Implementación de LogMein para controlar de manera remota un variador de velocidad Cuttler Hammer

LogMein Implementation to control in a remote way a speed variator Cuttler Hammer

Henry Camargo[1], Camilo Arrieta[2], Cindy Vergara[2], Iván García[2], Faustino Pulido[2]

1. Especialista en Informática y Telemática, Pedagogía para Desarrollo del Aprendizaje Autónomo, Ing. Sistemas, Tecnólogo en Electrónica y Comunicaciones. Universidad Autónoma del Caribe. Grupo de investigación IET-UAC. Email: henry.camargo@uac.edu.co, hcamargoa@yahoo.com
2. Estudiantes Noveno Semestre de Ingeniería Electrónica y Telecomunicaciones. Universidad Autónoma del Caribe. Barranquilla, Atlántico. Grupo de investigación IET-UAC.

Recibido 3/05/2010, Aceptado 31/08/2010

RESUMEN

En este documento se presenta una explicación minuciosa acerca de una aplicación de acceso remoto de telecomunicaciones para ejercer control a un sistema variador de velocidad de motores de la marca CUTTLER-HAMMER, utilizando el software LogMeIn para facilitar la conectividad desde un computador cliente con interfaz gráfica en una estructura de cliente-servidor en una red privada, hacia otra red privada donde se encuentra el dispositivo variador de velocidad adosado al computador servidor, ubicada en cualquier lugar del planeta utilizando como medio INTERNET en forma segura; todo lo anterior se plantea con el objetivo de que los receptores asimilen objetivamente el modo de operación y las ventajas que representa LogMeIn como es el factor seguridad, entre otras.

Palabras clave: DNS, FCDRIVE, IP, HTTPS, LogMeIn, SSL, TCP, UDP, Variador de Velocidad

ABSTRACT

In this document presents a deep explanation about a telecommunication remote access aplication to control a CUTTLER-HAMMER's speed variator for motors, using the LogMeIn software in order to facilitate the conection from a client computer, with a graphic interface, in a structure client-server in a private network to another private network where remains the speed variator device, conected to server PC in any place of the planet through the INTERNET in a safe way. The above information is proposed to make the receptors understand objectively the operation mode and advantages which LogMeIn represents, such as the security factor, among others.

Key words: DNS, FCDRIVE, IP, HTTPS, LogMeIn, SSL, TCP, UDP, Adjustable Frequency Drives.

1. Introducción

Las tecnologías de la información y la comunicación, TIC, han incursionado a nivel mundial y en particular en la industria Colombiana, para permitir la gestión de procesos a distancia, lo cual le da versatilidad, sencillez y sensación de ubicuidad al control ejercido desde cualquier lugar del planeta, al permitir la captura, transporte almacenamiento y procesamiento de información, utilizando el paradigma cliente-servidor y la Internet. Organizaciones con centenares de oficinas dispersas en una amplia área geográfica esperan tener la posibilidad de examinar en forma habitual el estado actual de todos los dispositivos y elementos implicados en los procesos de producción, simplemente oprimiendo una tecla. A medida que crece nuestra habilidad para recolectar procesar y distribuir información, la demanda de procesamientos más sofisticados crece de manera acelerada.

En vista de la necesidad de desarrollar experiencias que impliquen la ejecución de control sobre máquinas en ambientes cableados o inalámbricos, se ejecuta el control de manera remota de un variador de velocidad, mediante el software de escritorio o acceso remoto LogMeIn, aclarando conceptos relacionados con el tema, tales como, los protocolos en los que se basa el funcionamiento del arreglo y caracterizando de manera general la forma en la cual se afecta cada etapa de la comunicación cuando se emplean estas herramientas.

LogMeIn una suite de servicios de software, que provee acceso remoto a computadores sobre Internet, tiene varias versiones del producto, profesional y de help desk, este último de uso libre, por lo cual se decide usar para esta experiencia particular, en la ejecución de aplicaciones a distancia; en este caso para controlar un variador de velocidad, que se encuentra conectado a un ordenador por el puerto serial, a través de otro computador localizado en una ubicación geográfica diferente, y cuyo canal de comunicación es la red de internet.

El dispositivo que se maneja remotamente (CUTTLER-HAMMER SV9000) es capaz de monitorear y manipular características mecánicas y eléctricas de un motor asíncrono de corriente alterna y es maniobrado por un PLC que controla la electrónica de potencia de manera local por acción de un teclado de programación o utilizando un computador con la aplicación FCDRIVE, que es una interfaz gráfica propia del Cuttler-Hammer SV9000, para administrar el dispositivo por el puerto serial.

2. Metodología

2.1 Dispositivo

Se escoge como dispositivo a controlar el Variador de Velocidad Cutler-Hammer SV9000, debido a que su desarrollo permite generar una gran diversidad de aplicaciones industriales, por lo que la posibilidad de su manejo remoto se traduce en facilidades de monitoreo y manipulación de los elementos electrónicos y/o eléctricos asociados a él.

2.2 Conexión

El intercambio de información entre el ordenador y el variador de velocidad se realiza mediante una conexión serial a través del protocolo RS-232.

Figura 1. Conexión cable serial entre ordenador y variador
Figure 1. Serial cable connection between computer and device.

2.3 Software

El variador de velocidad SV9000 se puede colocar en funcionamiento utilizando el software FCDRIVE, usando la interfaz gráfica para monitorear, configurar, apagar y encender el motor asíncrono de corriente alterna.

Se instala el software LogMeIn en la computadora en la cual se encuentra conectado el dispositivo a controlar, creando así una cuenta de usuario y activando el programa en cuestión para ese equipo. Luego se ingresa por el navegador web a la página www.logmein.com en el equipo localizado en la ubicación remota, y se suministra el nombre de usuario y contraseña de la computadora a la que está conectado el variador de velocidad.

3. Descripción de la aplicación

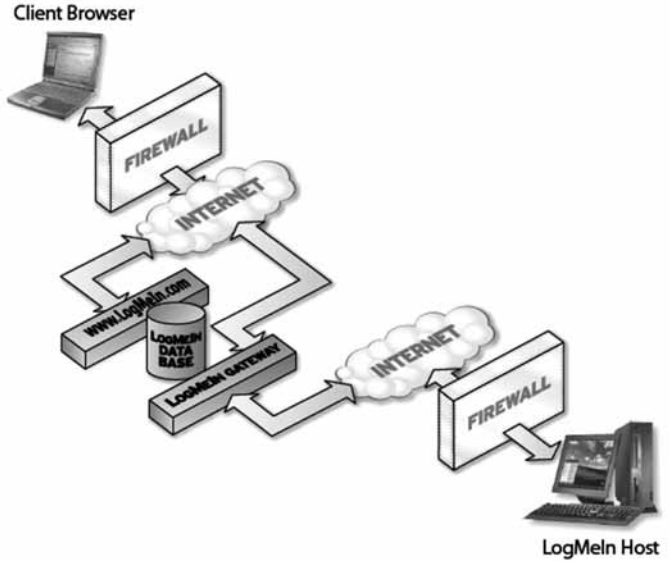
En la arquitectura general de LogMeIn, hay tres entidades que participan en cada sesión de acceso remoto. El "cliente" o "Usuario" para acceso a un recurso remoto, el "anfitrión" o "host" que es el equipo al que se accede, y el "gateway" que es la pasarela a través de la cual se presta el servicio de LogMeIn, y regula el tráfico entre el cliente y el host. LogMeIn ha sido diseñado para permitir el acceso remoto seguro a recursos críticos a través de una red insegura, tal como lo es Internet. En cuanto a las especificaciones técnicas, la aplicación LogMeIn utiliza el puerto 443/TCP, el puerto de acceso remoto 2002, y el puerto 80 para el protocolo de hipertexto, http; y en cuanto al ancho de banda, en modo de inactividad, LogMeIn genera alrededor de 200

bytes por minuto en cada equipo de destino. Simplemente hace un "ping" al Gateway para controlar si el equipo con LogMeIn está encendido y conectado en línea. Para conectarse y no usar el control remoto es suficiente una conexión de Internet (Siempre Encendido). Para una sesión de control remoto se recomienda un mínimo de 10 KB / s (KB, no Kb). El control remoto depende mucho de la resolución de la pantalla y profundidad de color, pero 10-12KB debería ser suficiente. Más de 30-40KB debería ser rápido [1].

Analizando la figura 2, se puede observar que el cliente debe establecer la conexión ingresando a www.logmein.com y autenticarse así mismo con la cuenta creada en el Host. También es evidente que antes de formarse la conexión de igual a igual o peer-to-peer entre cliente y servidor, se crea una comunicación entre el host y el servidor de LogMeIn, y entre el cliente y el servidor de LogMeIn; los parámetros o protocolos que se emplean para las conexiones nombradas anteriormente se explicarán a continuación [2].

La familia de protocolos del modelo TCP/IP [3] [4] que utiliza el arreglo implementado se describe a continuación.

Figura 2. La arquitectura de red establecida por LogMeIn.
Figure 2. The network architecture provided by LogMeIn



Tomado de: http://www.infosecurityproductsguide.com/technology/2007/wp_lmi_security.pdf

3.1 Capa de aplicación

LogMeIn utiliza el protocolo de aplicación http porque, tal como se había explicado con anterioridad, el cliente necesita emplear el navegador web para poder acceder remotamente al host conectado al dispositivo a controlar y autenticarse con la cuenta creada por tal host; en síntesis, el protocolo de hipertexto es el encargado de cada transacción web en el proceso de enlace entre el cliente y el host.

Por otra parte, otro protocolo de la capa de aplicación empleado en todo este proceso es el DNS dinámico, por permitir la asignación de un nombre de dominio de Internet a un computador con dirección IP variable, lo que permite conectarse con el equipo en cuestión sin necesidad de tener que rastrear la dirección IP del mismo. LogMeIn asigna nombres de dominio a las computadoras desde las cuales se instala su software y se crean cuentas de usuario, más precisamente, a la dirección IP del host al cual se quiere acceder remotamente le es asignado un nombre de dominio por el servidor DNS de LogMeIn.

3.2 Capa de transporte

La aplicación LogMeIn trabaja tanto con el protocolo de control de transmisión (TCP) como con el protocolo de datagramas de usuario (UDP). UDP se emplea para establecer la conexión entre el servidor de LogMeIn con el cliente y con el host, es decir que desde cada uno de ellos se envía un código o dato encriptado al servidor para que se pueda dar la comunicación, al realizar una especie de "Handshaking" para poder establecer finalmente la conexión entre el cliente y el host al cual se desea acceder remotamente mediante TCP dado que este es orientado a la conexión, y para que el acceso remoto sea posible ambos equipos deben estar conectados en red [5].

En cuanto al código de encriptación mencionado en el párrafo anterior, primero se debe explicar la manera en la que la aplicación LogMeIn cifra la información que está siendo transmitida o intercambiada por las partes a través de los protocolos SSL y/o TLS, siendo este último la segunda versión del primero; estos protocolos funcionan entre las capas de aplicación y transporte, a continuación se realizará una breve descripción de cada uno de ellos.

3.2.1 Secure Socket Layer (SSL)

Según [6], el protocolo SSL es un sistema diseñado y propuesto por Netscape Communications Corporation. Se encuentra en la pila OSI entre los niveles de TCP/IP y de los protocolos HTTP, FTP, SMTP, etc. Proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, típicamente el RC4 o IDEA, y cifrando la clave de sesión de RC4 o IDEA mediante un algoritmo de cifrado de clave pública, típicamente el RSA. La clave de sesión es la que se utiliza para cifrar los datos que vienen del servidor seguro y van a él. Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea encontrada por un atacante en una transacción dada, no sirva para descifrar futuras transacciones.

Proporciona cifrado de datos, autenticación de servidores, integridad de mensajes y, opcionalmente, autenticación de cliente para conexiones TCP/IP. Cuando el cliente pide al servidor seguro una comunicación segura, el servidor abre un puerto cifrado, gestionado por un software llamado Protocolo SSL Record, situado encima de TCP. Será el software de alto nivel, Protocolo SSL Handshake, quien utilice el Protocolo SSL Record y el puerto abierto para comunicarse de forma segura con el cliente.

3.2.2 Protocolo SSL Handshake

Durante el protocolo SSL Handshake, el cliente y el servidor intercambian una serie de mensajes para negociar las mejoras de seguridad. Este protocolo sigue las siguientes seis fases (de manera muy resumida):

La fase Hola, usada para ponerse de acuerdo sobre el conjunto de algoritmos para mantener la intimidad y para la autenticación.

La fase de intercambio de claves, en la que intercambia información sobre las claves, de modo que al final ambas partes comparten una clave maestra.

La fase de producción de clave de sesión, que será la usada para cifrar los datos intercambiados.

La fase de verificación del servidor, presente sólo cuando se usa RSA como algoritmo de intercambio de claves, y sirve para que el cliente autentique al servidor.

La fase de autenticación del cliente, en la que el servidor solicita al cliente un certificado X.509 (si es necesaria la autenticación de cliente).

Por último, la fase de fin, que indica que ya se puede comenzar la sesión segura.

3.2.3 Protocolo SSL Récord

El Protocolo SSL Récord especifica la forma de encapsular los datos transmitidos y recibidos. La porción de datos del protocolo tiene tres componentes:

MAC-DATA, el código de autenticación del mensaje.

ACTUAL-DATA, los datos de aplicación a transmitir.

PADDING-DATA, los datos requeridos para rellenar el mensaje cuando se usa cifrado en bloque.

3.2.4 TLS (Transport Layer Security)

Definido en el RFC 2246, es un protocolo para el establecimiento de una conexión segura entre un cliente y un servidor. TLS (Transport Layer Security) [7] es capaz de autenticar el cliente y el servidor y la creación de una conexión cifrada entre los dos. TLS es un reemplazo para Netscape anteriores SSL (Secure Sockets Layer). El TLS (Transport Layer Security) el protocolo es extensible, lo que significa que nuevos algoritmos pueden añadirse para cualquiera de estos fines, siempre y cuando tanto el servidor, como el cliente son conscientes de los nuevos algoritmos. Existen muchos protocolos de uso de TLS (Transport Layer Security) para establecer conexiones seguras, incluyendo HTTP, IMAP, POP3 y SMTP.

3.2.5 Protocolo TLS Handshake

El protocolo TLS Handshake primero negocia un intercambio de claves utilizando algoritmo asimétrico, como RSA o Diffie-Hellman. El protocolo TLS Registro comienza abre un canal cifrado mediante un algoritmo simétrico como RC4, IDEA, DES o 3DES.

3.2.6 Protocolo TLS Registro

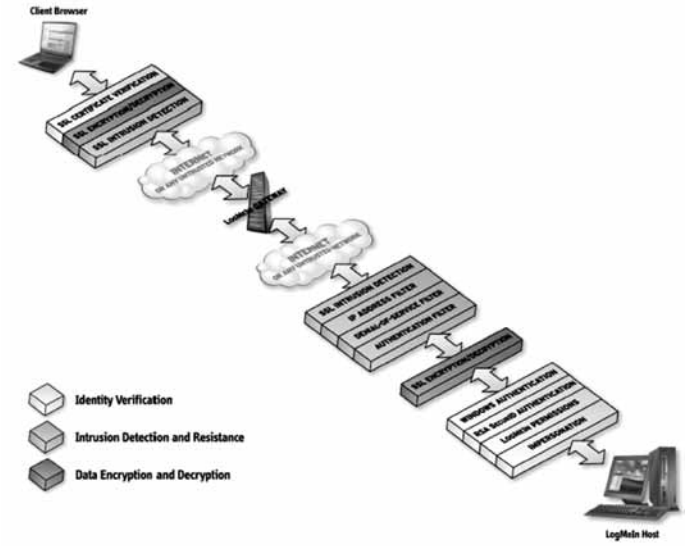
El protocolo TLS Registro también es responsable de garantizar que las comunicaciones no se alteren en tránsito. Algoritmos hash como MD5 y SHA se utilizan para este fin.

Una implementación libre de TLS, el proyecto OpenSSL es un conjunto de instrumentos no comerciales, en la aplicación de protocolos TLS (Transport Layer Security).

A continuación se muestra una imagen representativa, figura 3, de la autenticación entre el cliente y el host en las cuales participan los protocolos descritos en los párrafos anteriores.

Además de todo lo preliminar, también se debe citar que la conexión UDP que LogMeIn implementa, utiliza, traducción de direcciones de red transversal, NAT transversal, el cual además de basarse en el NAT convencional para el intercambio de paquetes entre dos redes que se asignan mutuamente direcciones incompatibles, (para el caso de LogMeIn específicamente entre el cliente y el ordenador al que se va a accesar remotamente ya que estos generalmente se encuentran ubicados en redes diferentes), consiste en encapsular los paquetes UDP para que pasen mejor a través de los firewalls.

Figura 3. Esquema de autenticación entre cliente y host.
Figure 3. Authentication scheme between client and host



Tomado de: http://www.infosecurityproductsguide.com/technology/2007/wp_lmi_security.pdf

3.3 Capa de red

En la capa de red, LogMeIn utiliza el protocolo de resolución de direcciones, ARP, porque es necesario para una comunicación segura, pero ¿como lo hace? Sencillo, como se sabe el protocolo ARP tiene como función principal obtener una dirección física o de acceso al medio, MAC de 6 bytes a partir de una dirección del protocolo de internet, IP [8].

Al momento de crear una cuenta, el sistema envía una petición ARP para obtener la dirección física del equipo en el cual se crea la cuenta. Esto se debe a que el equipo puede tener una IP dinámica, y la única forma que LogMeIn reconozca el equipo, es a través de la MAC. La MAC es almacenada en una base de datos del servidor LogMeIn, cuando activamos el programa en el equipo este envía al servidor la nueva IP del equipo, que no es reconocida inicialmente en la base de datos con un nombre de cuenta. LogMeIn envía nuevamente una petición ARP para ver cuál es la MAC del equipo con IP no reconocida. Luego de realizado este proceso LogMeIn obtiene la MAC del equipo, verifica si está en su base de datos, si es positivo la identifica con el nombre de su usuario y este equipo está disponible para ser controlado remotamente.

Este evento que ocurre en la capa de red solo es posible de esta forma si el servidor LogMeIn y el equipo pertenecen a la misma subred. Como normalmente el servidor y el equipo están en subredes diferentes se aplica Proxy-ARP, donde el router de la otra subred recibe la petición y este se encarga de difundir la información hasta el equipo correspondiente.

Considerando una red IP que usa Proxy-ARP, que esté dividida en subredes, interconectada por enrutadores, se usa el algoritmo de enrutamiento IP "antiguo", que significa que ningún host conoce la existencia de múltiples redes físicas. Si vemos los hosts A y B que están en diferentes redes físicas con la misma red IP y un router R entre las dos subredes, cuando un host A quiere enviar un datagrama IP a un host B, primero tiene que determinar la dirección de red física del host B usando el protocolo ARP.

Como el host A no puede diferenciar entre las redes físicas, su algoritmo de enrutamiento IP piensa que el host B está en la red física local y envía una petición ARP de broadcast (Difusión). El host B no recibe este broadcast, pero el router R sí.

El router R entiende de subredes, esto es, ejecuta la versión "subnet" del algoritmo de enrutamiento IP y será capaz de ver que el destino de la petición ARP (del campo de dirección de protocolo destino) está en otra red física. Si las tablas de enrutamiento del router R especifican que el próximo salto a esa otra red se hace a través de un dispositivo físico diferente, responderá a ARP como si fuera el host B, diciendo que la dirección de red del host B es la del mismo router R. El host A recibe esta respuesta ARP, la pone en su caché y enviará futuros paquetes IP para el host B hacia el router R. El router enviará tales paquetes a la subred correcta.

4. Descripción del dispositivo a controlar

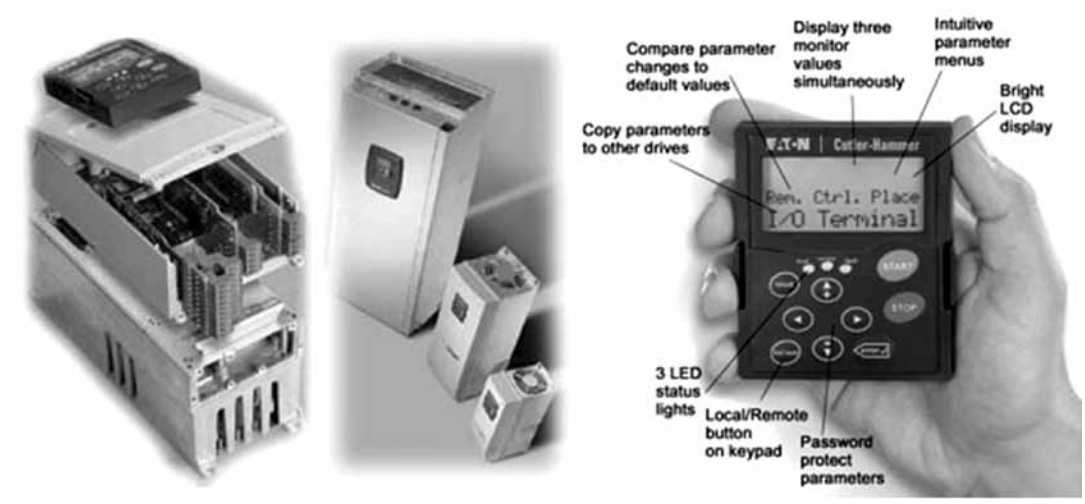
Para el desarrollo del proyecto se utilizó un modelo de demostración, o demo CUTTLER-HAMMERSV9000 que implementa un variador de velocidad [9], un motor junto con los pines de interrupción y su respectivo software para realizar el control remoto.

4.1.1 Dimensionado

Las condiciones de carga de su aplicación y la temperatura ambiente son los dos factores principales que más afectan al dimensionado correcto del accionamiento.

- Par de arranque
- Par variable
- Par constante
- Sobrecargas
- Temperaturas ambiente 40ºC, 45ºC y 50ºC
- Refrigeración: aire o agua
- Tamaño físico

Figura 4. CUTLER-HAMMER SV9000
Figure 4. CUTLER-HAMMER SV9000



Tomado de: http://www.galco.com/scripts/cgiip.exe/wa/wcat/webpromo2.htm?promo=110CHGPSVX9000

4.1.2 Prestaciones

La precisión de velocidad y de par, así como los tiempos de respuesta necesarios para su aplicación, determinan el tipo y el modo de control a utilizar.

- Control tensión-frecuencia
- Control vectorial en lazo abierto
- Control vectorial en lazo cerrado
- Precisión estática y dinámica de velocidad y par

4.1.3 Funcionalidad

Los requisitos específicos de la aplicación determinan el número de entradas y salidas, los principios de control y monitorización, y el software de aplicación adecuado.

- Integración en sistemas
- Lógica de control
- E/S ampliables
- Buses de campo
- Control de bombas y ventiladores
- Control PID
- Ajuste de parámetros
- Prestaciones de monitorización

4.1.4 Soporte técnico

La producción y otros procesos deben funcionar continuamente sin interrupciones 24 horas al día, 7 días a la semana.

- Soporte técnico
- Presencia local y global
- Servicio pos-venta 24/7
- Puesta a punto
- Unidades de intercambio
- Repuestos

4.1.5 Normas

Las instalaciones deben ser diseñadas y ejecutadas de acuerdo con las normas de seguridad, entre otras. El cumplimiento con las normas asegura que el variador funcione correctamente en el entorno especificado.

- Emisiones e inmunidad (EMC)
- RFI
- Corrientes y tensiones armónicas
- Directiva de baja tensión
- Directiva de máquinas
- Grado de protección (clases IP)
- Certificaciones CE, UL, C-UL y otras

4.1.6 Rapidez

Los pedidos deben ser entregados según el programa, especialmente en los proyectos.

- Calidad en producción
- Entrega a tiempo
- Logística eficiente

4.2 Aplicaciones del cutler-Hammer SV9000 [10]

Cuando se escoge una aplicación que corresponde a requerimientos específicos, el variador es mucho más fácil de ajustar. Todos los parámetros requeridos están dispo-

nibles, pero los parámetros que no son necesarios para la aplicación específica están ocultos. Para cada aplicación hay una ayuda de puesta en marcha que le guía a través del proceso de puesta en marcha y ajuste de parámetros. El variador también es capaz de identificar los parámetros de motor, facilitando aun más la puesta en marcha.

Todas las aplicaciones soportan buses de campo, los cuales permiten el acceso a todas las funciones y parámetros.

4.2.1 Aplicación básica

La aplicación básica es la más simple de las aplicaciones disponibles. Está pensada para una utilización sencilla donde haya una señal de referencia así como señales de Marcha/Paro externas y órdenes de dirección de marcha. Se necesita ajustar unos pocos parámetros dependientes del motor y de la aplicación.

4.2.2 Aplicación estándar

La aplicación estándar está pensada para casos donde la aplicación básica no sea suficiente. Las principales diferencias con la aplicación básica son la configuración de E/S y de fallos.

4.2.3 Aplicación Local/remoto

La aplicación Local/remoto está diseñada para casos donde el variador tenga que controlarse desde dos lugares distintos, típicamente uno local, cerca del motor, y el otro remoto desde una sala de control. La fuente de control se escoge mediante una E/S digital y es inequívoca en todo momento. Todos los parámetros relativos a la funcionalidad y el comportamiento general del variador también están disponibles.

4.2.4 Aplicación Multi-referencias de velocidad

La aplicación Multi-referencias de velocidad está diseñada para casos donde, entre una y tres entradas digitales, formen una consigna que defina la referencia de velocidad del variador.

Se pueden programar hasta 16 velocidades diferentes. Esta aplicación se usa típicamente en entornos donde el motor tenga que trabajar, de forma cíclica y repetitiva, a diferentes velocidades preseleccionadas, tales como aplicaciones en cintas transportadoras coordinadas, máquinas herramienta simples o posicionamiento simple.

4.2.5 Aplicación de control PID

La aplicación de control PID incluye un controlador PID interno.

Este controlador puede utilizarse para mantener alguna variable, típicamente presión o temperatura, en el punto deseado. La variable se mide, y si hay diferencia con el valor de referencia, la velocidad del motor cambia para llevar la variable hasta el valor correcto. El controlador PID también se puede utilizar con un sensor de velocidad externo para crear un lazo cerrado de velocidad simple.

4.2.6 Aplicación de control multi-propósito

La aplicación de control multi-propósito es la más flexible.

Proporciona acceso a todos los parámetros, a todas las E/S y da la posibilidad de crear funciones matemáticas utilizando una o varias entradas.

4.2.7 Aplicación de control de bombas y ventiladores con rotación

Esta aplicación está diseñada para controlar múltiples bombas y ventiladores conectados en paralelo. La idea es utilizar la cantidad de bombas/ventiladores requeridos para atender la demanda, utilizando el variador para controlar la velocidad de una bomba/ventilador y dar órdenes de arranque y paro a las otras bombas/ventiladores. La función de rotación permite igualar las horas de trabajo de todas las bombas/ventiladores del grupo, para su desgaste por igual.

4.3 Herramientas PC para variadores VACON

Existen una variedad de herramientas PC para hacer la utilización de los variadores de CA cutler-Hammer SVX lo más fácil y conveniente posible.

Las herramientas están pensadas para tareas tales como puesta a punto, monitorización, carga de las diferentes aplicaciones y programación de aplicaciones. El PC se conecta al variador mediante el RS232.

4.3.1 FCDrive

FCDrive es la herramienta de puesta a punto y monitorización para el cutler-Hammer SVX. Permite descargar y cargar parámetros entre el variador y el PC, comparar parametrizaciones, cambiar la aplicación activa, guardar en archivo e imprimir en papel parámetros y reportes de servicio, controlar el variador, ajustar referencias, operar el registrador de variables, y más.

También permite monitorizar simultáneamente hasta ocho variables escogidas por el usuario en un gráfico de tendencias en pantalla, y guardar el registro en el disco duro para un análisis posterior. En el Vacon NXP, también se puede operar el registrador de variables y comunicar a través de cutler-Hammer SVX bus con hasta 254 variadores.

Adicional a lo expresado anteriormente, se debe recalcar que como este dispositivo se conecta al PC para ser manejado por software a través de cable serial, es decir, que emplea el protocolo RS-232 para el envío de órdenes desde el ordenador al variador y viceversa, los pines del conector DB9 que se emplean para el intercambio de información PC-SV9000 son los de recepción RX (pin 2), transmisión TX (pin 3) y el de tierra GND (pin 5), conexión de modem nulo sin control de flujo.

5. Resultados

Para mostrar explícitamente lo logrado a través de la utilización de LogMeIn, es necesario dar a conocer el diagrama de la red que hace posible controlar de manera remota a través de ordenadores cualquier clase de dispositivos conectados a ellos, en este caso el variador de velocidad CLUTTER-HAMMER SV9000. La Figura 5 representa lo anterior.

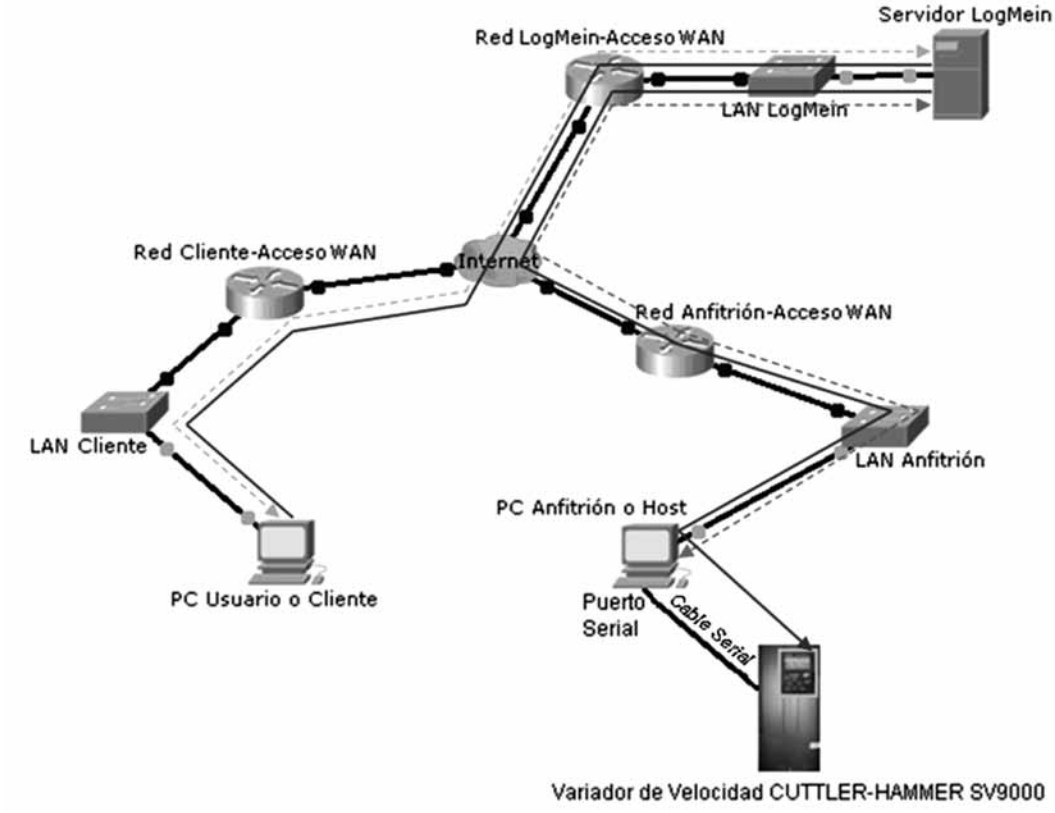
En la Figura 5, las líneas punteadas representan el proceso de autenticación descrito en el item 3, e ilustrado en la Figura 2, con la diferencia de que en aquella imagen no se presentaba el dispositivo a controlar ni tampoco los dispositivos de red necesarios para acceder a la Internet (Acceso a WAN) como son los Routers, que también funcionan como cortafuegos o firewalls, y los Switches que son los encargados de "extender la red". Por otra parte la línea continua azul simboliza la información necesaria para controlar el variador cuya interacción con las capas del modelo de referencia fueron resumidas en los ítems 3.1, 3.2 y 3.3.

6. Conclusiones

- Un sistema bien diseñado como solución de acceso remoto puede aumentar la productividad y proporcionar un rápido retorno de la inversión de una empresa. Cuando la implementación se hace con cuidado y con la utilización de las características de seguridad opcional de LogMeIn, los beneficios superan con creces los riesgos.

- Muchos sistemas operativos incluyen algún tipo de solución de acceso remoto de forma predeterminada. Windows 2000 y 2003 Server, por ejemplo, ofrecen una simple interfaz de administración remota, donde las consideraciones de seguridad NO siempre han prevalecido sobre las preocupaciones de uso.

Figura 5. Diagrama de red para controlar el CUTTLER-HAMMER SV9000.
Figure 5. Network diagram to control the CUTTLER-HAMMER SV9000.



- La aplicación de LogMeIn se ajusta más a los requerimientos académicos en comparación con otros software para acceso remoto, tales como Team viewer, ya que emplea el protocolo de hipertexto (HTTP), que permite la navegación WEB para el acceso remoto.

- La ventaja obvia de utilizar la puerta de enlace o pasarela, LogMeIn en lugar de establecer un vínculo directo entre el cliente y el host, es que uno, o ambos, de estas últimas entidades pueden ser cortafuegos. Al utilizar la puerta de enlace garantiza que los usuarios no tienen que preocuparse sobre la configuración del firewall.

- Es recomendable utilizar un ancho de banda adecuado, entre los pares, para que la transferencia de archivos en la conexión sea lo más próxima al tiempo real.

- Se presentan inconvenientes al momento de crear más de una cuenta en el mismo equipo (cuando se desinstala y se vuelve a instalar el programa); debido a que en la base de datos del servidor LogMeIn, ya se encuentra almacenada la dirección MAC de ese ordenador y se produce un error en la identificación de la IP.

6. Referencias

[1] LogMeIn, Inc Simply Connected (2003-2010) *GettingStartedGuide LogMeIn pro²* [internet], <https://secure.logmein.com/ES/documentation/pro2/Pro2_GettingStartedGuide.pdf>

[2] LogMeIn, Inc Simply Connected (2003-2010) *LogMeIn pro² Security* [internet], <https://secure.logmein.com/documentation/Security/wp_lmi_security.pdf>

[3] Andrew S. Tanenbaum (1997), Redes de Computadoras, En: *La Capa de transporte*, p. 532.

[4] Olifer Natalia, Olifer Victor (2009), Redes de Computadoras. En: *Interconexión de Redes TCP/IP,* p. 530-558.

[5] Kioskea (es.kioskea.net). (2008) *Criptografía - Secure Sockets Layers (SSL)* [internet], 16 de octubre de 2008, http://es.kioskea.net/contents/crypto/ssl.php3, Acceso [9 de Marzo de 2010]

[6] Datatracker.ietf.org, *Transport Layer Security (tls)* [internet], <http://www.ietf.org/dyn/wg/charter/, Acceso [8 de Octubre de 2009] tls-charter.html>

[7] Olifer Natalia, Olifer Victor (2009), Redes de Computadoras. En: *Protocolos Principales de la pila TCP/IP,* p. 615-631.

[8] Behrouz A. Forouzan (2002), Transmisión de Datos y Redes de Comunicaciones. En: *Conjunto de Protocolos TCP/IP,* p. 682, 695 y 696.

[9] Cutler-Hammer SV9000 Manual, [Internet] Disponible en: http://www.frankmachinery.com/docs/drives/sv9000.pdf, Acceso [20 de Octubre de 2009]

[10] CUTLER-HAMMER AC DRIVES, [Internet] Disponible en: http://www.galco.com/scripts/cgiip.exe/wa/wcat/webpromo2.htm?promo=110CHGPSVX9000, Acceso [20 de Octubre 2009]