

# Mechanism of Communication with Devices Via SNMP Protocol SCADA Systems CEDIN

Adrian Carmona Hernandez<sup>1</sup>

<sup>1</sup> Universidad de las Ciencias Informáticas, Cuba, acarmona@uci.cu

*Abstract— In the process of development of computer networks several communication protocols for the administration of local area networks have emerged. Among them it stands out the Simple Network Management Protocol (SNMP), this is highly used by the simplicity of its management model and the high volume of information on hardware and software offering. Currently its use has spread to monitoring devices in areas such as climate and energy storage to increase the potential of their services.*

*Within several national companies that have requested monitoring solutions and control Industrial Computing Center (CEDIN) they have identified a large number of devices that communicate using SNMP. Currently there is no mechanism for the exchange of information through this protocol. Which limits the possibility for operators to monitor processes in these facilities concerning the backup power and cooling. Given this situation being targeted for work, develop a handler that allows communication with devices that communicate using SNMP.*

*To this end a study protocol, delving into the mechanisms of capture of events, requests for information and writing values was performed. This allowed developing a solution that provides supervisory control systems and developed by the CEDIN access to information from devices that communicate via SNMP control.*

*Keywords— control, driver, protocol, monitoring, SNMP.*

**Digital Object Identifier (DOI):** <http://dx.doi.org/10.18687/LACCEI2015.1.1.275>

**ISBN:** 13 978-0-9822896-8-6

**ISSN:** 2414-6668

**13<sup>th</sup> LACCEI Annual International Conference:** “Engineering Education Facing the Grand Challenges, What Are We Doing?”  
July 29-31, 2015, Santo Domingo, Dominican Republic

**ISBN:** 13 978-0-9822896-8-6

**ISSN:** 2414-6668

**DOI:** <http://dx.doi.org/10.18687/LACCEI2015.1.1.275>

# Mecanismo de comunicación con dispositivos mediante protocolo SNMP de los sistemas SCADA del CEDIN.

Adrian Carmona Hernandez

<sup>1</sup>Centro de Informática Industrial, Universidad de las Ciencias Informáticas, Cuba, [acarmona@uci.cu](mailto:acarmona@uci.cu)

**Resumen**– En el proceso de desarrollo de las redes informáticas han surgido varios protocolos de comunicación para la administración de las redes de área local. Entre ellos se destaca el Protocolo Simple de Administración de Redes (SNMP), este es altamente usado por la simplicidad de su modelo de administración y el alto volumen de información sobre hardware y software que ofrece. Actualmente su uso se ha extendido al monitoreo de dispositivos de áreas como climatización y almacenamiento energético aumentando el potencial de sus servicios.

Dentro de varias empresas nacionales que han solicitado soluciones de supervisión y control del Centro de Informática Industrial (CEDIN) se han identificado una numerosa cantidad de dispositivos que se comunican mediante SNMP. Actualmente no existe un mecanismo para el intercambio de información mediante este protocolo. Situación que limita la posibilidad para los operadores de monitorear procesos en estas instalaciones referentes al respaldo energético y la climatización. Teniendo en cuenta esta situación se toma como objetivo para el trabajo, desarrollar un manejador que permita la comunicación con dispositivos que se comunican mediante SNMP.

Con tal objetivo se realizó un estudio del protocolo, profundizando en los mecanismos de captura de eventos, solicitudes de información y escritura de valores. Esto permitió desarrollar una solución que brinda a los sistemas del dominio de supervisión y control desarrollados por el CEDIN acceso a la información de los dispositivos que se comunican por SNMP.

**Palabras claves:** control, manejador, protocolo, supervisión, SNMP.

## I. INTRODUCCIÓN

Desde la segunda mitad del siglo pasado hasta la actualidad se ha desarrollado de forma exponencial la automatización de las industrias, debido a la complejidad de sus procesos y a la necesidad de tener un control exacto sobre ellos. Como parte del proceso de automatización surgen los sistemas SCADA, acrónimo de *Supervisory Control and Data Acquisition*, en español: Control, Supervisión y Adquisición de Datos. Estos se utilizan comúnmente en infraestructuras críticas (ej. plantas nucleares, plantas de generación eléctrica, refinerías, plantas químicas y plantas industriales) y en otras áreas como la domótica donde brinda servicios de gestión energética, confort, seguridad y otros. [2]

En la Universidad de las Ciencias Informáticas (UCI), específicamente en el Centro de Informática Industrial (CEDIN) de la facultad 5, se trabaja en el desarrollo de sistemas SCADA para empresas nacionales y para la exportación. Estos sistemas están siendo utilizados en la República Bolivariana de Venezuela en el control de procesos

de exploración, producción, comercio y suministro y supervisión energética. Igualmente han sido solicitados por varias empresas nacionales como: la oficina del historiador de la Habana, la UCI, el Instituto Nacional de Meteorología (INSMET), el Centro de Inmunología Molecular (CIM), Radio Cuba y la Empresa de Telecomunicaciones de Cuba (ETECSA).

Las empresas nombradas anteriormente cuentan con una numerosa cantidad de dispositivos que se comunican mediante protocolos de comunicación de redes. Estos se definen como un conjunto de reglas que permiten la transferencia e intercambio de datos entre los distintos puntos que conforman la red. [4] Los protocolos de comunicación más usados por los dispositivos en las redes de estas empresas son hasta el momento: modbus en sus variantes (ASCII, RTU, TCP/IP), UP1/LCD, BACnet Ethernet, BACnet/IP y SNMP acrónimo de *Simple Network Manager Protocol*.

El protocolo SNMP presenta buen rendimiento en las tareas de gestión y monitorización. Por esto, la mayoría de los dispositivos en la actualidad que se conectan a una red LAN (*Local Area Network*) soportan SNMP. [6] Dentro de los dispositivos que se comunican mediante SNMP en las instalaciones se encuentran: los sistemas de respaldo energético, sistemas de alimentación ininterrumpida de electricidad, aires acondicionados, consolas de climatización, rectificadores, onduladores y estaciones de trabajo. Actualmente solo se monitorean los sistemas de respaldo energético y los sistemas de alimentación ininterrumpida de electricidad, para el primero se cuenta con una herramienta de monitoreo y configuración, que brinda el fabricante de los dispositivos de la empresa EMERSON Network Power. Este software se encuentra instalado dentro del dispositivo que administra y se accede a su interfaz vía web. En el caso de los sistemas de alimentación ininterrumpida de electricidad se utiliza el software PowerStar. Esto indica que no se pueden gestionar todos los dispositivos desde una sola pantalla, creando dificultades para la visualización y previsión de eventos que notifican el mal funcionamiento de los dispositivos.

Las soluciones de software del CEDIN no cuentan con un manejador para el intercambio de información con dispositivos que se comuniquen mediante el protocolo SNMP. Lo que implica que actualmente no sea posible supervisar en toda su extensión a las instalaciones que posean estos dispositivos.

El objetivo general del trabajo es el desarrollo un manejador que permita la comunicación con los dispositivos que se comunican mediante el protocolo SNMP.

## II. ARQUITECTURA DE LOS SISTEMAS SCADA DEL CEDIN

Actualmente el centro CEDIN se encuentra en el desarrollo de sistemas de supervisión y control para la automatización de procesos industriales en instalaciones nacionales e internacionales. Estos sistemas tienen como objetivo estratégico lograr aumentar la productividad y aprovechar mejor las infraestructuras tecnológicas de las instalaciones donde sea instalado. Están diseñados para monitorear y supervisar los procesos de forma eficiente, siendo configurables para poder mostrar a los usuarios la información de una manera más agradable y flexible. A continuación se muestra la estructura:



Figura 1. Arquitectura tipo de los sistemas de Supervisión y Control del CEDIN.

**Servicio de Adquisición:** Encargado de la recolección y procesamiento de la información proveniente de los procesos productivos. Este módulo está compuesto por tres submódulos con tareas específicas los cuales son:

**Módulo Driver:** Actúa de forma independiente en forma de bibliotecas dinámicas, permitiendo mediante diversos protocolos la comunicación con los dispositivos de campo (Autómatas, reguladores autónomos, sensores inteligentes, controladores, entre otros).

**Módulo Recolector:** Se encarga de crear un modelo de planificación y ejecutarlo, para esto se crean las listas de puntos a consultar según una frecuencia de muestreo. La función central del recolector es obtener la información del campo.

**Módulo Procesamiento:** Recibe, procesa y distribuye hacia otros niveles (ej. Base de datos históricos y la interfaz hombre máquina) toda la información recolectada. Entre las tareas que ejecuta están las de procesar las variables calculadas, trabajo con alarmas, verificación de la calidad de los datos y la linealización de la información recolectada entre otras.

**Servicio de Configuración:** Es el encargado de almacenar, persistir, garantizar la consistencia y suministrar la configuración a los demás módulos del sistema. Dentro de los

elementos de configuración que almacena el módulo se destacan los grupos operacionales de privilegios, usuarios, perfiles, grupos de transferencia a histórico, puntos, alarmas, dispositivos, canales de comunicación, tareas, despliegues, reportes entre otros.

**Servicio de Comunicaciones:** Es el encargado de la comunicación entre los módulos del sistema, implementa dos formas de comunicación la síncrona y la asíncrona. Permite enviar y recibir comandos y sus respuestas así como datos complejos como alarmas, eventos, estados de la comunicación, bitácoras de usuario entre otros. Además soporta la comunicación simultánea de los módulos.

**Servicio de Almacenamiento de Datos Históricas (BDH):** Es el encargado de almacenar la información del sistema con el objetivo de que sea utilizada en la generación de reportes y tendencias. Es la base suministradora de información para los sistemas de inteligencia de negocio o inteligencia artificial que ofrecen métricas sobre el comportamiento de los procesos.

**Servicio de Seguridad:** Proporciona las funcionalidades necesarias para garantizar el trabajo autorizado de los usuarios y constituye una fuente detectora de ataques maliciosos o no autorizados. Ejecuta acciones de protección en situaciones de corte de energía o problemas de conectividad.

**Cientes de Interfaz Hombre Máquina (HMI):** Se encarga de mostrar de forma amigable al usuario los procesos que ocurren en el campo en tiempo real y los componentes implicados. Está compuesto por dos partes fundamentales: el ambiente de configuración y el ambiente de ejecución.

## III. PROTOCOLO SNMP.

El protocolo simple de administración de redes más conocido como SNMP por sus siglas en inglés tiene como objetivo la administración y monitorización de los dispositivos de una red. Este protocolo surge sobre el año 1989 como un estándar de gestión y ya en 1990 surgen los primeros software que lo implementaban, estos tenían como características comunes que eran simples, pequeños y de bajo costo. Actualmente este protocolo es ampliamente utilizado para la obtención de estadísticas en la red. Este protocolo situado en la capa de aplicación del modelo OSI da la posibilidad a los operadores de tener una supervisión sobre el desempeño de la red y buscar problemas. Dentro de los elementos de la red SNMP se encuentran:

**Recursos administrados:** Los recursos administrados o dispositivos administrados como comúnmente se les conocen son los nodos de la red que contienen un agente SNMP. Los recursos administrados pueden ser *routers*, *switches*, servidores, estaciones de trabajo, impresoras, *hubs*, *bridges*, *pdas* y otros.

**Agente SNMP:** Un agente SNMP es un software de administración de la red que se encuentra instalado en el dispositivo administrado. Los agentes se encargan de responder las solicitudes realizadas por las entidades administradoras, así como de informar de las situaciones

anómalas en el dispositivo donde se encuentra alojado. Para esto realiza una traducción de la información a un lenguaje compatible con la sintaxis que especifica el protocolo SNMP. [5]

**Entidad administradora:** La entidad administradora es la encargada de supervisar y controlar a los recursos administrados mediante la solicitud de información a los agentes. También se encarga de establecer valores a variables en el dispositivo mediante órdenes de escritura realizadas al agente. Igualmente es la receptora de los eventos notificados por los agentes. [5]

**Base de información de gestión (MIB):** Base de datos donde se almacena la información referente a las variables gestionadas dentro de los recursos administrados, se encuentra alojada en la memoria interna de dichos dispositivos. Son la fuente que provee los datos a los agentes en cada dispositivo administrado.

La estructura que la forma es un árbol donde cada nodo está compuesto por una etiqueta nombrando al nodo y un identificador numérico único continuo en el nivel de profundidad donde se encuentra y en caso de que el nodo sea hoja, entonces estará el valor en el formato correspondiente al tipo de dato que represente. Teniendo en cuenta la descripción anterior se define entonces que las direcciones de las variables en este protocolo tienen dos formatos; uno que estaría formado por una secuencia de nombres separados por punto que definen el camino desde el nodo raíz hasta el nodo hoja y el segundo sería una secuencia de identificadores numéricos con igual semántica en su formación que las direcciones formadas por nombres. La MIB define un conjunto de variables estándares para todos los dispositivos administrados, la definición de dicha variables se encuentra registrada en el estándar RFC1157. [1]

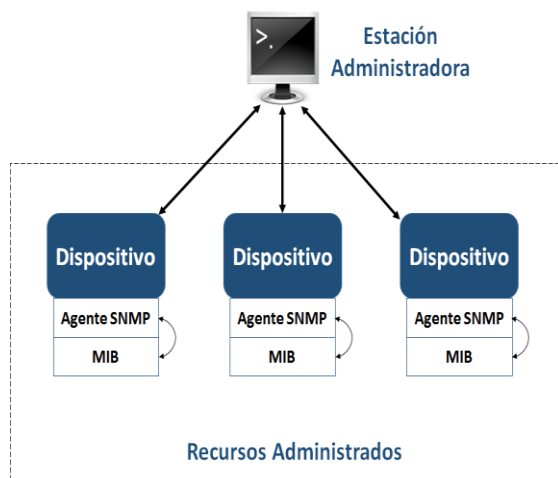


Figura 2. Arquitectura de las redes administradas por SNMP.

#### A. Operaciones del protocolo

**Operación GET-REQUEST:** Operación ejecutada por la estación administradora para obtener el valor de una o más variables.

**Operación GET-NEXT-REQUEST:** Operación ejecutada por la estación administradora para obtener el valor de la próxima variable en la rama de la dirección que se especifica.

**Operación SET-REQUEST:** Operación realizada por la estación administradora para establecer un valor sobre una o más variables.

**TRAP:** Operación ejecutada por el agente SNMP de forma no solicitada por la estación administradora; el objetivo de esta funcionalidad es notificar a la entidad administradora sobre cualquier evento o condición en la estación administradora.

#### IV. CARACTERISTICAS DEL MANEJADOR SNMP

Los manejadores son encargados de intercambiar información con los dispositivos de campo. Son componentes de software creados como bibliotecas dinámicas. Toda la información que obtienen así como las solicitudes hechas a los manejadores se realizan mediante la interfaz genérica la cual es la encargada de encapsular el comportamiento de todos los manejadores del SCADA abstrayendo al sistema de las especificaciones de cada uno de los protocolos de comunicación. El manejador SNMP fue desarrollado bajo la interfaz genérica 6 que ofrece las bases para lograr un proceso de recolección más eficiente. Además esta provee los mecanismos necesarios para aquellos protocolos donde las alarmas son generadas desde los dispositivos sean capturadas y subir la información de manera rápida a los módulos superiores.

##### A. Funcionalidades del manejador SNMP.

**Configuración de dispositivo, transporte y protocolo:** El manejador permite configurar los parámetros de los dispositivos SNMP estos son: comunidad de lectura y escritura, versión del protocolo y fichero con la configuración de la severidad de las alarmas. También se le pueden configurar al transporte los parámetros dirección IP y puerto remoto. Estas operaciones están basadas en la capacidad de introspección de los manejadores del SCADA los cual posibilita establecer y consultar valores a partir del nombre de los parámetros configurables.

**Evaluación de la comunicación con el dispositivo:** Esta funcionalidad provee de conocimiento valioso acerca del estado de comunicación entre los dispositivos de las instalaciones y el SCADA. Es vital en la detección de fallas de comunicación y en la evaluación del rendimiento del manejador. Ir al anexo #3 para ver los posibles valores del estado de la comunicación.

**Calidad de los datos recolectados:** El manejador reporta la calidad de los datos recolectados en la operación de lectura, en esta calidad intervienen factores como las fallas de comunicación, la capacidad de respuesta y cálculo de los dispositivos, el tráfico en la red y otros. La calidad de los datos es una información valiosa ya que mediante ella se conoce que

tan buena es la respuesta y los datos con que se cuenta y en algunos casos diagnostica problema en los dispositivos. El establecimiento de ese valor en el caso del protocolo SNMP lo establece el manejador según la evaluación de los factores antes mencionados y los valores son discretos, únicos y bien conocidos

**Notificación de errores:** El manejador tras realizar cualquier transacción con los dispositivos tiene en cuenta el error en la transacción, los valores de error notifican sobre problemas de configuración, comunicación y sobre formaciones incorrectas en los datagramas del protocolo SNMP. Es de vital importancia para evaluar los datos recolectados, para reintentar las operaciones y notificar a los operadores.

**Lectura de variables en los dispositivos:** Es una de las operaciones fundamentales del manejador SNMP con ella se pueden obtener los valores de cualquiera de las variables que expone los dispositivos mediante el protocolo SNMP.

**Escritura de variables en los dispositivos:** Esta operación le permite al sistema establecer los valores deseados a las variables que sean de escritura.

**Captura y notificación de Alarmas:** El manejador es capaz de capturar las alarmas emitidas por los dispositivos que monitorea y enviar la información de valor a los módulos superiores.

### B. Modelo de Dominio

Para el correcto análisis del modelo de dominio se puntualizan los siguientes conceptos:

**SCADA:** Concepto generalizador de los componentes del SCADA.

**Manejador:** Componente del SCADA encargado del intercambio de información con los dispositivos que se comunican mediante un protocolo específico.

**Mensaje:** Representa la información que es intercambiada entre el manejador y cualquier agente SNMP.

**Protocolo de comunicación:** Conjunto de reglas que rigen la comunicación entre dispositivos. En este caso el protocolo es SNMP.

**Agente SNMP:** Aplicación que administra los dispositivos e intercambia información con el manejador mediante mensajes.

**Recursos Administrados:** Representa los dispositivos que son administrados mediante el protocolo SNMP.

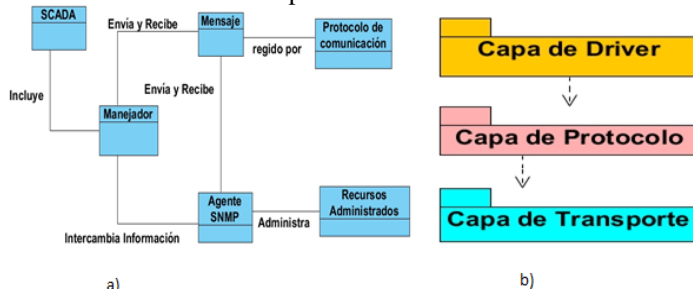


Figura 3. a) Modelo de dominio b) Arquitectura del manejador.

### C. Arquitectura en capas del manejador

Para el diseño del manejador se utiliza el patrón en capas el cual establece que:

Organiza la estructura lógica de gran escala de un sistema en capas separadas de responsabilidades distintas y relacionadas. Con una separación clara y cohesiva de intereses donde las capas "más bajas" son servicios generales de bajo nivel, y las capas más altas son más específicas de la aplicación.

La colaboración y el acoplamiento es desde las capas más altas hacia las más bajas; se evita el acoplamiento de las capas más bajas a las más altas. [3]

Para el caso del manejador se definen tres capas que a continuación se muestran:

La **capa de driver** es la encargada de traducir a llamadas de la capa de protocolo las solicitudes realizadas mediante la interfaz genérica. Esta desarrolla la capacidad de introspección del manejador registrando los parámetros de configuración de redes, dispositivos y manejadores.

Esta es la capa superior del sistema la cual transmite los datos al resto del SCADA. Esta capa está relacionada con la capa de protocolo de forma bidireccional. La capa de driver realiza las solicitudes de operaciones a la capa de protocolo y recibe las respuestas de ellas para transmitir las a los niveles superiores.

La **capa de protocolo** proporciona una serie de funciones que encapsulan la construcción e interpretación de los mensajes necesarios para la comunicación con los dispositivos de acuerdo a las reglas del protocolo. Esta capa recibe las solicitudes de las operaciones a realizar de la capa de driver, utiliza la capa de transporte para comunicarse con el dispositivo y resolver la información. Finalmente envía la respuesta de las operaciones a la capa de driver.

La **capa de transporte** es la encargada de manejar la conexión y los detalles de la transmisión del flujo de datos a través del medio físico. Para desarrollar estas capacidades utiliza la biblioteca *TransportProvider 2.0* la cual provee una comunicación mediante el protocolo de transporte UDP. Además en esta capa se desarrolla el mecanismo para la captura de alarmas basada en funcionalidades de la biblioteca *boost* específicamente las definidas en *asio*.

### D. Diagrama de componentes del manejador SNMP

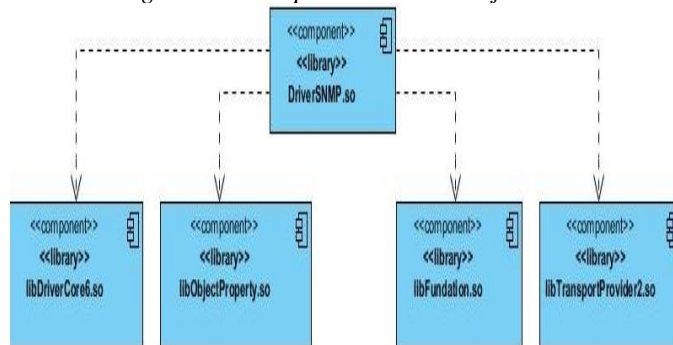


Figura 4: Diagrama de componentes del manejador SNMP.

### E. Diagrama de Despliegue

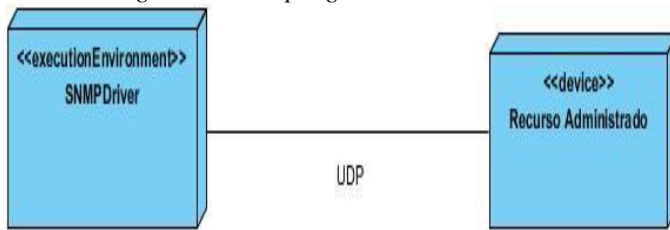


Figura 5: Diagrama de despliegue del manejador SNMP.

### V. RESULTADOS DEL DESARROLLO DEL MANEJADOR SNMP.

- 1) A nivel mundial existe una gran cantidad de herramientas para la administración de redes, dentro de las mejores encontramos las desarrolladas mediante SNMP, esto indica que el protocolo por sus características ofrece altas garantías en las tareas de monitorización y control.
- 2) Los sistemas SCADA más prestigiosos a nivel internacional cuentan entre sus soluciones con manejadores o herramientas para el monitoreo de dispositivos que se comuniquen mediante SNMP. En muchos de los casos utilizan el protocolo para la supervisión y control de la red distribuida del SCADA lo cual proporciona una vía eficiente para reducir las fallas de comunicación y las fallas de forma general del sistema SCADA.
- 3) El protocolo SNMP posibilita supervisar tanto recursos de hardware como de software ofreciendo altos volúmenes de información acerca de los dispositivos administrados.
- 4) El manejador se desarrolló a partir de una investigación del protocolo y de las herramientas de renombre el que utilizan el protocolo SNMP. El sistema está en condiciones de intercambiar información con los dispositivos con que cuentan las instalaciones de las empresas que solicitaron el producto. Además se tienen en cuenta la posible integración a la red de otros dispositivos que se puedan administrar vía SNMP, el sistema no se restringe a tipos específicos de dispositivos.
- 5) El manejador está desarrollado sobre una plataforma de software libre, con herramientas de software libre.
- 6) El desarrollo del protocolo fue desarrollado bajo las normativas de las especificaciones certificadas a nivel internacional.
- 7) Es el primer SCADA nacional que posee un manejador SNMP, lo que posibilita la conectividad del mismo con un número mayor de dispositivos. Esto implica que el sistema pueda extender sus servicios en las instalaciones donde se despliegue.
- 8) Es un aporte más de la Universidad de las Ciencias Informáticas en busca de la independencia tecnológica del país y elevar la productividad de las empresas haciendo un uso adecuado de las tecnologías.
- 9) Con el desarrollo de este manejador se crean las bases para lograr que el mismo sistema SCADA de forma

autónoma y sin recurrir a otro sistema pueda administrar su red distribuida. Esto permitirá calcular parámetros como caudal, disponibilidad, pérdida de paquetes y otros que permitirá tener un diagnóstico correcto sobre el estado de la red en que se comunican sus dispositivos.

- 10) Este producto facilita el trabajo a los operadores ya que elimina para ellos :  
Recorridos constantes de largas o medianas distancias para ejecutar operaciones sobre los dispositivos.
  - Registro manual de la información de los dispositivos.
  - Fallas de apreciación (Algunos casos los dispositivos no tienen pantallas de comunicación con los usuarios y la información se obtiene a partir de la observación y la experiencia del operario).
- 11) Mejora para la empresa la fiabilidad de la información obtenida a partir de los dispositivos y tienen conocimiento de forma inmediata sobre anomalías en los dispositivos lo que les permite tomar acciones de forma más rápida.
- 12) Evita roturas en dispositivos de alto costo como aires acondicionados, consolas de climatización y sistemas de respaldo energético los que influyen en la productividad de la instalación de manera directa o indirecta. Por ejemplo los aires acondicionados influyen en la climatización de los locales y brindan confort a los trabajadores, también los sistemas de respaldo energéticos posibilitan mantener la electricidad tras un falla de esta naturaleza.
- 13) Muchos de los dispositivos que se administran mediante SNMP en estas empresas son dispositivos de almacenamiento energético o respaldo energético que su operación manual es peligrosa y a menudo existen accidentes laborales. Con el manejador se conoce de situaciones como esta, permitiendo prevenir a tiempo accidentes.

### VI. CONCLUSIONES

Se obtuvo el manejador para el protocolo SNMP capaz de comunicarse e intercambiar información con los dispositivos que se comunican mediante este protocolo. Durante el proceso investigativo inicial se logró estudiar las especificaciones certificadas del protocolo y realizar un estudio del arte sobre los sistemas de administración de red que lo utilizan en sus tareas, esto influyó positivamente en el desarrollo del manejador pues se tomaron las mejores experiencias y se acotaron al dominio del manejador.

El manejador para el protocolo SNMP permitirá a los sistemas SCADA del CEDIN tener un campo de ejecución de mayor alcance donde podrán interactuar con nuevos dispositivos de las ramas de climatización, almacenamiento energético, interconexión de redes e instrumentos de medición.

## VII REFERENCIA BIBLIOGRÁFICAS

- [1] **Group, N.W., P.S. International, and M.L.f.C. Science. 1990.** *A Simple Network Management Protocol (SNMP) RFC 1157*. s.l. : Network Working Group, 1990.
- [2] **Krutz, R.L. 2006.** *Securing SCADA System*. Indiana : Estados Unidos Wiley Publishing, 2006. 978-7645-9787-9..
- [3] **Larman, C. 1999.** *UML y Patrones*. Juarez, Mexico : Prentice Hall, 1999.
- [4] **Marquez, J.E.B. 2005.** *Transmision de datos*. s.l. : dtion ed. Merida: taller de publicaciones de la facultad de ingenieria, ULA, 2005.
- [5] **Systems, C., B.S. Inc., Inc., and IBM. 1999.** *An Architecture for Describing SNMP Management Frameworks RFC 2571*. s.l. : Network Working Group., 1999.
- [6] **Tejedor R.J.M. 2004.** *Tendencias en gestión de red*. 2004.
- [7] **Siemens.** SCADA System, SIMATIC WinCC Open Architecture [En línea]. 2011, [cited 15 octubre 2014]. Available from Internet:<[www.siemens.com/wincc-open-architecture](http://www.siemens.com/wincc-open-architecture)>.
- [8] **Wonderware.** Industry Application for Facilities Management [En línea]. 2013, [cited 15 noviembre 2013 ]. Available from 58 Internet:<<http://global.wonderware.com/DK/Pages/WonderwareIndustryApplicationFacilityManagement.aspx>>.
- [9] **Union, I.T.** Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). In., 2002.
- [10] **Rodriguez Penin, A.** *Sistemas SCADA*. Edtion ed. Barcelona,España: Marcombo, 2007. ISBN 978-84-267-1450-3.
- [11] **Power, E.N.** PowerStar Remote Management Software For The PS Series DC Power Systems [En línea]. 2014, [cited 24 enero 2014]. Available from Internet:<[http://www.emersonnetworkpower.com/en-ASIA/Products/DCPower/ensys\\_Monitoring/Pages/PowerStar.aspx](http://www.emersonnetworkpower.com/en-ASIA/Products/DCPower/ensys_Monitoring/Pages/PowerStar.aspx)>.
- [12] **Industrial, C.D.I.** 2011. Introducción a la Arquitectura del Guardián del ALBA. In *Proceedings of the Sistema Supervisor Guardián del ALBA*, Ciudad de la Habana ,Cuba2011 Universidad de las Ciencias Informáticas.
- [13] **Kepware.** Water and Wastewater Infrastructure Monitoring with SCADA [En línea]. 2013, no. 12-febrero-2014 ] [cited 18 octubre 2013. Available from Internet:<[http://www.kepware.com/Solution\\_Chronicles/water\\_wastewater\\_infrastructure\\_monitoring\\_SCADA.asp](http://www.kepware.com/Solution_Chronicles/water_wastewater_infrastructure_monitoring_SCADA.asp)>.
- [14] **Autores, C.D.** 2013. Recolección y Manejadores en el “GUARDIAN DEL ALBA”. In *Proceedings of the Sistema Supervisor Guardián del ALBA*, Habana , Cuba 2013.