Universidad de las Ciencias Informáticas
Facultad 5 “Hardware y Automática”

Título: Módulos de adquisición y análisis para la interacción con dispositivos de campo en un SCADA.

Memoria de Individual para optar por el título de Ingeniero en Ciencias Informáticas

Autor: Antonio Cedeño Pozo

Tutor: Dr. Rafael Arturo Trujillo

Co-tutor: Amado Espinosa Hidalgo

Consultante: Juan Antonio Fung Goizueta

Cuidad de la Habana, abril de 2009
“Año del 50 Aniversario del Triunfo de la Revolución”

Datos de contacto

Dr. Rafael Arturo Trujillo Codorniu.
Email: rafaeltc@uci.cu

Máster en Ciencias Físico-matemáticas en 1979, Universidad de Odessa, URSS. Doctor en Ciencias Físico-matemáticas en 1986, Universidad de Rostov del Don, URSS. Ostenta la categoría docente de Profesor Titular.

Ing. Amado Espinosa Hidalgo
Email: aespinosa@uci.cu

Graduado de Ingeniero Informático en el 2004 y profesor instructor con cuatro años de experiencia docente en la Universidad de las Ciencias Informáticas (UCI) y cinco en el desarrollo de software.

Agradecimientos

A Nuestra Revolución Socialista por darme la oportunidad de estudiar en una Universidad tan especial como la UCI, en ningún otro sistema un jóven humilde podría soñar con este privilegio.

A mi novia Katia, por soportarme todos estos años, por su interés, dedicación y amor muchas gracias, no creo que hubiese alcanzado resultado alguno sin tu ayuda, te amo.

A mis futuros suegros Maira y Roberto, presentes siempres en cada evento, gracias por su apoyo y por enseñarme que lo realmente importante no se logra con talento, sino con mucho sacrificio.

A mis compañeros de trabajo Fung, Amado, René, Ariel, Roberto, Luis Enrique, Manuel, Ana Silvia, Irina, Iliana, Sachel, Hardys y a toda la familia HA, gracias por ser como hermanos y por hacerme creer que siempre puedo contar con ustedes.

A mi tutor Trujillo, por enseñarme a ser un mejor profesional y una mejor persona.

A mis padres, que desde niño supieron formar en mi los valores más puros, que me enseñaron las bondades del trabajo duro, la importancia de la sencillez y la humildad, que confían en que su hijo siempre dará lo mejor para que se sientan orgullosos. Gracias Viejo, gracias Mamá, los amo.

A todas las personas que haciendo uso de la tolerancia y el empeño aportaron su granito de arena en mi formación, llegue hoy mi más sincero agradecimiento.

Dedicatoria

A mis padres Maira y Antonio.
A mis abuelitos que ya no están.
A mi hermano Arleis.
A mi novia Katia.
A mis futuros suegros Maira y Roberto.
A toda mi familia.

Síntesis

En el presente material se exponen las principales características de los manejadores de dispositivos desarrollados para el Sistema de Supervisión y Control de Procesos "Guardián del ALBA" , SCADA nacido en el marco de colaboración Cuba-Venezuela con la participación de un grupo de profesores y estudiantes de la Universidad de las Ciencias Informáticas, la Universidad Central de las Villas y el Instituto Superior Minero Metalúrgico de Moa. El trabajo explicará además el funcionamiento de un Analizador de Tramas desarrollado con el objetivo de brindar mantenimiento a la comunicación del sistema SCADA con los dispositivos de campo. A partir de una serie de actividades desarrolladas, el autor realiza una explicación sobre temas relacionados con el diseño, implementación y pruebas de los manejadores referentes a los protocolos Modbus y Ethernet/IP, así como los elementos fundamentales que hicieron posible el desarrollo del Sniffer. Se ofrece al lector una visión sobre los principales resultados obtenidos en materia de productos palpables y puestos en producción, trabajos presentados en diferentes eventos, así como los aportes realizados al país desde el punto de vista económico.

Palabras claves

- Manejadores de dispositivos
- SCADA
- Analizador de tramas
- Dispositivos de campo
- Protocolos
- Modbus TCP
- Modbus ASCII
- Modbus RTU
- Ethernet/IP
- ABEthernet
- Sniffer

Índice

Datos de contacto....2
Agradecimientos....3
Dedicatoria....4
Síntesis....5
Introducción....7
1-Fundamentación Teórica....9
1.1-Dispositivos....10
1.2- Protocolos....12
1.3- Manejadores de dispositivos....13
2- Manejadores de dispositivos industriales....15
2.1- Capa de transporte....16
2.2- Capa de Protocolo....18
2.3- Capa de Implementación de la IGD....19
2.4- Demo....19
2.5- Modbus....20
2.5.1- Protocolo Modbus....21
2.5.2- Manejador Modbus....22
2.6- Ethernet/IP....23
2.6.1- Protocolo Ethernet/IP....24
2.6.2- Manejador Ethernet/IP....25
3- Analizador de tramas....26
3.1- Tecnologías y funcionalidades....26
Resultados....29
Conclusiones....31
Referencias....31
Anexos....32

Introducción

El acontecimiento más relevante y dramático ocurrido durante toda la historia de la industria petrolera venezolana ha sido sin dudas el sabotaje cometido contra PDVSA entre diciembre del año 2002 y enero de 2003. Los hecho fueron organizados por dirigentes de los sindicatos petroleros de los sectores de la oposición que promovieron la paralización de la industria, los objetivos estaban muy bien delimitados, lograr la desestabilización de la principal fuente de ingresos de Venezuela que terminaría por asfixiar al gobierno bolivariano y obligaría a la renuncia del presidente Hugo Chávez. Una de las maniobras más significativas del sabotaje estuvo marcada por el bloqueo de los sistemas de automatización existentes para la supervisión y el control de los procesos dentro de la industria petrolera. Los sectores opositores una vez más tuvieron a su favor la mano del imperio, pues gran parte de los sistemas de software con los que contaba PDVSA estaban controlados por INTESA, una empresa norteamericana dedicada a este tipo de actividad que, ante el golpe petrolero, adoptó una actitud servil a los intereses de la oposición. A partir de este lamentable incidente, el Gobierno Bolivariano decidió comenzar el largo camino para lograr una verdadera soberanía tecnológica, la concepción de la idea de desarrollar un sistema de supervisión y control para la industria petrolera, constituye sin dudas uno de los primeros pasos para lograr el objetivo deseado.

A mediados del año 2006 comenzó a desarrollarse el sistema que daría solución a la supervisión y el control de los procesos en la industria petrolera de Venezuela. El equipo de trabajo se dividió en dos, la parte cubana y la venezolana. El capital humano de la parte cubana se nutrió de estudiantes y profesores de la Universidad de las Ciencias Informáticas y de profesionales en diferentes especialidades de la Universidad Central de las Villas Marta Abreu y del Instituto Superior Minero Metalúrgico de Moa. El "Equipo Cuba" inició sus actividades a partir de la primera iteración de la fase de elaboración, se realizó la definición de una arquitectura candidata y se crearon diferentes líneas de trabajo para dar cumplimiento a los requisitos recibidos de la parte venezolana, uno de las líneas definidas sería la encargada del desarrollo del módulo de manejadores de dispositivos.

En PDVSA existe un gran número de elementos de hardware destinados a la automatización de los procesos fundamentales para la producción, el sistema debía ser capaz de ofrecer un mecanismo para el acceso a la información tanto de proceso como de estado de diferentes dispositivos, sensores y actuadores. El intercambio de datos con dichos instrumentos se realiza mediante protocolos de comunicación, que no son más que el "lenguaje" mediante el cual se realizan las peticiones de escritura y lectura de las variables configuradas y de relevancia para el sistema SCADA.

Ante esta situación, se analizó el siguiente **problema**:

¿ Cómo acceder a la información de las variables configuradas en los dispositivos de campo de forma eficiente, segura y con mecanismos para mantenimiento de la comunicación ante posibles fallos ?

Para resolver este problema se planteó como **objeto de estudio** el proceso de adquisión de datos en los sistemas SCADA, y como **campo de acción** los mecanismos para el acceso a la información de proceso o de estado de los dispositivos de campo en el SCADA "Guardián del ALBA".

El **objetivo general** consistió en el desarrollo de un conjunto de manejadores encargados del acceso a los dispositivos para realizar las operaciones soportadas por los mismos, así como el desarrollo de una aplicación de mantenimiento para monitorear el flujo de información entre el sistema de supervisión y los elementos de campo.

Para dar cumplimiento al objetivo planteado, en la línea se propuso el desarrollo de las siguientes **tareas de investigación**:

- Estudio de las tecnologías y mecanismos de transporte de tramas a través de los medios físicos más usados.
- Diseño e implementación de una capa de transporte para el envío y la recepción de paquetes mediante las interfaces RS-232 e IEEE802.3i (Ethernet).
- Diseño e implementación de una interfaz genérica para los manejadores.
- Desarrollo de un manejador Demo.
- Desarrollo de los manejadores Modbus ASCII, Modbus RTU y Modbus TCP.
- Desarrollo del manejador Ethernet IP.
- Desarrollo del manejador ABEthernet.
- Estudio de los mecanismos para el análisis de tramas.
- Estudio de las tecnologías para la comunicación entre procesos.
- Diseño e implementación del analizador de tramas.

- Diseño e implementación de plugins para el analizador de tramas.
- Desarrollo de aplicaciones de prueba para cada uno de los manejadores desarrollados.

De manera general, las tareas relacionadas ilustran los retos fundamentales a los que se enfrentaron los integrantes de la línea de manejadores, o "línea de drivers" como se le llamó de forma habitual. El autor de este material participó de manera activa y directa en la realización y cumplimiento de cada una de ellas. Para el desarrollo no se requirió de ningún tipo de inversión, los recursos humanos se prepararon sobre la marcha, la bibliografía consultada se encuentra de forma gratuita en Internet y las tecnologías utilizadas desde el punto de visto del software fueron siempre Software Libre.

Contar con un equipo y un mecanismo propio para el desarrollo de manejadores de dispositivos constituyó un reto enorme, el impacto del resultado está basado en diferentes criterios. El primero de ellos es el relacionado con la independencia tecnológica, las transnacionales proveedoras de tecnologías para la automatización a nivel mundial, obtienen enormes ganancias por concepto de software, y claro está, por las actualizaciones periódicas de los mismos, los manejadores para acceder a los dispositivos constituyen una parte importante de esas ganancias. Al contar con un equipo de desarrollo de manejadores no sólo se reutilizarían los instrumentos instalados en PDVSA, sino que se contaría con suficiente conocimiento acumulado para enfrentar el desarrollo de manejadores para futuras adquisiciones de hardware. Por otra parte Cuba se encuentra en el proceso de transición hacia el Software Libre, y en esa tarea el desarrollo de manejadores resulta de vital importancia para todas las empresas nacionales que pretenden sustituir sus sistemas propietarios por tecnologías libres.

1-Fundamentación Teórica

Cuando se habla de dispositivo en la terminología de las ciencias informáticas, se hace referencia a los componentes de la computadora, es decir, elementos de hardware que interactúan para brindar un conjunto de funcionalidades útiles para los usuarios. El sistema operativo es el programa más importante de un ordenador, para que funcionen los otros programas, cada computadora debe tener un sistema operativo, encargado de realizar tareas básicas, tales como reconocimiento de la conexión del teclado, enviar la información a la pantalla, el manejo de archivos y directorios en el disco, y controlar los dispositivos

periféricos tales como teclado, impresoras, escáner, entre otros. Ante tales afirmaciones podría plantearse la siguiente interrogante:

¿Cuál es el mecanismo que permite la comunicación del sistema operativo con los diferentes periféricos?

Los controladores de dispositivos son los encargados de realizar esta tarea. Un controlador de dispositivo (en inglés, *driver*), no es más que programa informático que permite al sistema operativo interactuar con los periféricos, haciendo una abstracción del hardware y permitiendo, mediante una interfaz bien definida, el acceso a los mismos. En el presente capítulo se abordarán temas relacionados con los dispositivos y manejadores de dispositivos, pero trasladando los conceptos hacia el mundo de la automatización de procesos industriales.

1.1-Dispositivos

En la actualidad existe un gran número de dispositivos, entre los que se destacan los llamados dispositivos de entrada-salida (E/S), divididos en tres grandes grupos :

- Dispositivos de interfaz de usuario: Permiten la comunicación entre los usuarios y la computadora. Dentro de este grupo se incluyen todos los dispositivos que sirven para proporcionar interfaz con el usuario, tanto para entrada (ratón, teclado, etc.) como para salida (impresoras, pantalla, etc.).

- Dispositivos de almacenamiento: Se usan para proporcionar almacenamiento de datos y memoria. Su principal función es abastecer de datos y almacenamiento a los programas que se ejecutan en la unidad central de procesamiento (UPC). Según la velocidad con la que pueden acceder a los datos almacenados en los dispositivos, se pueden dividir en almacenamiento secundario (discos y disquetes) y terciario (cintas).

- Dispositivos de comunicaciones: Permiten la comunicación entre nodos a través de una red. Entre los dispositivos más importantes se destacan los módem, para comunicación vía telefónica, y las tarjetas de interfaz a la red, para la conexión en áreas locales.

En el presente material se utilizan los términos dispositivos industriales y dispositivos de campo para hacer referencia a elementos de hardware, tales como Controladores Lógicos Programables (PLC), Computadoras Industriales, Sistemas de Control Distribuidos, sensores o actuadores inteligentes con capacidad de comunicación. Cada uno de estos elementos puede albergar información de proceso o estado de sí mismo y forma parte de un sistema automatizado.

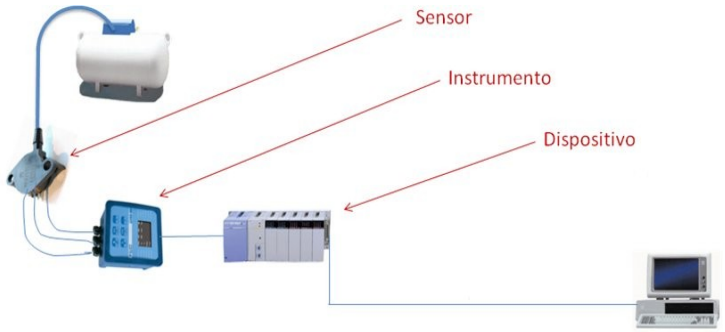

Figura 1.1 Elementos de campo.

La **Figura 1.1** muestra elementos que generalmente están presentes en un mecanismo de automatización. Un sensor es un aparato que detecta manifestaciones de cualidades o fenómenos físicos, como la energía, velocidad, aceleración, tamaño, cantidad, etc. El instrumento por su parte es una especie de traductor de la magnitud física obtenida por el sensor en otra que facilita su medida, mientras que los dispositivos controlan la lógica de funcionamiento de las máquinas, plantas y procesos industriales, realizando además operaciones aritméticas para manejar señales y realizar estrategias de control (1).

Dentro de los dispositivos de campo más difundidos encontramos a los Controladores Lógicos Programables (PLC). Un autómata programable industrial, como también se los conoce, es un equipo electrónico de control con un cableado interno independiente del proceso a controlar, que se adapta a dicho proceso mediante un programa de software específico que contiene la secuencia de operaciones a realizar. Estas operaciones se definen sobre las señales de entrada y salida al proceso, cableadas directamente al autómata. Las señales de entrada pueden proceder de elementos digitales, como detectores de proximidad, o analógicos, como sensores de temperatura y dispositivos de salida en tensión o corrientes continuas. El autómata gobierna las señales de salida según el programa de control previamente almacenado en una memoria, a partir del estado de las señales de entrada. Este programa se introduce en el autómata a través de la unidad de programación que permite además funciones adicionales como depuración de programas, simulación, monitorización de control de autómata, etc.

1.2- Protocolos

En el mundo de las Ciencias Informáticas se conoce como protocolo de comunicación a determinadas reglas que deben cumplir los dispositivos que desean comunicarse, de forma análoga a un idioma, los nodos deben aprender la gramática, la sintaxis y todas las reglas del idioma para lograr comunicación entre ellos. En los protocolos se pueden reconocer algunas propiedades, por ejemplo:

- Rigen los pasos para comenzar la comunicación entre dos nodos.
- Determinan el inicio y el fin de los mensajes, así como el resto del formato de los mismos.
- Realizan la corrección de los errores.
- Marcan la terminación de la sesión de conexión.
- Plantean estrategias de seguridad.

Cuando se trata de protocolos de comunicación no puede dejar de mencionarse al modelo de referencia de Interconexión de Sistemas Abiertos (OSI), considerado un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones y formado por las capas o niveles que se muestran a la izquierda en la **Figura 1.2** .

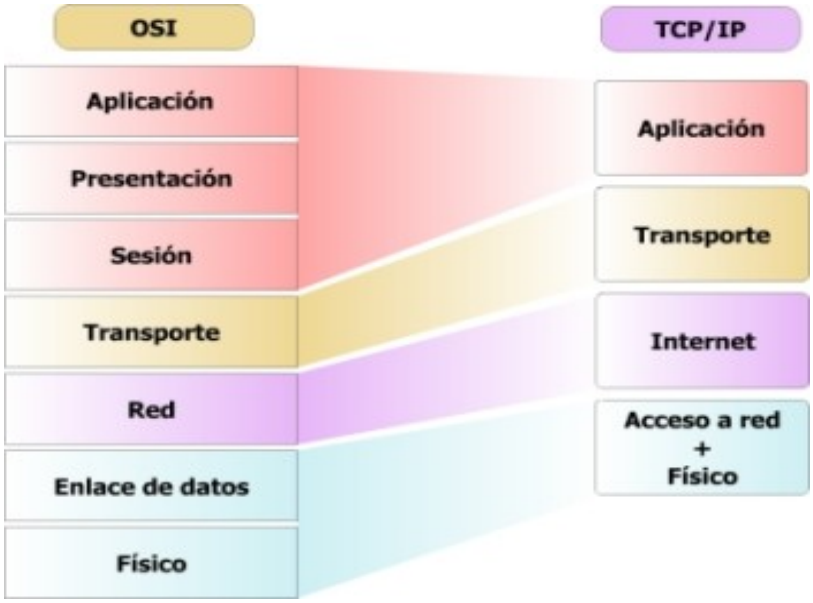

Figura 1.2 Modelos OSI y TCP/IP.

El modelo OSI fue desarrollado en 1983 y adoptado en 1984 por la Organización Internacional para la Estandarización (ISO, por sus siglas en inglés), dicho modelo de referencia muestra cómo debe transmitirse un mensaje entre nodos en una red de datos, posee siete niveles o capas, donde la función de una capa "n" es la de proveer un servicio a una capa "n+1" (2). Por su parte en el modelo TCP/IP, como se muestra en la **Figura 1.2**, cada nivel corresponde a uno o más niveles del modelo de referencia OSI, y constituye, por lo tanto, una simplificación de éste último.

1.3- Manejadores de dispositivos

Un controlador o manejador de dispositivo (en inglés, *driver*) es un programa informático que permite al sistema operativo interactuar con un periférico, proporcionando una interfaz que hace posible la abstracción del hardware. Los manejadores de dispositivos constituyen piezas esenciales de los sistemas computarizados, pues sin ellos no se podría usar el hardware. Se puede afirmar que existen tantos tipos de controladores como tipos de periféricos, y con mucha frecuencia se puede encontrar más de un manejador para un mismo dispositivo, donde cada uno ofrece un nivel distinto de funcionalidades. Normalmente son los fabricantes del hardware quienes escriben sus controladores, ya que conocen mejor el funcionamiento interno de cada aparato, pero también se encuentran controladores libres, por ejemplo en los sistemas operativos libres. En este caso, los creadores no son siempre miembros de la empresa fabricante, aunque a veces hay una cooperación con ellos, cosa que facilita el desarrollo.

A nivel internacional son muchas las empresas y marcas dedicadas a la elaboración de componentes de hardware, específicamente, en el mundo de la automatización de procesos industriales podemos citar las siguientes:

- ABB
- Siemens
- Rockwel (Allen-Bradley)
- Trend Controls
- Omron
- General Electric
- Panasonic
- Mitsubichi
- Isi Matrix Machines
- Fraz Max
- Tesco Controls

- Koyo
- Schneider Electric

La mayoría de estas empresas utilizan estándares internacionales para definir los protocolos mediante los cuales será posible la comunicación con los elementos de hardware que fabrican. Las formas como los instrumentos fabricados por éstas firmas se comunican con otros dispositivos son muy variadas, típicamente tienen integradas interfaces de comunicación, tales como: RS-232, RS-485, RS-222 y Ethernet (IEEE 802.3); sobre estos tipos de interfaces las comunicaciones se establecen utilizando diferentes protocolos o lenguajes de comunicaciones, por ejemplo: Modbus, Ethernet-IP, Profibus, DH+, DF1, DNP, Device Net, Control Net, etc.

Generalmente los fabricantes proveen uno o varios manejadores para sus dispositivos. Conociendo la especificación del protocolo utilizado, los controladores pueden ser desarrollados por terceros, en algunas oportunidades los fabricantes de elementos de hardware no siguen exactamente estándares de protocolos conocidos; sino que realizan algunas modificaciones en su implementación, en esos casos sería muy complicado desarrollar el manejador correspondiente, resultando necesario conocer los cambios realizados o los elementos introducidos.

En Cuba existen algunas empresas que poseen experiencia en el diseño y ensamblado de equipos para la automatización de procesos industriales, entre ellas se puede mencionar a la Empresa de Servicios Técnicos de Computación Comunicaciones e Informática del Níquel (SerCoNi), perteneciente a la Unión del Níquel en el municipio Moa de la provincia Holguín, y al Instituto Central de Investigaciones Digitales(ICID), ésta última institución trabaja en los campos de automatización y sistemas integrados, sistemas médicos de tecnología avanzada, computación, desarrollo y producción de equipos electrónicos y circuitos impresos. Ambas entidades se basan en estándares internacionales a la hora de diseñar e implementar los protocolos para sus dispositivos y muchas veces proveen los manejadores asociados a los mismos. La empresa SerCoNi desarrolló además un Sistema de Supervisión y Control de Procesos denominado "EROS", que constituye dentro de las aplicaciones de su tipo, una de las más difundidas y usadas, con más de 50 copias instaladas en plantas productivas de Cuba y del extranjero.

2- Manejadores de dispositivos industriales

En la cadena de tratamiento de la información en un SCADA el primer eslabón es la adquisición de los datos. Estos provienen de disímiles equipos que pueden ser autómatas, PLC, reguladores autónomos, sensores inteligentes, controladores, etc. Esta variedad está generalmente ligada al tipo de proceso y a consideraciones de orden económico. Es difícil que un SCADA contemple, en su código, todos los protocolos posibles para esta gran variedad de dispositivos. Por el contrario lo común es crear un protocolo genérico y la tarea de traducir este protocolo genérico a los protocolos específicos se le encarga a los manejadores, que, como regla, se programan en módulos independientes al SCADA (3). A partir de esa idea surge la Interfaz Genérica de los Manejadores de Dispositivos para el proyecto SCADA "Guardián del ALBA" (IGD), que consiste, desde el punto de vista del programador, en un conjunto de funciones definidas en el lenguaje de programación ANSI C, que brindan la posibilidad del acceso a dispositivos industriales.

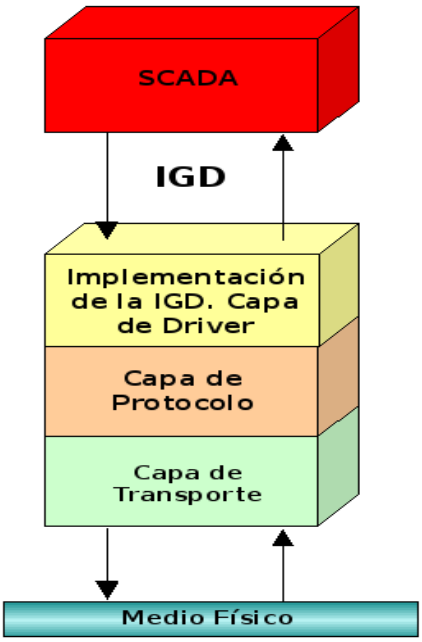

Figura 2. Arquitectura de los manejadores.

Como se observa en la **Figura 2**, la Implementación de la IGD constituye la capa superior de la arquitectura de los manejadores, la misma está compuesta por un conjunto de clases que representan las características y funcionalidades comunes para todos los

manejadores que serán desarrollados para el SCADA "Guardián del ALBA". La Capa de Protocolo por su parte, se encarga del modo de funcionamiento y de la semántica de las tramas de los protocolos, y hace uso de la Capa de Transporte para el intercambio de información con los dispositivos de campo.

El autor de este trabajo participó en el desarrollo de las capas mencionadas. En próximos epígrafes se realizará un análisis más detallado de cada una de ellas, brindando elementos relacionados con el diseño y la implementación de algunos manejadores.

2.1- Capa de transporte

La interacción entre los manejadores y los dispositivos se efectúa mediante el envío y recepción de mensajes a través de un medio físico determinado, por tanto, uno de los primeros retos a la hora de tratar de desarrollar algún tipo de controlador es la implementación de un transporte, que no es más que un conjunto de funcionalidades que permiten la abstracción en el intercambio de información entre diferentes nodos dentro de una red. La Capa de Transporte sería la encargada de brindar los servicios para el envío y la recepción de tramas mediante los medios físicos Ethernet y RS-232, en el primer caso bajo la semántica de los protocolos TCP/IP y UDP, y en el segundo caso cumpliendo con los requerimientos de las comunicaciones utilizando el puerto serie.

Para el desarrollo de la Capa de Transporte primeramente se realizó un estudio de las tecnologías y bibliotecas existentes para el envío y la recepción de tramas a través de diferentes medios físicos. De forma paralela se realizaron investigaciones y pruebas de concepto por diferentes integrantes de la Línea. El autor del presente material participó en la realización de muchas de ellas, específicamente las relacionadas con la biblioteca QtNetwork del Framework QT.

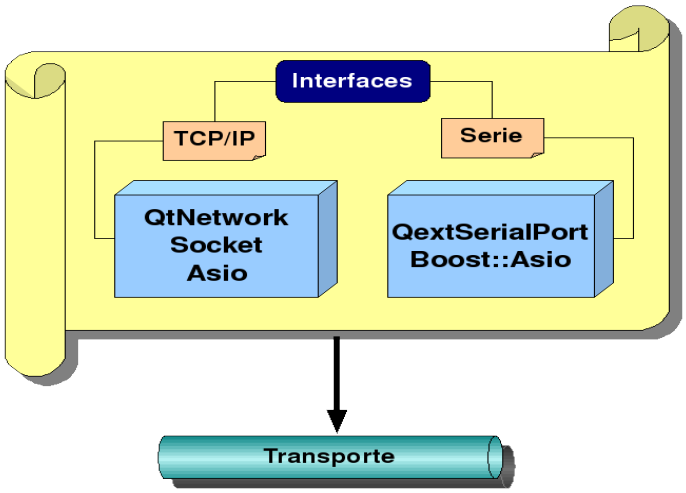

Figura 2.1 Bibliotecas de transporte.

Otras bibliotecas analizadas fueron Socket, Asio y QtExtSerialPort; cada una de ellas con sus peculiaridades, las dos primeras para transportes TCP y UDP, y la tercera para transporte serie. Se diseñaron un conjunto de pruebas con el objetivo de comparar los resultados obtenidos para cada una de las bibliotecas en cuanto a rendimiento, facilidad de uso, portabilidad, etc. De conjunto se decidió utilizar a las bibliotecas QtNetwork y QtExtSerialPort para la implementación de la interfaz definida para las primeras versiones de la Capa de Transporte.

Para el desarrollo de versiones posteriores el equipo de trabajo de la Línea de Manejadores decidió remplazar las bibliotecas QtNetwork y QtExtSerialPort por Boost::Asio. Diferentes razones motivaron a realizar dicha modificación, entre las más significativas podemos mencionar:

- La biblioteca Asio brinda la posibilidad de desarrollar un modelo asíncrono para la Capa de Transporte de forma sencilla y natural.
- A partir de la versión 1.35 la biblioteca Boost incluyó a la biblioteca Asio dentro de sus espacios de nombre (Boost::Asio), lo que demuestra el nivel de robustez y madurez de dicha biblioteca.
- Boost::Asio incorporó las funcionalidades para el manejo del puerto serie, evitando así el uso de una biblioteca adicional.

Actualmente la Capa de Transporte se distribuye en forma de biblioteca dinámica (.so ó .dll), es multiplataforma y por su bajo acoplamiento con otros módulos puede reutilizarse en el desarrollo de otras aplicaciones.

2.2- Capa de Protocolo

Las especificaciones de protocolos no solo tratan sobre la semántica de las tramas que se intercambian entre nodos de una red, sino también de los procedimientos para el uso de los mensajes. El tratamiento de los errores, los estados por los que puede transitar la comunicación, así como el modo de funcionamiento son aspectos que se deben tener presentes a la hora de implementar un protocolo determinado.

La Capa de Protocolo dentro de la arquitectura de los manejadores constituye el elemento lógico que representa la comunicación con los dispositivos de campo.

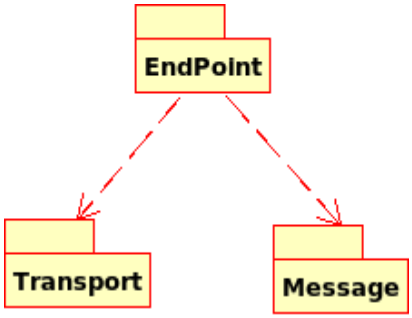

Figura 2.2 Paquetes de la Capa de Protocolos

En la **Figura 2.2** se muestra la arquitectura básica en forma de paquetes de la Capa de Protocolo. El paquete EndPoint rige la mecánica de funcionamiento de los protocolos, hace uso de los elementos del paquete Message para trabajar con la semántica de los mensajes, básicamente en cuanto al ensamblado y desensamblado de los mismos, y utiliza las funcionalidades que brinda la Capa de Transporte para el envío y la recepción de tramas a través del medio físico correspondiente.

En próximos epígrafes se explicará brevemente las decisiones tomadas en el desarrollo de los protocolos para el SCADA "Guardián del ALBA" en los que ha participado, de una forma u otra, el autor de este trabajo.

2.3- Capa de Implementación de la IGD

En la concepción de los manejadores para el SCADA "Guardián del ALBA" hay un conjunto de características y conceptos que son comunes para todos los controlares. Las abstracciones sobre los conceptos de variables, dirección de una variable, dispositivo, manejador, bloque de variables, etc; se encuentran implementados en un componente de software que se conoce a nivel de proyecto por el nombre DriversCore. El mismo consiste en un conjunto de clases, la mayoría de las cuales son abstractas, que tienen declaradas e implementadas las funcionalidades comunes para todos los manejadores, su desarrollo fue posible luego de un largo estudio por parte del líder de la Línea de Manejadores, el Doctor Rafael Trujillo, de las características que debían reunir los manejadores para el SCADA "Guardián del ALBA". A partir del DriversCore se desarrollan todos los manejadores, para ello, es preciso implementar funcionalidades y conceptos específicos para cada uno de los controladores. Algunos de los aspectos que se deben especificar son los siguientes:

- Establecer la forma de validar tanto la direcciones de las variables como las de los dispositivos.
- Establecer los criterios de comparación para las direcciones de las variables.
- Especificar el concepto de bloque de variables para el manejador que se esté desarrollando.
- Determinar la forma de conexión la Capa de Protocolo para establecer la comunicación con los dispositivos.
- Identificar los parámetros de configuración que son necesarios.
- Colocar el nombre por el que se identificarán los manejadores en la biblioteca resultante.

2.4- Demo

El dispositivo "Demo" y su correspondiente manejador fueron los primeros módulos que se desarrollaron en el ciclo de vida de SCADA "Guardián del ALBA". El objetivo era contar con un controlador para el acceso a un dispositivo virtual que simulara el comportamiento de algunos protocolos; y de esta manera probar las características de la IGD y su integración con las capas superiores del sistema se supervisión y control. El autor participó en la implementación tanto del dispositivo como del manejador "Demo".

El dispositivo virtual dispone de cuatro tipos de registros, discretos de entrada, discretos de entrada salida, analógicos de entrada y analógicos de entrada salida. Los registros discretos ocupan un byte de memoria y los registros analógicos ocupan una palabra de 16 bits. Los registros de entrada cambian su valor en el tiempo a partir de simulaciones realizadas por ecuaciones matemáticas que representan diferentes tipos de funciones, mientras que los registros de entrada salida mantienen de forma persistente la información depositada en ellos (4).

El manejador "Demo" realiza una implementación de la IGD y para el acceso a las variables del dispositivo "Demo" utiliza una API definida por las funciones *readMemory*, y *writeMemory***.** Es importante destacar que el manejador permite el acceso al dispositivo tanto de forma local como remota, utilizando para ello un transporte UDP implementado a partir de la biblioteca QtNetwork.

Para probar el funcionamiento del "Demo" se desarrolló una herramienta visual utilizando el Framework Qt, la misma permite configurar los parámetros del manejador, establecer el modo de funcionamiento (local o remoto), comenzar la comunicación con el dispositivo, obtener el estado de todos los registros, así como establecer valores en aquellas direcciones que pertenezcan a registros de entrada salida. La aplicación cuenta además con una vista que ofrece la posibilidad de graficar el comportamiento de las variables simuladas en el dispositivo.

El desarrollo del dispositivo, el manejador y la aplicación visual "Demo" cumplió con los objetivos que se perseguían, pues a partir de ese momento:

- Se contó con un prototipo para poner a prueba el enlace con la IGD.
- El código y la documentación del manejador "Demo" servirían como ejemplo para el desarrollo de futuros manejadores.
- Se demostró que los integrantes de la Línea de Manejadores del Equipo Cuba eran capaces de desarrollar manejadores para el SCADA "Guardián del ALBA".
- Los visitantes al Distrito Socialista y Tecnológico de Mérida presenciaron la primera aplicación funcional que ilustraba el inicio del lo que se lograría años más tarde.

2.5- Modbus

El protocolo Modbus fue creado por la empresa de tecnologías de automatización MODICON y constituye el estándar más usado dentro del mundo de las redes industriales.

Con el tiempo han surgido un gran número de variantes de este protocolo, entre las más conocidas se pueden mencionar: Modbus RTU, Modbus ASCII, Modbus TCP, Modbus UDP, Modbus PLUS, JBUS, etc.

Este epígrafe hace referencia al desarrollo de las variantes RTU y ASCII pertenecientes al modo de transmisión serie, y TCP del modo de transmisión Ethernet, en cuyo diseño e implementación participó el autor del presente material.

2.5.1- Protocolo Modbus

El protocolo Modbus permite el intercambio de datos con dispositivos de campo que se comunican utilizando este protocolo, para ello se establece un enlace Máster-Esclavo, donde el máster manipula toda la información. Los dispositivos Modbus organizan la información en cuatro bancos de memoria (Bobinas, Entradas Discretas, Registros de Entrada, Registros de Entrada/Salida), y para acceder a ella es necesario el envío de diferentes solicitudes asociadas a códigos de funciones con diferencias en los formatos de las tramas, siempre dependiendo de la variante en cuestión.

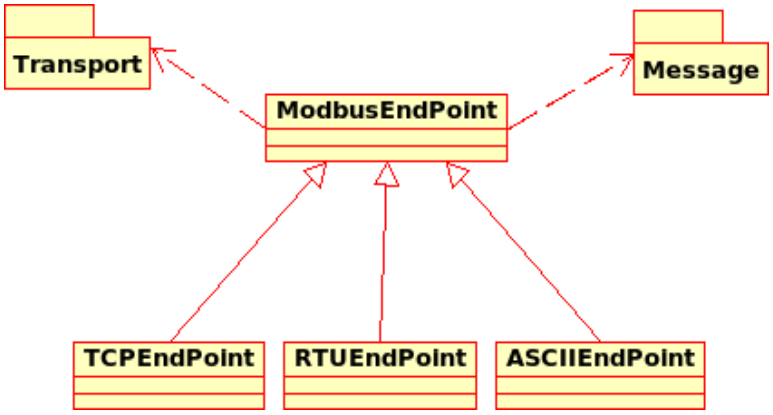

Figura 2.5 Diseño del protocolo Modbus

La **Figura 2.5** muestra en términos generales el esquema de diseño de la Capa de Protocolo Modbus que se utilizó para su desarrollo, la clase ModbusEndPoint agrupa las funcionalidades que son comunes para las tres variantes, por ejemplo el modo de funcionamiento de encuesta-respuesta, las funciones asociadas y algunos parámetros de configuración para hacer posible la comunicación con los dispositivos. Por su parte las clases TCPEndPoint, RTUEndPoint y ASCIIEndPoint se encargan de los elementos específicos, por ejemplo la creación del transporte correspondiente dependiendo del medio físico que utilicen y el ensamblado de las tramas utilizando la capa Message.

2.5.2- Manejador Modbus

El manejador Modbus en las tres variantes mencionadas fue el primer controlador desarrollado para la comunicación con un dispositivo real para el proyecto SCADA "Guardián del ALABA". Las variantes RTU, ASCII y TCP fueron implementadas en un mismo módulo de manejadores, es decir, como resultado del desarrollo del manejador para el protocolo Modbus se obtendría una biblioteca dinámica que contaría con la implementación de las tres variantes mencionadas.

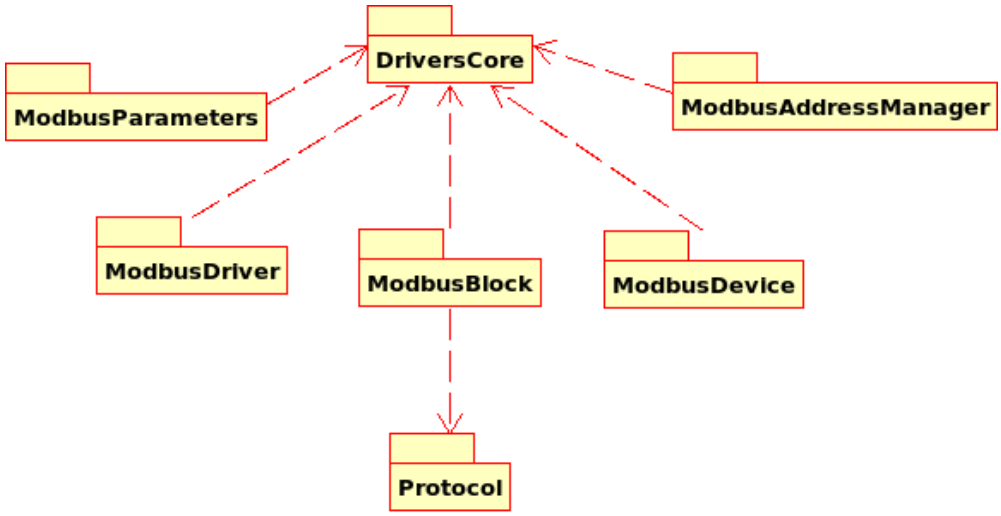

Figura 2.5.2 Diseño del Manejador Modbus.

En la **Figura 2.5.2** se exponen los paquetes relacionados con el diseño de las variantes implementadas del manejador Modbus para el SCADA "Guardián del ALBA". El paquete ModbusAddressManager se encarga del trabajo con las direcciones modbus que son configuradas desde el sistema de supervisión y control; primeramente se realiza la validación de las mismas, por convenio, una variable modbus se considera válida si cumple con el siguiente formato:

- Coils: 0:N
- Inputs: 1:N
- Inputs Registers: 2:N
- Holdings Registers: 3:N

Donde los valores de **N** representan la referencia a partir de la cual se desea acceder a la memoria de los bloques. El paquete ModbusAddressManager establece además los criterios de comparación para las direcciones modbus, los que están dados por el bloque de memoria al que corresponden la variable y por su ubicación dentro del mismo, este último aspecto está determinado por el valor de **N.**

El paquete ModbusBlock sintetiza los elementos del concepto de bloque de variables modbus para el SCADA "Guardián del ALBA". Para que dos variables modbus pertenezcan a un mismo bloque deberán pertenecer al mismo banco de memoria y su "distancia" no debe sobrepasar la cantidad de bytes permitidos en una transacción, éste elemento, todavía relacionado con las direcciones, es responsabilidad del paquete ModbusAddressManager, pero define a las variables que formarán parte de los bloques. ModbusBlock es el paquete encargado de realizar las lecturas y escrituras de las variables pertenecientes a los bloques que se formen con las variables configuradas, para cumplir con dicha funcionalidad este paquete hace uso de las clases implementadas en la Capa de Protocolo, que son realmente, las encargadas de acceder a los dispositivos físicos.

Los paquetes ModbusDevice, ModbusAdress y ModbusParamenters definen a los dispositivos, manejadores y parámetros modbus respectivamente. En estos paquetes las principales actividades que se realizan son la validación de las direcciones de los dispositivos modbus, las que para considerarse válidas deberán cumplir con las exigencias convenidas para las diferentes variantes, y la configuración de los parámetros necesarios para la comunicación y el funcionamiento de los manejadores resultantes.

2.6- Ethernet/IP

Ethernet/IP es un protocolo de red en niveles, apropiado al ambiente industrial. Es el producto acabado de cuatro organizaciones que aunaron esfuerzos en su desarrollo y divulgación para aplicaciones de automatización industrial: La Open DeviceNet Vendor Association (ODVA), la Industrial Open Ethernet Association (IOANA), la Control Net International (CI) y la Industrial Ethernet Association (IEA) (5). Gran parte de los sistemas de automatización de la empresa petrolera venezolana PDVSA son controlados con PLC ControlLogix de la firma Allen Bradley, por tal motivo surgió la necesidad de desarrollar un manejador para la comunicación con este tipo de dispositivos, el autor de este trabajo participó en la toma de decisiones de diseños importantes para el desarrollo del mismo, fue parte del equipo de trabajo que implementó las pruebas de conceptos, así como el manejador en su conjunto.

2.6.1- Protocolo Ethernet/IP

EtherNet/IP proporciona un modelo productor / consumidor para el intercambio de información de control crítica en el tiempo. El modelo productor / consumidor permite el intercambio de información entre un dispositivo emisor y varios dispositivos receptores sin la necesidad de que se envíe el mismo bloque de datos varias veces a diferentes destinos (5).

Desde el punto de vista de diseño la representación del protocolo se realizó a partir de la definición de los paquetes Ethernet y CIP.

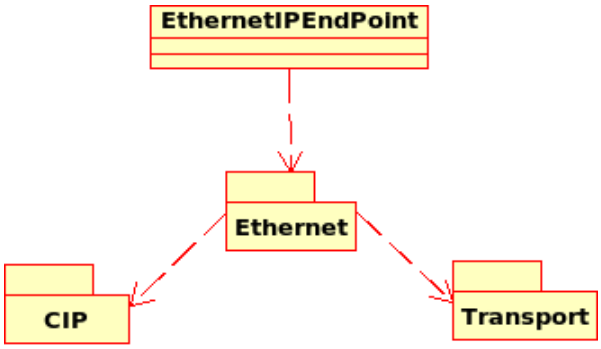

Figura 2.6.1 Diseño del protocolo Ethernet/IP

El paquete Ethernet se encarga del encapsulamiento de CIP, este último es un protocolo orientado a objetos que proporciona conexiones entre dispositivos industriales y controladores de alto nivel, es independiente del medio físico de transmisión de datos y orientado a conexión, asignado identificadores para las mismas (5).

Como muestra la **Figura 2.6.1** la clase EthernetEndPoint hace uso del paquete Ethernet para obtener las funcionalidades referentes a la semántica de los mensajes Ethernet/IP, tales como el ensamblado y desensamblado teniendo en cuenta la especificación del protocolo industrial abierto, que es un dialecto de Ethernet/IP creado por Allen Bradley para acceder a las variables configuradas en sus controladores a través de nombres simbólicos de cadenas de caracteres ASCII o "tags".

2.6.2- Manejador Ethernet/IP

La **Figura 2.6.1** muestra los principales paquetes en los que se agrupan las elementos que forman el diseño de clases del manejador Ethernet/IP.

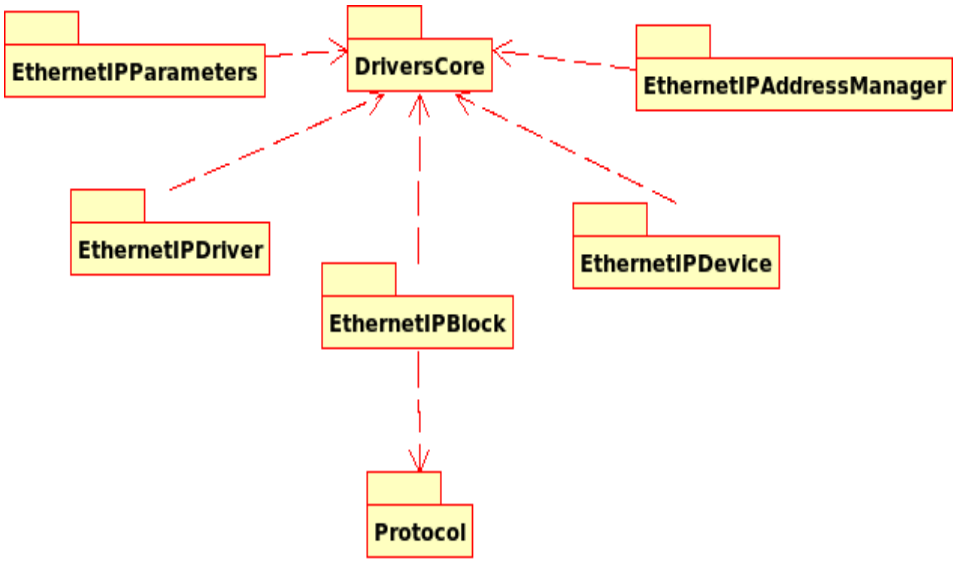

Figura 2.6.2 Diseño del manejador Ethernet/IP

Dentro de los aspectos más importantes de la Capa de Implementación de la IGD se encuentran los temas relacionados con los "tags" y su validación. Cada tag es un nombre simbólico por el cual se accede a la información de las variables configuradas en los dispositivos, su longitud no sobrepasa los 40 caracteres y en dependencia de su alcance se clasifican en globales y locales, tienen un tipo de dato asociado que determina las operaciones que se pueden realizar sobre ellos, y pueden agruparse para formar estructuras que funcionan como entidades independientes.

El autor participó directamente en el diseño e implementación de cada uno de los componentes que se desarrollaron alrededor del manejador Ethernet/IP. Más adelante se referencian diferentes artículos y documentos que contienen información detallada de los manejadores Modbus y Ethernet/IP, analizados brevemente en este material.

3- Analizador de tramas

Una de las principales actividades en el manejo y puesta a punto de un sistema SCADA es el mantenimiento y la detección de fallas. Un SCADA comprende todas aquellas soluciones de aplicación que se encargan de la captura de información de un proceso o planta, para que, con esta información, sea posible realizar una serie de análisis o estudios con los que se pueden obtener valiosos indicadores que permitan una retroalimentación sobre un operador o sobre el proceso. Durante este proceso surgen problemas eventuales en los dispositivos, o en las redes de comunicación, que provocan, con relativa frecuencia, que las variables configuradas no muestren correctamente su valor en los despliegues. La detección de la naturaleza y el lugar exacto del fallo puede ser una operación costosa que exija incluso salidas no programadas del SCADA. Para dar solución a esta problemática surge la idea del desarrollo de una herramienta para realizar un monitoreo constante del tráfico a través de la red y la recolección al igual que el reporte estadístico de datos importantes para conocer el estado de las comunicaciones de un sistema SCADA con los dispositivos del campo (6).

Tomando como punto de partida los argumentos relacionados en el párrafo anterior surge el Analizador de Tramas para Sistemas SCADA, más conocido como ***Sniffer***, y así lo llamaremos en el resto de este documento. El autor del presente material participó desempeñando roles de desarrollador y documentador en el proceso de desarrollo de esta herramienta, que está dirigida principalmente a los mantenedores del SCADA "Guardián del ALBA".

3.1- Tecnologías y funcionalidades

La **Figura 3** muestra las tecnologías que se utilizaron en el desarrollo del Sniffer. C ++ como lenguaje de programación, el entorno de desarrollo Eclipse, Qt para el desarrollo de componentes gráficos y ICE en el módulo de comunicación con el sistema de supervisión y control.

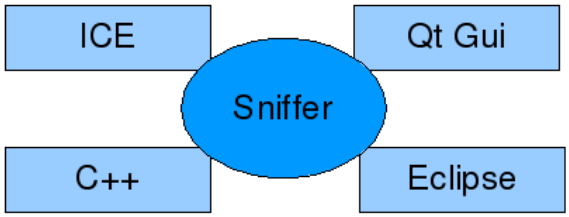

Figura 3.1 Tecnologías para el desarrollo del Sniffer.

Debido a que las tecnologías escogidas para el desarrollo son multiplataforma y están estandarizadas, la aplicación final puede ser utilizada en diferentes arquitecturas y sistemas operativos, esta característica de portabilidad resulta de mucho valor para gran parte de los usuarios. Los requerimientos de robustez y eficiencia exigidos por el cliente, fueron algunos de los elementos que influyeron en la elección principalmente de C++ como lenguaje de programación, y de ICE como mecanismo en la implementación del módulo que se encarga de establecer el flujo de datos entre el Sniffer y el SCADA.

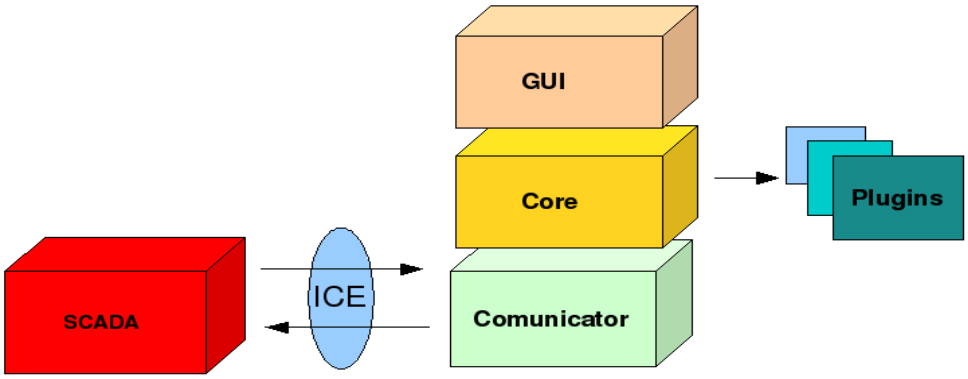

Figura 3.2 Arquitectura del Sniffer.

El Analizador de Tramas posee una interfaz gráfica que permite al usuario, de una forma amigable, realizar las siguientes operaciones:

- Establecer comunicación con el sistema SCADA.
- Comenzar o detener la captura de tramas asociadas al flujo de datos entre el SCADA y los dispositivos de campo.
- Obtener diferentes vistas de las tramas, en las que se ofrece información detallada

relacionada con el origen, la hora de captura, el protocolo al que pertenecen, el evento que las generó, la composición en bytes y en algunos casos una especificación sobre la semántica de las mismas.

- Realizar filtrado de las tramas por protocolos, dispositivos y eventos.
- Almacenar en un fichero las tramas capturadas para realizar análisis "off-line".

El Sniffer posee un sistema de plugins para realizar la interpretación de la semántica de los mensajes. Los plugins para el Analizador no son más que bibliotecas de carga dinámica con una interfaz bien definida que permiten el análisis de las tramas. Por cada manejador del SCADA es necesario desarrollar un plugin para la interpretación de las tramas asociadas al protocolo implementado, de ésta forma el Sniffer podrá brindarle al usuario una información más detallada sobre la estructura interna de cada paquete asociado a dicho protocolo.

Resultados

Como parte importante del ciclo de desarrollo de los módulos y herramientas tratadas en este material se encuentran las actividades de investigación, pruebas de concepto, análisis de tecnologías, interacción con los clientes, entre otras; como resultado de las mismas se realizaron varios trabajos que fueron presentados en diferentes eventos tanto a nivel nacional como internacional, los más relevantes, así como los premios alcanzados se muestran en la Tabla 1.

Trabajos		
Título del trabajo	**Evento**	**Premio**
Framework para el desarrollo de manejadores	Jornada Científica a nivel de Universidad	Relevante
Analizador de Tramas para Sistemas SCADA	Jornada Científica a nivel de Universidad	Relevante
Framework para el desarrollo de manejadores	Concurso Nacional de Computación	Relevante
Analizador de Tramas para Sistemas SCADA	Fórum Provincial	Relevante
Interfaz Genérica para los Manejadores de Dispositivos en el Proyecto SCADA PDVSA	Evento Internacional FIE 2008	Publicación del artículo
Manejador Ethernet/IP para los PLC Controllogix en el Proyecto SCADA PDVSA	Evento Internacional FIE 2008	Publicación del artículo

Tabla 1 Trabajos premiados en eventos.

La Tabla 2 hace referencia a diferentes pilotos instalados en 10 plantas pertenecientes a 8 estados de la hermana República de Venezuela. Los buenos resultados obtenidos en las pruebas realizadas avalan el desempeño de los productos desarrollados por los integrantes de la Línea Manejadores de Dipositivos.

Pilotos					
Planta	**Ubicación**	**Fecha de Instalación**	**Comunicación con el Campo**		
			Señales	**Equipamientos**	**Drivers SCADA**
PDT Bajo Grande	San Francisco-Edo. Zulia	Dic-08	120	Allen Bradley PLC 5/40E	ModbusRTU
Planta Compresadora Altagracia	Altagracia de Otituco-Edo. Guárico	08	Por verificar	Por verificar	Por verificar
AIT-Barinas	Localidad Campo de Mesa-Edo Barinas	Ene-09	Por verificar	Por verificar	ModbusRTU Ethernet-IP ABEthernet
Complejo Jusepin	Localidad Jusepin-Edo Monagas	Sep-08	Por verificar	Modbus TCP vía Terminal Server	ModbusTCP ModbusRTU
Tren de pruebas y flujo total , Makolla K203	División Faja Distrito Morichal	Oct-08	600	PLC Modicon 3, Gateway Telemecanique 2	ModbusRTU
Estación de flujo Muri	Localidad de Pinta Mata, Dto Norte-Edo Monagas	Sep-08	Por verificar	Por verificar	ABEthernet
Estación de flujo Orocual	Localidad Orocual, Dto Norte-Edo Monagas	Sep-08	Por verificar	ControlLogix con tarjeta Profoft Modbus TCP	ModbusTCP
José	Puerto La Cruz	Oct-08	570	Por verificar	ModbusTCP ModbusRTU
Patio de Tanques Silvestre	Localidad San Silvestre-Edo Barinas	Ene-09	Por verificar	Por verificar	ABEthernet
Patio de Tanques Pta de Palmas	Punta de Palmas	Dic-08	372	PLC Modicom Quantum	ModbusTCP ModbusRTU

Tabla 2 Pruebas pilotos en plantas venezolanas.

Por último es importante destacar, que el conjunto de productos analizados en este trabajo han aportado al país un monto de 959 550 dólares, pactados en diferentes documentos en formas de anexos pertenecientes al Convenio Marco PDVSA – ALBET.

Conclusiones

Las herramientas y módulos de software analizados en este material constituyen una plataforma de componentes reutilizables para el desarrollo y el mantenimiento de nuevos manejadores de dispositivos. La empresa petrolera de Venezuela cuenta hoy con un conjunto de controladores para la comunicación con los dispositivos de campo existentes en sus instalaciones. Se cuenta además con una aplicación para realizar actividades de mantenimiento mediante el análisis de los datos que intercambia el Sistema de Supervisión y Control con los dispositivos industriales, así como mediante el chequeo del estado de las conexiones con los mismos.

Referencias

1. Herrera*, Moisés. Recolección y Manejadores en el Guardián del ALBA. 2008.*
2. *ISO 7498-1:2004, Organización Internacional de Normalización.* 2004.
3. Trujillo, *Rafael Arturo*. *Interfaz Genérica de los Manejadores de Dispositivos, versión 4.2.* Enero 2009.
4. Trujillo, *Rafael Arturo*. *Guía de Implementación del Manejador Demo.* 2007.
5. Trujillo, *Rafael Arturo*; Cedeño Pozo, *Antonio*; García Hernández, *Luis Enrique*; Pérez Pérez, *Yasmany*. *Manejador Ethernet/IP para los PLC Controllogix en el proyecto SCADA PDVSA. 2008*
6. Trujillo, *Rafael Arturo*. *Especificación de Requerimientos de Software e Interfaces Públicas del Sniffer.* 2008

Anexos

Como material de apoyo y aval del presente material a continuación se relacionan anexos firmados como parte de los convenios PDVSA – ALBET:

Primer Convenio Marco PDVSA-ALBET, S.A

Anexo 13. Desarrollo del Subsistema de Drivers del SCADA Nacional.
Anexo 31. Proyecto de desarrollo del Subsistema de Drivers del SCADA Nacional versión 2.

Segundo Convenio Marco PDVSA-ALBET, S.A

Anexo 14. Proyecto de Extensiones al subsistema de Drivers de la versión 2.0 del Guardián del ALBA.