistema cabecera, un medidor inteligente y un dispositivo HAN.

El sistema de cabecera se encarga de reunir la información de los sensores inteligentes con fines de monitorización y facturación.

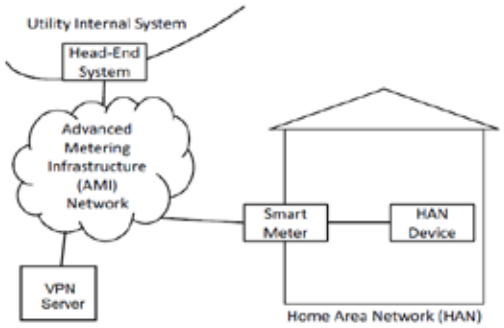

Figura 4. Visión general del sistema entre la red HAN y la red AMI [22].

3 www.cdio.org

A. Descripción general

La arquitectura propuesta debe realizar verificación sobre la legitimidad del medidor, es decir que el medidor debe estar autenticado para poder unirse a la red, de esta manera se puede evitar el problema de suplantación, una vez autenticado la trasmisión de datos debe ser cifrada, con el fin de garantizar la confidencialidad de la información, y por último debe estar en capacidad de realizar funciones de monitorización.

Actualmente en la Universidad Nacional de Colombia desde el Grupo de Investigación en Microelectrónica (GMUN) se está llevando a cabo el proyecto de extensión Desarrollo e Implementación de un Smart Grid en el Campus de la Universidad Nacional. El cual consiste en un sistema de medición inteligente que permite monitorizar diferentes nodos del sistema de distribución eléctrica. Dentro de los objetivos de este proyecto está el uso de la infraestructura de la Universidad Nacional de Colombia para convertirla en un laboratorio que permita el estudio de arquitecturas, protocolos de comunicación y aplicaciones de Smart Grids.

Actualmente se han elaborado prototipos en los cuales se utilizaron herramientas de software y hardware libre (figura. 5 y figura. 6); su objetivo principal es procesar y entregar información relacionada con el consumo energético y calidad de energía para el uso en Smart Grids; estos prototipos cumplen con las normas técnicas IEC 61000 4-7 y 4-30 y de la Comisión de Regulación de Energía y Gas (CREG). Uno de los objetivos es el uso de herramientas de software libre con el fin de no incurrir en costos de licenciamiento y de poder modificar la solución según sea necesario sin tener limitaciones legales [24].

Figura 5. Sistema de medición de energía utilizando el ASIC MAXQ3183 [24]

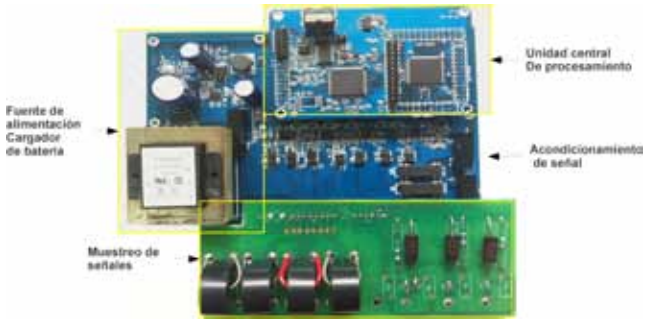

Figura 6. Sistema de medición de energía utilizando la arquitectura de tratamiento de señales discretas [24]

Para la implementación de estos prototipos se utilizó la plataforma de desarrollo de hardware copyleft STAMP como unidad de procesamiento y de comunicaciones, esta tarjeta tiene embebido un sistema operativo Linux; gracias al soporte que tiene Linux para los protocolos de red existentes y para la configuración de las redes inalámbricas es posible utilizar diferentes tecnologías de telecomunicaciones.

Para la implementación del sistema de autenticación y cifrado de los datos se va hacer uso del software OpenVPN[4] el cual además de proveer la autenticación y cifrado de los datos nos permite implementar infraestructura de llave pública (PKI), la cual nos brinda una mayor seguridad.

En cuanto a las funciones de monitorización se va a implementar Nagios[5] el cual se puede configurar fácilmente de acuerdo a las necesidades del sistema.

B. OpenVPN

OpenVPN es una solución de conectividad basada en software libre: SSL (Secure Sockets Layer) VPN Virtual Private Network (red virtual privada), OpenVPN ofrece conectividad punto a punto con validación jerárquica de usuarios y host conectados remotamente. Está publicado bajo la licencia GPL, de software libre.

La tecnología PKI permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad (por ejemplo, las claves públicas de otros usuarios) para cifrar y descifrar mensajes, firmar digitalmente información, garantizar el no repudio de un envío, y otros usos. En una operación criptográfica que use PKI, intervienen conceptualmente como mínimo las siguientes partes:

- Un usuario iniciador de la operación.
- Unos sistemas servidores que dan fe de la ocurrencia de la operación y garantizan la validez de los certificados implicados en la operación (autoridad de certificación, autoridad de registro y sistema de sellado de tiempo).
- Un destinatario de los datos cifrados/firmados/enviados garantizados por parte del usuario iniciador de la operación (puede ser él mismo).

Las operaciones criptográficas de clave pública, son procesos en los que se utilizan unos algoritmos de cifrado que son conocidos y están accesibles para todos. Por este motivo la seguridad que puede aportar la tecnología PKI, está fuertemente ligada a la privacidad de la llamada clave privada y los procedimientos operacionales o políticas de seguridad aplicados.

4 https://openvpn.net/

5 http://www.nagios.org/

Para esto se deben generar certificados públicos y privados y debe existir una entidad certificadora la cual verifica la autenticidad de estos certificados y permite el ingreso o no de los nodos a la red.

C. Nagios

Nagios es un sistema de monitorización de redes de código abierto ampliamente utilizado, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado. Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugins específicos para nuevos sistemas.

Se trata de un software que proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables correspondientes mediante (entre otros medios) correo electrónico y mensajes SMS, cuando estos parámetros exceden de los márgenes definidos por el administrador de red.

VI. IMPLEMENTACIÓN

Como sistema operativo se escogió Buildroot[6] el cual está diseñado para uso con sistemas embebidos y nos permite compilar solo los paquetes necesarios sin necesidad de agregar paquetes que no sean necesarios al sistema operativo, también se estudió la posibilidad de usar otra distribución como Openwrt[7], Debian[8], entre otros pero el más adecuado es buildroot, además porque en este se habían implementado los medidores previamente mencionados. El sistema hace uso de una red inalámbrica con seguridad WPA2, la cual ofrece mejor seguridad que los estándares WPA y WEP. La configuración del servidor OpenVPN se realizó en un sistema operativo Fedora[9], se utilizó cifrado SSL de 2048 bits mediante OpenSSL[10], durante el desarrollo de esta investigación se divulgó un serio problema de seguridad en OpenSSL, este bug se conoce como Heartbleed y fue necesario corregirlo mediante la aplicación de un parche en el código fuente y después con la actualización correspondiente tanto en el servidor como en el sistema embebido en la STAMP, también se configuró un servidor de monitorización con Nagios, en el cual se registra la disponibilidad de la tarjeta el sistema revisa si la tarjeta está o no conectada a la VPN mediante el uso del comando ping, además monitoriza si el servicio SSH está activo en caso de ser necesario un acceso remoto al medidor.

6 http://buildroot.uclibc.org/

7 https://openwrt.org/

8 www.debian.org/ports/arm/

9 fedoraproject.org/

10 www.openssl.org/

Uno de los factores más importantes fue el uso del firewall de Linux «iptables» con el cual se permitió acceso solo por el puerto asignado a la VPN. De esta manera se pueden rechazar todas las conexiones al sistema a excepción de las que están autenticadas en la VPN y se les han asignado permisos suficientes.

Finalmente se establecieron políticas de seguridad de administración del sistema teniendo en cuenta parámetros como caducidad de los certificados, complejidad de las contraseñas de acceso al sistema, número de reintentos y tiempos de espera en caso de intentos de autenticación fallidos con el fin de realizar una correcta administración del sistema.

VII. CONCLUSIONES

- Las plataformas de desarrollo hardware libre brindan grandes ventajas economizando tiempo y dinero en el desarrollo de productos.
- Al implementar como sistema operativo Linux tenemos una amplia gama de aplicaciones que podemos utilizar, sin incurrir en costos adicionales de licenciamiento
- Al utilizar OpenVPN como sistema para implementar la VPN obtenemos una gran flexibilidad y fácil configuración de la misma; permite además tener una gestión sencilla sobre los certificados y los permisos de los clientes VPN.
- Las políticas de seguridad son unas de las herramientas más importantes para un administrador de infraestructura pues garantiza el buen funcionamiento del sistema implementado.
- Es necesario hacer un seguimiento a las políticas de seguridad con el fin de mejorar constantemente el sistema, esta labor debe ser realizada periódicamente por el personal encargado de administrar el sistema.

VIII. REFERENCIAS

[1] K.-C. Chen, P.-C. Yeh, H.-y. Hsieh, and S.-C|. Chang, "Communication Infrastructure of Smart Grid," in 2010 4th International Symposium on Communications, Control and Signal Processing (ISCCSP), n.º March, 2010, pp. 3-5.

[2] V. C. Güngör, D. Sahin, T. Kocak, S. Ergüt, C. Buccella, S. Member, C. Cecati, and G. P. Hancke, "Smart Grid Technologies: Communication Technologies and Standards," IEEE Transactions on Industrial Informatics, vol. 7, n.º 4, pp. 529-539, 2011.

[3] *El Tiempo*, "Error humano habría causado apagón de este jueves en Colombia" 2007. [Online]. Available: www.eltiempo.com/archivo/documento/CMS-3531953

[4] *El Tiempo*, "Se restableció el servicio de energía suspendido por una falla en el sistema de generación", 2006. [Online]. Available: www.eltiempo.com/archivo/documento/CMS-3353763

[5] C. Inteligente, "Seminario en redes inteligentes, redes inteligentes para un futuro sostenible (II)". [Online]. Available: www.rcgsas.com/Documentos/Seminario/SRI-UN s02.pdf.

[6] A. Aggarwal, S. Kunta, and K. Pramode, "A Proposed Communications Infrastructure for the Smart Grid," in Innovative Smart Grid Technologies (ISGT), 2010, pp. 1-5.

[7] V. C. Güngör, B. Lu, and G. P. Hancke, "Opportunities and Challenges of Wireless Sensor Networks in Smart Grid," Industrial Electronics, IEEE Transactions on, vol. 57, n.º 10, pp. 3557-3564, 2010.

[8] R. Céspedes, E. Parra, A. Aldana, and C. Torres, "Evolution of Power to Smart Energy Systems", in 2010 IEEE/PES Transmission and Distribution Conference and Exposition: Latin America (T&D-LA). IEEE, Nov. 2010, pp. 616-621. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5762946

[9] D. J. Mackay, Sustainable Energy without the hot air, 2009.

[10] B. Unhelkar, Handbook of Research on Green ICT: Technology, Business and Social, 2011.

[11] INTERNATIONAL TELECOMMUNICATION UNION, "Deliverable on Requirements of communication for smart grid," pp. 1-81, 2011.

[12] National Institute of Standards and Technologies, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, 2010, vol. Publication.

[13] OECD ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, "Smart Sensor Networks: Technologies and Applications for Green Growth," no. December, 2009.

[14] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges", IEEE Communications Surveys & Tutorials, n.° 99, pp. 1-16, 2012. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6157575

[15] A. Robnik, "The ICT sector hand-in-hand with other sectors for a VESTNIK, vol. 78, no. 5, sustainable future", ELEKTROTEHNI SKI 263-269, 2011.

[16] X. Miao and X. Chen, "Research on IPv6 Transition Evolvement and Security Architecture of Smart Distribution Grid Data Communication System", in 2010 China International Conference on Electricity Distri-bution (CICED), 2012, pp. 1-5.

[17] K. Rikitake and K. Nakao, "NGN AND INTERNET : FROM CO-EXISTENCE TO INTEGRATION Network Security Incident Response Group, National Institute of Information and Communications Technology (NICT) 4-2-1 Nukui-kitamachi , Koganei, Tokyo 184-8795 Japan Information Security Fellow, KDD", in First ITU-T Kaleidoscope Aca-demic Conference Innovations in NGN: Future Network and Services,2008. K-INGN 2008, 2008, pp. 315-322.

[18] R. Yu, Y. Zhang, S. Gjessing, C. Yuen, S. Xie, and M. Guizani,"Cognitive Radio Based Hierarchical Communications Infrastructure for Smart Grid," IEEE Network, vol. 25, n.° 5, pp. 6-14, 2011.

[19] a. Ghassemi, S. Bavarian, and L. Lampe, "Cognitive Radio for Smart Grid Communications," in 2010 First IEEE International Conference on Smart Grid Communications. IEEE, Oct. 2010, pp. 297–302. [Online].Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5622097.

[20] R. H. L. Rodríguez and R. H. G. Céspedes, "Challenges of Advanced Metering Infrastructure Implementation in Colombia", in 2011 IEEE PES Conference on Innovative Smart Grid Technologies (ISGT Latin America), 2011, pp. 1-7.

[21] G. N. Ericsson, "Cyber Security and Power System Communication Essential Parts of a Smart Grid Infrastructure" IEEE Transactions on Power Delivery, vol. 25, n.° 3, pp. 1501-1507, 2010.

[22] Y. Tanaka, Y. Terashima, M. Kanda, and Y. Ohba, "A Security Architecture for Communication between Smart Meters and HAN Devices" in 2012 IEEE Third International Conference on Smart Grid Communications(SmartGridComm), 2012, pp. 460-464.

[23] Heartbleed Bug, 2013. [Online]. Available: http://heartbleed.com/

[24] C. Camargo, M. Asprilla, N. Rosas, "Sistema electrónico para la adquisición, procesamiento y comunicación de las señales eléctricas para el uso en redes inteligentes (Smart Grids)", in *Ingenium*, n.° 27, pp. 15-24.