UNIVERSIDAD DEL AZUAY

Maestría en Telemática

"Estudio de las tecnologías de redes de área extendida (WAN) para su aplicación en sistemas de supervisión, control y adquisición de datos (SCADA, Supervisory Control and Data Acquisition)"

Trabajo de graduación previo a la obtención del título de Magister en Telemática

Autor: Marcelo Enrique García Rodas.

Director: Ing. Francisco Salgado.

Cuenca, Ecuador

2008

AGRADECIMIENTOS.

Mi agradecimiento a aquel que vela mis sueños y orienta mis despertares. A mi familia, colaboradora incondicional de mis causas y a todas las personas que permanecen a mi lado en cada aventura y desventura.

INDICE

RESUMEN

El desarrollo de esta tesis se centra en el estudio de las necesidades que tiene cada uno de los diversos tipos de sistemas SCADA en cuanto a su adquisición de datos, comunicación a distintos niveles de operación y la manera en como ellos pueden ser interconectados entre sí; sistemas desarrollados en escenarios de área extendida en los que se hace uso de tecnologías WAN para el transporte de datos, consiguiendo el mejor desempeño y obteniendo la mayor eficiencia con los protocolos recomendados para cada caso, además se desarrolla el planteamiento de topologías que refuercen la seguridad de los sistemas para hacerlos menos vulnerables a ataques externos e inclusive internos.

Al final de este trabajo monográfico se presenta una pequeña aplicación en forma de prototipo para exponer en breves rasgos el uso y la implementación de tecnologías WAN y su comportamiento con una de las redes más extendidas en el mundo, como lo es el protocolo IP, con un soporte para transporte de datos en tiempo real a cargo del protocolo UDP.

ABSTRACT

This thesis focuses on the study of the necessities of SCADA systems in terms of data acquisition, communication in all operational levels, and the way they interconnect with each other; systems that have been developed in wide area locations by using WAN (Wide Area Network) technologies for data transportation and getting the best performance and reliability in each case at the same time. Furthermore, this thesis analyzes the most reliable topologies to get obtain a better security behavior of SCADA systems.

At the end of this document, a small prototype application is displayed. This prototype will be used as demonstration in small scale of SCADA systems functioning with WAN technologies.

INTRODUCCIÓN.

La implementación de sistemas automatizados que asistan al ser humano en la ejecución de tareas ha alcanzado un nivel de complejidad que corresponde únicamente al crecimiento exponencial que ha tenido la tecnología en general en estas últimas décadas, esta ha dado como consecuencia una considerada dificultad en mantener estos sistemas bajo control y monitoreados adecuadamente, de manera que junto a ellos surgieron los sistemas de supervisión, control y adquisición de datos (SCADA por sus siglas en ingles de Supervisory Control and Data Adquisition).

Por otra parte, el crecimiento industrial se ha extendido hasta llegar a implementar procesos en lugares remotos dispersos de su estación central, debido a sus requerimientos operacionales, como es el caso los sistemas de captación de aguas para su distribución a las urbes o en el caso de una empresa que decide expandirse e instalar una nueva planta industrial en otra ciudad para abaratar sus costos hacia el cliente. En estos casos los administradores de estos sistemas SCADA necesitan mantener el control, monitoreo y conseguir registros de sus niveles de producción, para esto se echa mano de tecnologías de comunicaciones bien conocidas que se extienden sobres áreas amplias, las llamadas tecnologías WAN (Wide Area Network).

A pesar de que en los últimos años se han desarrollado ayudas para implementaciones de sistemas SCADA en redes amplias, mediante la creación de protocolos o dispositivos dedicados, lamentablemente las redes WAN, en su desarrollo, no han considerado el tipo de estructuras necesarias para los requerimientos particulares de los sistemas SCADA, dejando pasar por alto falencias como fallas de seguridad o un incorrecto dimensionamiento de las redes. Es por eso que en el desarrollo de esta tesis se pretende dar pautas que ayuden a la implementación de sistemas SCADA que se desplieguen sobre áreas extendidas manteniendo la seguridad, eficiencia y confiabilidad en la transmisión de sus datos con las redes WAN.

1. LOS SISTEMAS SCADA.

En la actualidad, en la industria se puede encontrar un sin número de sistemas automatizados desarrollando tareas de fabricación y manufactura, sistemas diseñados para traer al mundo las facilidades con las que contamos para nuestro diario vivir. Desde la revolución industrial estos procesos de fabricación han sufrido una evolución acelerada que, como es lógico, va de la mano con los adelantos tecnológicos que se han venido dando.

A medida que estos sistemas automatizados fueron creciendo se fue haciendo necesario mantener sus tareas bajo supervisión de manera que se pueda controlar el proceso de producción. En un inicio esta tendencia en supervisión y control de los procesos automatizados era la que cada fabricante debía resolver por sí solo valiéndose de un departamento de desarrollo dedicado, es decir eran implementaciones propietarias de cada empresa y dedicadas a procesos específicos dependiendo de las tareas que tuviera para realizar dicha empresa. Con este constante crecimiento de los sistemas automatizados las soluciones de supervisión y control dedicadas fueron requiriendo de más tiempo para su implementación y su puesta en marcha se hacía cada vez más complicada, además del hecho de que por ser tecnologías dedicadas quedaban obsoletas cuando se incorporaban nuevas herramientas en los procesos de fabricación. De tal manera que como consecuencia lógica a este problema nacen nuevas tecnologías de supervisión y control que puedan ser programables, actualizables y se acoplen a cada aplicación industrial. A estas herramientas se las conoce actualmente con el nombre genérico de sistemas de supervisión, control y adquisición de datos o SCADA (Supervisory Control and Data Acquisition) por sus siglas en inglés.

1.1. Definición y partes de un sistema SCADA.

Los sistemas SCADA son un conjunto de aplicaciones de hardware, controladores, interfase hombre-máquina, redes, comunicaciones y software que permiten monitorear y controlar desde un centro de gestión los procesos de cualquier tipo de tarea. Para llevar a cabo el monitoreo se necesita inicialmente realizar la adquisición de datos desde los puntos en donde se efectúa el proceso, mediante sensores que capturan los parámetros de operación y los transmiten con unidades remotas o RTU (Remote Terminal Unit) hacia un centro de control y monitoreo en donde los datos recogidos pueden ser interpretados, con la ayuda de una interface hombre – máquina (HMI, por sus siglas en inglés), por un operador o administrador del sistema. El control es realizado mediante actuadores que se encargan de llevar a cargo los procesos mismos de la empresa, estos reciben a manera de comandos, órdenes de ejecución transmitidas desde el centro de control por los mismos medios de comunicación que se realiza el monitoreo.

En base a estos conceptos se puede decir que los tres componentes principales de un sistema SCADA son [1]:

- Múltiples unidades terminales remotas para los dispositivos de campo, sensores o actuadores.
- Una o varias estaciones de control y monitoreo en las que residen los aplicativos HMI.
- La infraestructura de comunicación, que puede ser una red LAN en el caso de que los procesos sean desarrollados en una misma localidad o una WAN para cuando se piensa extender el sistema entre varias localidades.

En la solución SCADA regularmente se tiene como unidades terminales remotas a elementos de control programable o PLC (Programable Logic Control), los cuales son capaces de realizar el control y monitoreo de procesos mediante el uso de algoritmos

programados inicialmente antes de la puesta en funcionamiento del dispositivo. Mediante ellos es posible enviar reportes periódicamente de sus sensores hacia cualquier centro de control o ejecutar comandos sobre los dispositivos que tiene a su mando.

Estos elementos de control pueden operar de manera autónoma, entre varios de ellos o mediante la asistencia de un centro de control maestro para facilitar una implementación SCADA. Es posible también que existan varios centros de control distribuidos, cada uno encargado de un subsistema de procesos y comunicados entre sí. Cuando el sistema SCADA tiene esta última configuración es llamado sistema de control distribuido o DCS (Distributed Control System). Y también es posible la combinación de los sistemas, de tal manera que un SCADA puede tener en algún sector un DCS y el resto ser administrado por un solo centro de control, como es el caso de las empresas de generación y distribución eléctrica en las que las distintas subestaciones tienen su control autónomo, de tal manera que están configuradas como DCS, pero todas ellas se reportan hacia un solo centro de control ubicado en la planta generadora y que es parte de un sistema SCADA propio de esa planta.

La "Estación Maestra" hace referencia a los servidores con el software necesario para comunicarse con el equipo del campo (RTU's, PLC's, etc.) y en estos servidores se encuentra el programa HMI corriendo para las estaciones de trabajo en el cuarto de control o en cualquier otro lado. En un sistema SCADA pequeño, la estación maestra puede estar en un solo computador mientras que a gran escala la estación maestra puede incluir muchos servidores, aplicaciones de software distribuido, mecanismos de respaldo de la información y sitios de recuperación de desastres [1].

El sistema SCADA usualmente presenta la información al personal operativo de manera gráfica, en la forma de un diagrama de procesos, esto significa que el operador puede ver un esquema que representa la planta que está siendo controlada. Por ejemplo un dibujo de una bomba conectada a la tubería puede mostrar al operador cuanto fluido

está siendo bombeado desde ella a través de la tubería en un momento dado y el operador puede cambiar el estado de la bomba a apagado en caso de necesitarlo. El software HMI mostrará el promedio de fluido en la tubería disminuyendo en tiempo real. Estos diagramas de representación pueden consistir en gráficos de símbolos esquemáticos que muestren los elementos de cada parte del proceso o pueden consistir en fotografías digitales de los equipos sobre los cuales se animan las secuencias [1].

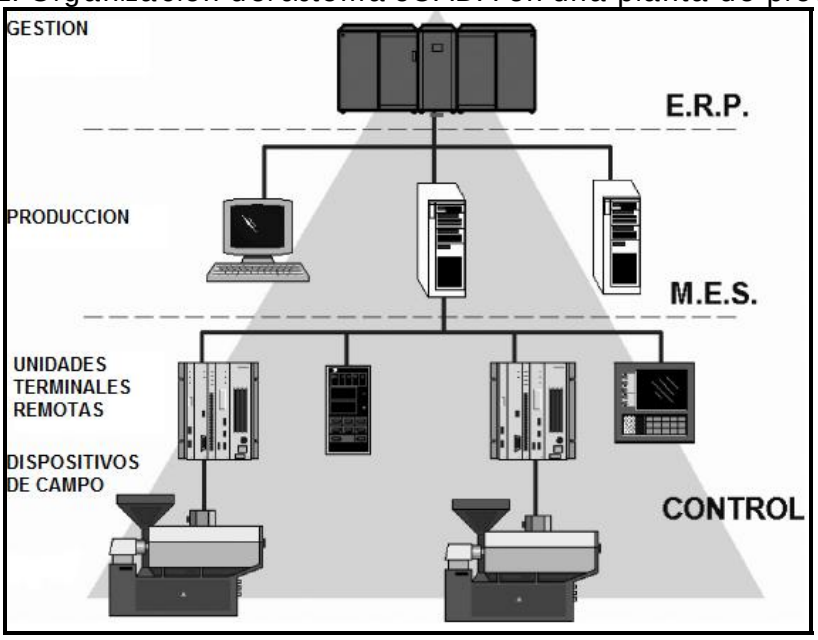
El paquete HMI para el sistema SCADA típicamente incluye un programa de dibujo, el cual los operadores o el personal de mantenimiento del sistema usa para configurar la manera en que los procesos son representados en la interface. Esta representación puede ser tan simple como una barra indicadora del nivel o tan complejo como una pantalla que muestre varios procesos y en cada uno de ellos la opción de abrir una nueva ventana con la descripción estadística de sus sucesos.

Además, los paquetes HMI tienen asociado un módulo de programación que sirve a los usuarios para la implementación lógica de los procesos por medio de algún lenguaje de programación, que por lo general es propio del fabricante. Mediante este módulo se ingresan líneas de código que determinarán el comportamiento de cada uno de los objetos representados en el interfaz gráfico.

Los reportes de los eventos recogidos por las estaciones remotas son transportados hacia la estación central por un medio de comunicación que puede ser del tipo inalámbrico o mantener una topología tipo bus mediante un cableado por toda la localidad en la que se desarrollan los procesos a controlar. Generalmente el medio utilizado para el transporte de los datos dentro de una red para un sistema SCADA depende de la naturaleza de los procesos a ser gestionados y obviamente de las facilidades para la implementación de los medios de transmisión (En el capítulo 3 se describe las arquitecturas de red más convenientes para mantener comunicados los distintos niveles de un sistema SCADA).

Los componentes de los sistemas SCADA que se han descrito, son comúnmente organizados dentro de un esquema de operaciones que facilita la implementación y gerenciamiento de estas redes. Aunque existe una leve variación de la división de estos sistemas, en general, se lo puede organizar como se muestra a continuación [2]:

Figura 1.1. Organización del sistema SCADA en una planta de producción.



Fuente: Sistemas de visualización industrial [2]

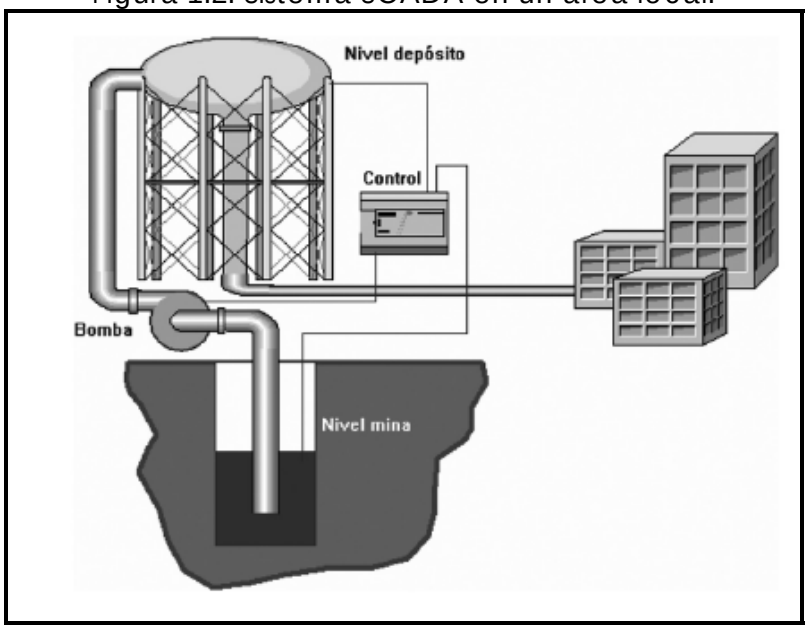
- Nivel de control. Está conformado por los elementos de campo como sensores, actuadores y RTU's. En este nivel se realiza toda la parte de automatización y control de procesos.
- Nivel MES (Manufacturing Execution System). En este nivel el sistema se encarga de realizar el monitoreo y control de los procesos así como la gestión de la calidad, gestión de la producción, mantenimiento y optimización de procesos.
- Nivel ERP (Enterprise Resource Planning). En este nivel, de gestión de recursos empresariales, se realiza el gerenciamiento y administración del sistema SCADA, en el se llevan a cabo las finanzas, compras, ventas y logística necesaria para el normal funcionamiento de todos los procesos.

1.2. Clasificación de los sistemas SCADA por el área geográfica en la que trabajan.

Los sistemas SCADA fueron diseñados inicialmente con el objetivo de realizar el monitoreo, control y mantenimiento de plantas industriales o procesos de producción, de tal manera, que su alcance estaba sustentado por una red de datos industrial de área local, en la actualidad con el desarrollo tecnológico y por ende el crecimiento industrial, estos sistemas han llegado a ser implementados para realizar control y monitoreo de procesos que se desarrollan en varios sitios de una ciudad, país o inclusive a nivel internacional, por lo tanto, pueden estar clasificados, de manera similar a las redes de comunicaciones, por el área geográfica en la que se desempeñan.

De tal manera que puede haber sistemas SCADA que tienen su campo de acción sobre un área local, como por ejemplo las plantas de manufacturación o de procesos de producción en los que por lo general se conecta la maquinaria encargada de la producción hacia un centro de control mediante un cableado industrial. Estas redes tradicionalmente han funcionado con el estándar RS-485 en una arquitectura de red tipo bus, característica de este medio de transmisión. En la figura a continuación se muestra un ejemplo de una planta de producción con su conexión hacia un nodo central que sirve como estación de monitoreo y control del sistema SCADA implementado.

Figura 1.2. Sistema SCADA en un área local.



Fuente: Sistemas de visualización industrial [2]

En la actualidad, la comunicación entre las máquinas encargadas del proceso de producción y el nodo central de monitoreo puede ser realizada con estándares de comunicación más modernos y con mejores prestaciones, como el Ethernet o Fast Ethernet, con algunas pequeñas modificaciones en los parámetros de funcionamiento para su desempeño óptimo en medios industriales (Industrial Ethernet), como se verá más adelante.

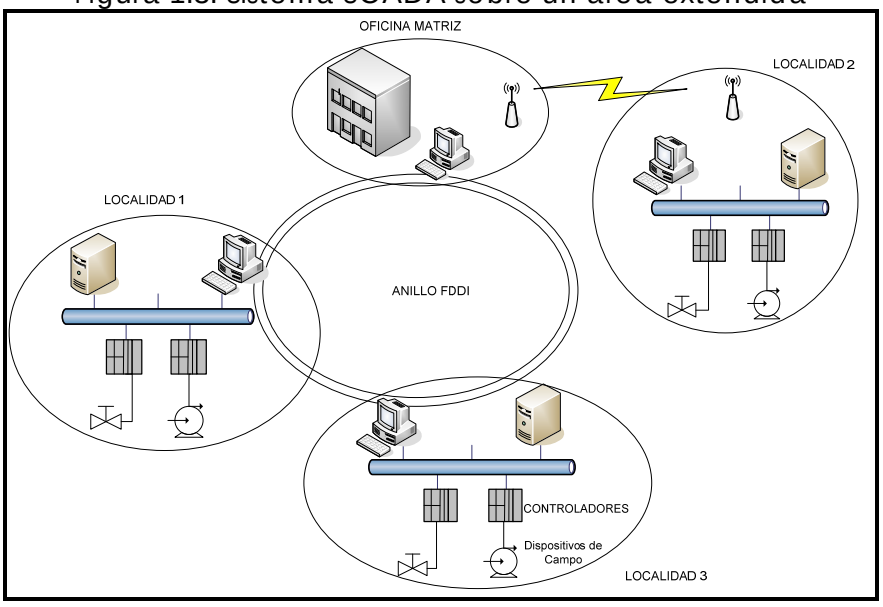
Con el advenimiento de nuevas y mejores tecnologías, tanto en medios de transmisión como en dispositivos de control y monitoreo, las empresas que se extendían en territorios más amplios que una única localidad empezaron requerir de sistemas de control y monitoreo que funcionen en todos sus emplazamientos de producción y que a la vez se encuentren comunicados entre sí de alguna manera. Esto, con el objeto de administrarlos desde un solo centro de control general, y en algunos casos con más de uno, para poder generar redundancia y mantener cierto nivel de seguridad. En el despliegue de estas implementaciones, los medios de transmisión con los que se

pasarían los reportes hacia un nodo central pasaron a ser una cuestión primordial, por lo que se tuvo que considerar tecnologías de comunicación de área amplia WAN (Wide Area Network) con probada seguridad y fiabilidad.

Con el uso de tecnologías de transmisión de redes WAN se puede facilitar uno o varios centros de control en donde se tenga los detalles de los distintos procesos de cada localidad y a la vez se mantenga un aceptable nivel de confiabilidad en los datos transmitidos. En los capítulos posteriores se verá cuales son los inconvenientes que se presentan en estas redes para los sistemas SCADA.

Los sistemas SCADA pueden ser extensibles para empresas que tienen un campo de acción nacional o inclusive internacional. En este caso se construye una estructura de comunicación de tipo distribuido DCS, en la que existe un centro de gestión en cada una de las localidades responsables de los distintos procesos de producción, con todos los elementos propios de un sistema SCADA y por otro lado se tiene una oficina matriz con una estación de monitoreo en la que se registran los reportes de los distintos centros de gestión, con la información necesaria, únicamente para conocer los rangos de producción y con privilegios limitados o completamente nulos para tomar acciones en los procesos mismos, como lo sería en un nivel ERP.

Figura 1.3. Sistema SCADA sobre un área extendida



Fuente: Tecnologías WAN para sistemas SCADA, Ing. Marcelo García R.

1.3. Protocolos comúnmente utilizados por los sistemas SCADA.

La comunicación e interacción entre maquinas y dispositivos monitoreados y controlados por medio de un sistema SCADA se realiza en la industria por medio de estándares abiertos de comunicación, para facilitar la integración de distintos dispositivos o inclusive distintos sistemas integrales y de esta manera evitar las soluciones tipo isla tanto a nivel de automatización como de tecnologías de la información. Para lograr esto se requiere que en la empresa se tenga un sistema de comunicación que permita:

- Un flujo de información desde los sensores encargados de la adquisición de los datos y de los actuadores hasta el nivel de gestión de la empresa.

- Disponibilidad de la información en cualquier punto.
- Suficiente capacidad en el canal de información para que la información fluya de manera rápida entre la planta y la unidad de gestión de la empresa.
- Configuración simple y homogénea con eficientes funciones de diagnóstico.
- Funciones de seguridad integradas que eviten accesos no permitidos.

Para obtener esta solución de tipo global se requiere el uso de estándares que presenten herramientas útiles para soluciones específicas del tipo industrial en cada uno de los niveles de operación (Nivel ERP, Nivel MES y Nivel de campo) y que a su vez sean compatibles entre cada nivel a pesar que funcionen en distintas áreas de la empresa. De tal manera que para conseguir un sistema global, homogéneo y funcional en cuanto al flujo de información se usan más comúnmente los siguientes estándares de comunicación:

1.3.1. MODBUS.

MODBUS es un protocolo de comunicaciones situado en el nivel 7 del Modelo OSI, basado en la arquitectura maestro/esclavo o cliente/servidor, diseñado en 1979 por Modicon para su gama de controladores lógicos programables (PLCs) y convertido en un protocolo de comunicaciones estándar de facto en la industria. Este protocolo es el que goza de mayor disponibilidad para la conexión de dispositivos electrónicos industriales y en la actualidad es todavía uno de los más usados en sistemas SCADA [4]. Las razones por las cuales se popularizó el uso de MODBUS sobre otros protocolos de comunicaciones son:

- Es público
- Su implementación es fácil y requiere poco desarrollo
- Maneja bloques de datos sin suponer restricciones.

La especificación Modbus/TCP define un estándar interoperable en el campo de la automatización industrial, el cual es simple de implementar para cualquier dispositivo que soporta sockets9 TCP/IP [3]. MODBUS permite el control de una red de dispositivos, por ejemplo la gestión de un sistema de medida de temperatura y humedad que comunica sus resultados a un ordenador. MODBUS también se usa para la conexión de un ordenador de supervisión con una unidad remota (RTU) en sistemas de supervisión adquisición de datos (SCADA). Existen versiones del protocolo MODBUS para puerto serie y Ethernet (MODBUS/TCP). MODUS en su implementación puede ser encontrado en dos modos distintos:

MODBUS ASCII. Este formato usa una representación legible del protocolo en el formato ASCII (American Estándar Code for Information Interchange) para la trasmisión de sus datos. Este formato es útil y práctico pero menos eficiente, debido a que el protocolo envía dos caracteres ASCII por cada byte que se genera como información y este modo se permiten intervalos de tiempo de hasta un segundo entre caracteres durante la transmisión sin que se generen errores [4].

MODBUS RTU. Usa una representación binaria compacta de los datos en los bytes que se transmiten entre un centro de control (Maestro) y los dispositivos de campo (Esclavos). El flujo de bits es continuo a diferencia del formato ASCII [4], esto hace que la transmisión de los datos en modo RTU sea más efectiva con la misma tasa de baudios.

Ambas implementaciones del protocolo son serie. El formato RTU finaliza la trama con una suma de control de redundancia cíclica (CRC), mientras que el formato ASCII utiliza una suma de control de redundancia longitudinal (LRC). La versión Modbus/TCP usa el formato RTU, pero además usa TCP/IP para su transmisión entre estaciones. Por medio de TCP/IP, MODBUS consigue trabajar sobre redes WAN, ampliando de esa manera su utilidad.

MODBUS Plus (MODBUS+ o MB+). Es una versión extendida del protocolo que permanece como propietaria de MODICON. Dada la naturaleza de la red precisa un coprocesador dedicado para el control de la misma. Con una velocidad de 1 Mbps en un par trenzado sus especificaciones son muy semejantes al estándar EIA/RS-485 aunque no guarda compatibilidad con este.

Cada dispositivo de la red MODBUS posee una dirección única en la red inclusive si está extendida sobre una red WAN. Cualquier dispositivo puede enviar órdenes MODBUS, aunque lo habitual es permitirlo sólo a un dispositivo maestro y el resto a manera de esclavos solo responden peticiones. Cada comando MODBUS contiene la dirección del dispositivo destinatario de la orden. Todos los dispositivos reciben la trama pero sólo el destinatario la ejecuta (salvo un modo especial denominado "Broadcast"). Cada uno de los mensajes incluye información redundante que asegura su integridad en la recepción de esta manera se asegura su transmisión dado que por ser un protocolo de naturaleza de tiempo real no puede realizar reenvío en caso de pérdida de paquetes.

Existe gran cantidad de módems que aceptan el protocolo MODBUS, inclusive algunos están específicamente diseñados para funcionar con este protocolo. Además, existen implementaciones para conexión por cable, wireless, SMS o GPRS. En la implementación de este protocolo inicialmente se usaba RS-232 por lo que la mayoría de problemas presentados en la red se presentaban en la latencia y la sincronización de los datos, sin embargo actualmente se pueden usar otros estándares para las capas inferiores, como Ethernet por ejemplo, dando así más fiabilidad a la transmisión de bits.

1.3.2. PROFIBUS.

PROFIBUS (por sus siglas en inglés de *Process Field Bus*) es un popular estándar de bus de campo. Se trata de una red abierta, estándar e independiente de cualquier fabricante que cuenta con varios perfiles y se adapta a las condiciones de las aplicaciones de automatización industrial para la transmisión de datos de los dispositivos de automatización tales como PLC, PC, HMI, sensores u actuadores. Este estándar fue desarrollado en el año 1987 por las empresas alemanas Bosch, Klöckner Möller y Siemens, en 1989 la adoptó la norma alemana DIN19245 y fue confirmada como norma europea en 1996 como EN50170. En la actualidad es reconocida como la normativa IEC 61158/EN 50170 [5] y esta sienta además las bases para garantizar la proyección de futuro de sus inversiones ya que se permite ampliar con componentes conformes a las instalaciones existentes.

Este protocolo trabaja con nodos maestros y nodos esclavos, los nodos maestros se llaman también activos y los esclavos pasivos. PROFIBUS soporta una gran variedad de equipos que van desde PC´s y PLC´s hasta robots, pasando por todo tipo de elementos de campo y puede ser utilizado en la mayoría de las aplicaciones industriales gracias a las tres posibilidades que ofrece para la configuración de una red de monitoreo y control: FMS (Field bus Message Specification), DP (Decentralize Periferia) y PA (Process Automation), es decir desde máquinas sencillas, pasando por aplicaciones a nivel de célula hasta nivel de proceso con PROFIBUS-PA.

Las características relevantes del estándar PROFIBUS son [6]:

- Velocidades de transmisión: 9.6, 19.2, 93.75, 187.5 y 500 KBaudios.
- Número máximo de estaciones: 127 (32 sin utilizar repetidores).
- Distancias máximas alcanzables (cable de 0.22 mm. de diámetro): hasta 93.75 KBaudios: 1200 metros 187.5 KBaudios: 600 metros 500 KBaudios: 200 metros.
- Estaciones pueden ser activas (maestros) o pasivas (esclavos).

- Conexiones de tipo bidireccionales, multicast o broadcast.

PROFIBUS puede aplicarse, entre otras, en las siguientes áreas:

- Automatización manufacturera.
- Automatización de procesos.
- Automatización de edificios.

De acuerdo a los posibles sectores de aplicación se diferencia en PROFIBUS entre las siguientes variantes:

- Comunicación de proceso o campo.

    - **PROFIBUS DP** (por sus siglas en inglés de Decentralize Periferia) Es usado cuando se necesita un intercambio de datos rápido y cíclico entre los aparatos de campo con las unidades de gestión [5].
    - **PROFIBUS PA** (por sus siglas en inglés de Process Automation) para aplicaciones de automatización de procesos en zonas que exigen una seguridad intrínseca al sistema de gestión [5].

- Comunicación de datos.

    - **PROFIBUS FMS** (por sus siglas en inglés de Fieldbus Message Specification) para la comunicación de datos entre dispositivos de automatización y aparatos de campo [5].

1.3.3. ETHERNET INDUSTRIAL.

Las redes Ethernet que en la actualidad han tenido una gran aceptación a nivel mundial en entornos corporativos y de pequeñas oficinas, están empezando a encontrar un nuevo campo de acción en el ambiente industrial. Las características sobresalientes que hacen de Ethernet un protocolo atractivo para su implementación son, entre otras, su habilidad para monitorear la transmisión de los datos, la existencia de utilitarios tales como telnet o el soporte para el protocolo SNMP que permiten configurar los equipos vía remota y la capacidad de cargar programas de control de dispositivos desde una estación central.

Pero sobre todo, el principal objeto de mantener una red industrial Ethernet, a nivel de dispositivos de campo en una empresa o en una planta industrial, es la capacidad de incluir en el manejo de la red, las utilidades que presta la pila de protocolos TCP/IP, como pudiera ser la transmisión de señales de control o monitoreo con un buen nivel de seguridades o inclusive de redundancia de datos, garantizando la fiabilidad e inviolabilidad de estos, además de conservar la estructura del protocolo Ethernet, a lo largo de la red, sin la necesidad de utilizar conversores de protocolos o conversores de medios para pasar del nivel de campo al nivel de operación y ejecución de sistemas o al administrativo de la planta industrial.

Una red industrial Ethernet que vaya desde la oficina de gerencia hasta el piso de la planta industrial debe considerar los ambientes extremos a los que estará sometida, es decir que si se piensa conectar el nivel de producción con los equipos que fueron inicialmente adquiridos para una aplicación de oficina, existe el riesgo de causar un gran daño en el sistema industrial en general. Es por esto que los equipos a ser utilizados en el nivel industrial deben considerar aspectos como [7]:

- Temperaturas extremas (40°C a 75°C).
- Operación con diferentes tensiones de alimentación, tanto en corriente continua como en corriente alterna.
- Protección contra sobretensiones (de hasta 3000 voltios).
- Altos niveles de ruido eléctrico, transitorios e interferencia electromagnética causada por motores y maquinas de conmutación eléctrica.
- El uso de gabinetes herméticos para trabajar en atmósferas agresivas, nocivas y condiciones de uso extremas.

Además en una red Ethernet Industrial, a diferencia de una red de oficina, se necesita un medio de comunicación robusto y con la habilidad de reponerse rápidamente a las fallas para poder garantizar un sistema de monitoreo y control que se mantenga activo las 24 horas del día durante 7 días a la semana y sin que existan cortes prolongados en la transmisión de datos.

Cuando se implementa una red Ethernet Industrial se hace uso de switches industriales que además de considerar los aspectos industriales antes nombrados, ellos también implementan el protocolo 802.1p mediante el cual se asigna una prioridad al tráfico que cursa por él, junto con un filtrado multicast dinámico, dependiendo del puerto escogido. Esencialmente este protocolo proporciona un mecanismo para implementar Calidad de Servicio (QoS) a nivel de la capa MAC (Media Access Control). Esta funcionalidad podría ir de la mano de la aplicación de redes virtuales para segmentar las diferentes áreas de la red.

1.3.4. PROFINET.

PROFINET es una pila de protocolos que fusiona Ethernet Industrial con Profibus para el uso de la automatización de sistemas y está definido por la norma IEC61158 y IEC61784 [8]. Esta pila de protocolos soporta estrategias de automatización avanzadas y ayuda

a las empresas a crecer rápidamente en la gestión de sus procesos. Además este protocolo ofrece una funcionalidad mejorada en comparación con PROFIBUS debido a que hace uso de técnicas que son familiares con las tecnologías de la información y a su vez con la teoría de buses de transmisión industriales, haciendo de PROFINET un estándar con flexibilidad y escalabilidad casi ilimitadas.

Esta suite de protocolos usa tres diferentes canales de comunicación para realizar la transferencia de datos [9]:

- Un canal estándar TCP/IP es usado para realizar la transmisión de la información de configuración del sistema, para transferir grandes archivos u operaciones de lectura y escritura no programadas y también como puerto de Entrada/Salida para diagnósticos y reportes.

- Un canal llamado RT (por sus siglas en inglés de Real Time) se usa para transmitir datos de reportes programados, información de alarmas y datos de entrada/salida generales. Las comunicaciones en este canal son independientes de la interfase TCP/IP y básicamente por aquí se transmite información hacia los controladores programables (PLC's) de manera similar al canal DP de PROFIBUS, de esta manera se asegura la compatibilidad entre estos dos protocolos.

- El tercer canal, también conocido como IRT (por sus siglas en inglés de Isochronous Real Time), es de muy alta velocidad de comunicación y usado principalmente para aplicaciones de control de motores o en aplicaciones en las que se requieran altas tasas de transmisión de bits.

En general, dos conceptos sostienen el estándar PROFINET: Profinet I/O como solución para el acceso determinístico y en tiempo real de señales distribuidas (similar a Profibus DP); y establecer el medio de comunicación para las nuevas plataformas de

desarrollos de plantas industriales con las facilidades de acceso hacia las tecnologías de la información y comunicación, en muchos casos sin importar el medio de acceso y con análisis en un verdadero tiempo real.

1.3.5. DNP3

DNP3 (por sus siglas en inglés de Distribution Network Protocol) es un protocolo que fue creado para permitir a dispositivos de control comunicarse entre sí haciendo uso de un enlace que se establezca sobre IP, con características sobresalientes de robustez, eficiencia y confiabilidad en la transmisión de sus datos, de manera que sus especificaciones van desde la capa física hasta la de transporte. Su uso inicial se dio en las plantas eléctricas y compañías de distribución de agua potable.

En este protocolo se establecen comunicaciones entre estaciones Maestro y Esclavo (a estas últimas se les suele llamar Outstation en Inglés) y los sistemas que trabajan con este protocolo soportan comunicaciones entre estaciones en modo múltiple-esclavo, peer-to-peer y múltiple-maestro, en función de cómo se implementen las topologías para el funcionamiento de los distintos sistemas SCADA. Los tipos de topologías que se soportan en los sistemas que implementan el protocolo DNP3 son [11]:

- Maestro – Esclavo,
- "Multidrop" desde un maestro,
- Jerárquica con concentradores de datos intermedios,
- Múltiples Maestros.

Es probable que en algunas situaciones se haga uso de convertidores de protocolo, principalmente en redes jerárquicas, en donde una subdivisión de la red puede estar diseñada para operar con DNP3 y obtener en esta sección sus beneficios, mientras que

en otras áreas de la empresa se utilice un protocolo alterno, por ejemplo para acceso a usuarios de más alta jerarquía como un jefe de planta o un administrador de procesos, en estos casos DNP3 puede ser encapsulado en paquetes Ethernet de TCP/IP y aunque esto aumente el "overhead" asociado a cada paquete, permitirá que los paquetes se transporten por otras áreas del sistema SCADA.

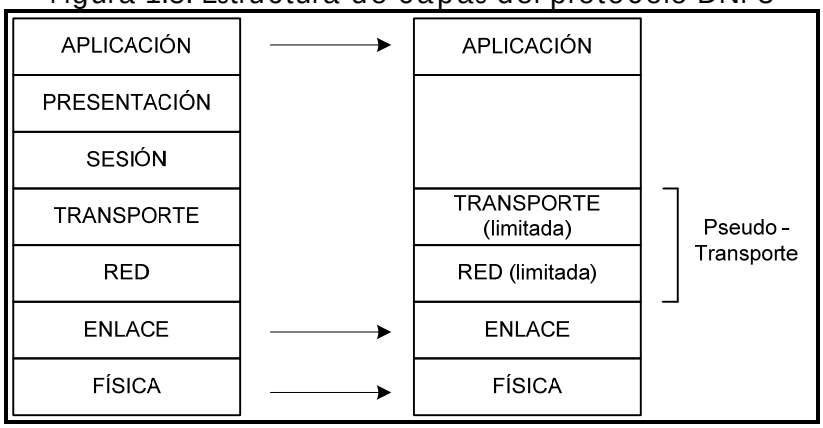
Para su transporte DNP3 usa un sistema de capas que está basado en el modelo EPA (de sus siglas en inglés de Enhanced Performance Architecture), que fue creado por la IEC (por sus siglas en inglés de International Electrotechnical Commission) a partir del modelo OSI pero excluyeron algunas capas superiores para conseguir un estándar simplificado que se adapte de mejor manera a las necesidades de los sistemas de transmisión de datos en telemetría, que hasta ese momento existían y en la actualidad se ven ampliados por la extensión de su uso hacia los sistemas SCADA [12]. Este modelo usa dos capas físicas para el enlace en hardware y una para la capa de aplicación como se muestra en la figura a continuación.

Figura 1.4. Modelo EPA (Enhanced Performance Architecture)

Fuente: Tecnologías WAN para sistemas SCADA, Ing. Marcelo García R.

DNP3 usa este modelo de tres capas como referencia pero además incluye algunas funciones de transporte, que comúnmente son referidas como pseudo – capas de transporte o también descritas como capas de red y transporte limitadas, en comparación con las capas establecidas en el modelo OSI. En la figura a continuación se muestra la estructura del protocolo DNP3 en relación con el modelo OSI y en los párrafos siguientes se describe, en términos de la estructura del mensaje del protocolo, la función de cada una de las capas mostradas.

Figura 1.5. Estructura de capas del protocolo DNP3

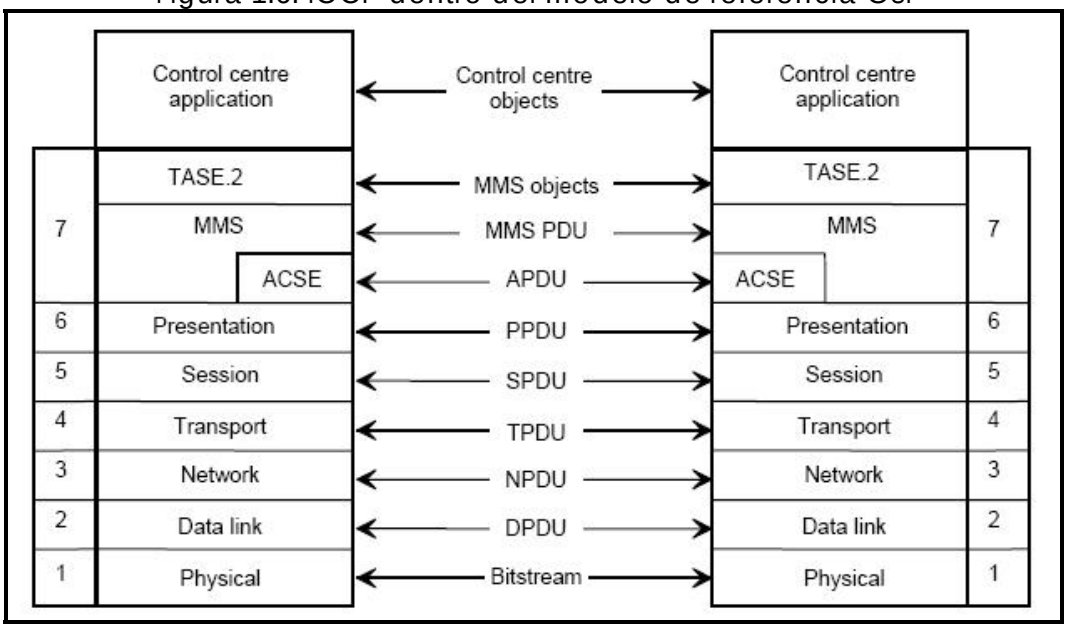


Fuente: Tecnologías WAN para sistemas SCADA, Ing. Marcelo García R.

1.3.6. ICCP.

El protocolo ICCP (Inter – Control Center Communications Protocol) constituye básicamente un mecanismo para implementar una comunicación óptima entre dos centros de control SCADA que necesiten estar enlazados, en tiempo real, para intercambiar información e interactuar entre ellos y entre los elementos de campo que tengan bajo su mando. Este protocolo facilita los medios para que el usuario, junto con su API (Application Program Interface) pueda realizar la gestión de procesos que estén subordinados a un centro de control remoto, de tal manera que este protocolo se desarrolla en la capa de aplicación del modelo OSI de intercomunicación, montado directamente sobre los mensajes que se envían entre centros de control, es decir que en las capas inferiores, ICCP permite la implementación de otros protocolos que optimicen la transmisión de los datos. Esta característica presenta la ventaja de que cualquier mejora en la gestión remota de los centros de control será transparente para los protocolos de comunicación que estén implementados en las capas inferiores. En la figura a continuación se muestra como trabaja ICCP en función del modelo OSI.

Figura 1.6. ICCP dentro del modelo de referencia OSI



Fuente: SCADA Protocols [14].

Dentro de ICCP se especifica el uso de mensajes de manufactura MMS (Manufacturing Messages Specfication) que son los que definen la mecánica de la nomenclatura, listado y direccionamiento de las variables e interpretación de los mensajes [13]. Estos mensajes se generan mientras las aplicaciones (API's) que corran en cada uno de los centros de control, que posiblemente sean desarrolladas por diferentes fabricantes, se encarguen de gestionar los eventos y procesos de sus propias redes, así, ICCP obtendrá valores de ellos y especificará objetos dentro de los mensajes MMS como parámetros o métodos que se leerán o ejecutarán remotamente entre centros.

Por otra parte la topología de una red ICCP está basada en los conceptos de maestro – servidor, ya que todo intercambio de datos tiene su origen en una solicitud de un centro de control (cliente) hacia otro que posee o administra diferentes datos (maestro). Para establecer las conexiones lógicas entre los centros de control ICCP usa el mecanismo llamado ACSE (Association Control Service Element). Las asociaciones pueden ser entre un servidor o maestro y varios centros de control cliente. En este esquema los accesos entre servidores y clientes se administran mediante tablas

bilaterales en las que se especifican los permisos de escritura, lectura o acceso bloqueado para las comunicaciones en tiempo real, además de la periodicidad de reporte, reporte de excepción, banderas de calidad, etc. Parámetros que son determinados por el cliente al momento del establecimiento de una asociación [13].

1.3.7. AS – Interface.

AS-Interface o AS-i (Actuator/Sensor Interface) es un Bus de Sensores y Actuadores (bus de campo), que se encuentra estandarizado bajo la norma internacional IEC62026-2 y europea EN 50295 para el nivel de campo más bajo en la capa física. Fue diseñado en 1990 como una alternativa económica al cableado tradicional y fue concebido con la idea original de crear una red simple para sensores y actuadores binarios, con capacidad de transmitir datos y proveer alimentación a través del mismo bus, manteniendo una gran variedad de topologías que faciliten la instalación de los sensores y actuadores en cualquier punto del proceso con el menor esfuerzo posible.

Tradicionalmente para interconectar elementos de campo se usaba un estándar analógico llamado 4-20 que usaba una fuente de corriente entre 4 y 20 mA y a manera de sensor transmitía los valores programados para indicar un estado determinado del elemento de campo hasta llegar a dispositivos de control y comunicación superior como un PLC. Este fue sustituido por protocolos más confiables como AS-i aunque en la actualidad todavía se lo puede encontrar en la industria.

1.4. Equipos sensores y actuadores utilizados para realizar la adquisición de datos en el campo.

Existe una gama muy variada de equipos sensores, que se utilizan en los sistemas SCADA, para realizar la recolección de los datos desde el nivel de campo en los distintos procesos industriales. El tipo de sensores usados depende de la naturaleza del proceso a ser monitoreado, de esta manera, estos pueden ser de presión, temperatura, nivel, humedad, etc.

Los sensores pueden reportar una cantidad determinada de bits según el proceso que estén monitoreando, en algunos casos, inclusive, ellos solo indican el estado de un determinado suceso, de dos posibles opciones (On/Off); por ejemplo si un motor se encuentra encendido o apagado, en estos casos el sensor es llamado del tipo binario y en teoría no necesita mas que un bit para reportar este cambio. En otras ocasiones un sensor puede dar como salida varios niveles posibles que varíen en el tiempo y el número de bits que usen para reportar estas variaciones depende directamente de la cantidad de niveles en que puedan ocurrir. A continuación se detallan algunos equipos sensores que pueden ser utilizados en la adquisición de datos de un sistema SCADA [16]:

- Termómetros de Dilatación.
- Termómetros bimetálicos.
- Termómetros de resistencia metálica.
- Termistores.
- Termopares.
- Pirómetros Ópticos.
- Pirómetros de radiación total.
- Pirómetros de dos colores.
- Sensor de presión tipo Bourdon.
- Sensor de presión de Fuelle.

- Sensor de presión de diafragma.
- Sensor capacitivo de presión.
- Sensor de presión de galgas extensiométricos.
- Sensor inductivo de presión.
- Sensor piezoeléctrico.

1.5. Aplicativos de Software utilizados en los sistemas SCADA.

En el mercado actual de los sistemas SCADA's se puede encontrar una serie de aplicativos de software para realizar la gestión de los diferentes procesos que se llevan a cabo en la industria. El software SCADA puede ser del tipo propietario o abierto. Las empresas que desarrollan software propietario, para que el centro de gestión se comunique con su hardware de adquisición, venden su producto en forma conjunta con su aplicación de hardware. El principal problema con estos sistemas es la gran dependencia que se crea con el proveedor, para futuras ampliaciones, repuestos o mantenimiento en general. Debido a esto los aplicativos de software abierto se han vuelto muy apetecidos, además que estos sistemas permiten la interoperabilidad entre varios elementos de la red SCADA con lo cual su instalación, mantenimiento y futuras ampliaciones estarían determinadas por los reales requerimientos de la empresa sin importar el proveedor de la tecnología.

En muchos casos el software que utilizan las empresas a nivel de gestión es del mismo fabricante al que se le concesiona la instalación de los dispositivos de nivel de campo, independientemente de que sea propietario o abierto. Entre los más populares se puede encontrar a SIEMENS con su programa de desarrollo para automatización de procesos WinCC, a National Instruments con LabVIEW, entre otros. En cuanto a sistemas independientes de los fabricantes de hardware se puede listar a CITEC y WanderWare,

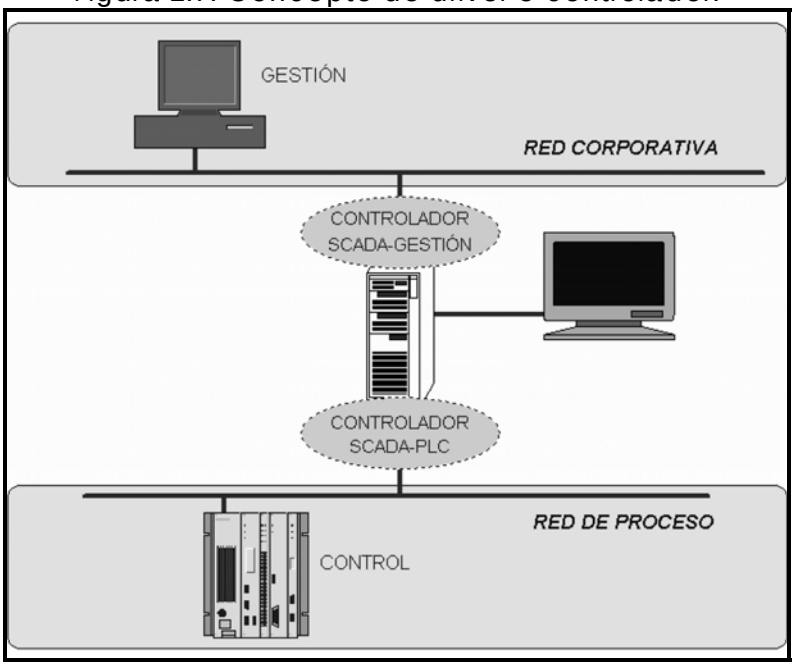
los cuales son dos paquetes de software abierto que manejan varias de las facilidades de gerenciamiento que se incluyen en otros sistemas propietarios avanzados.

Descripción.

Un software SCADA, como programa del tipo HMI (Human Machine Interface), se ejecuta en un computador o terminal gráfico, con el que interactúa el operador o administrador del sistema y contiene unos programas específicos o agentes de software que le permiten comunicarse con los dispositivos de planta, para realizar el control, diagnóstico y monitoreo de los procesos de la empresa, y también posee los elementos de gestión que le dan las facilidades de administración.

Estos programas, encargados de las comunicaciones en la red del sistema SCADA, son los denominados controladores o drivers (en inglés) y vienen formados como un solo paquete que se encarga de gestionar los enlaces, el tratamiento de la información que se transmite y los protocolos utilizados para establecer la comunicación (Profibus, AS-i, Ethernet, etc.). En la figura a continuación se muestra como se distribuyen los controladores a la largo de la red. En esta se observa como el controlador realiza la función de traducción entre el lenguaje del programa SCADA y el del Autómata o PLC (por ejemplo, Profibus), o entre el SCADA y la red de gestión de la empresa (con Ethernet, por ejemplo).

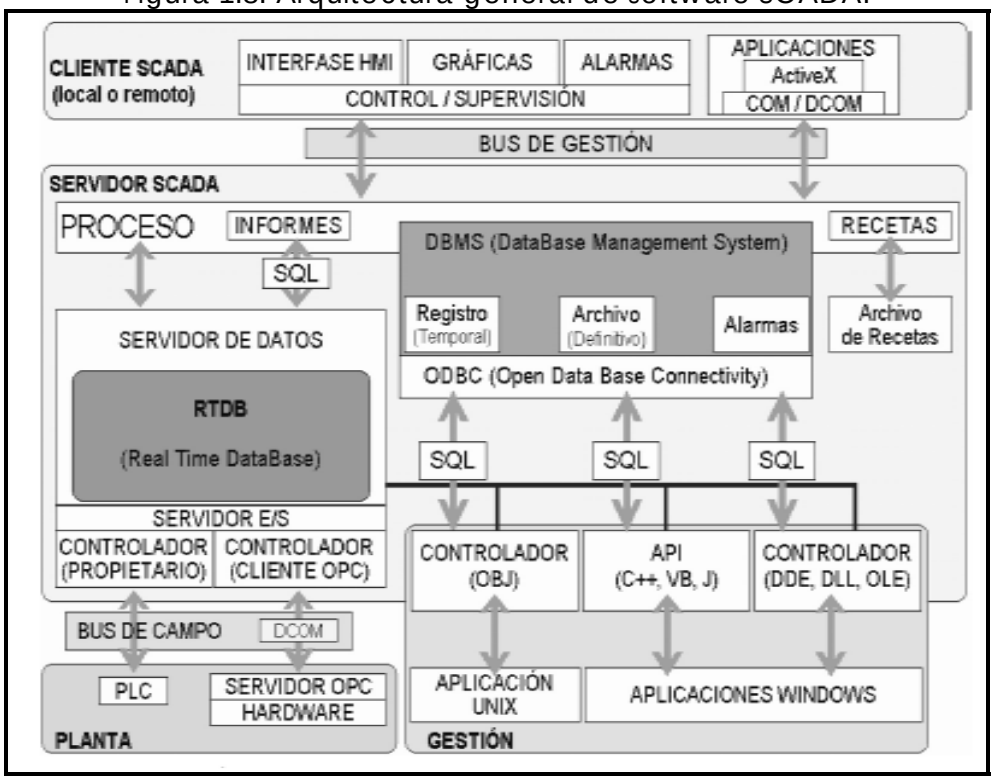
Figura 1.7. Concepto de driver o controlador.



Fuente: Sistemas de visualización industrial [2]

Según la importancia del sistema es posible especializar componentes realizando tareas exclusivas dentro del sistema de control, como por ejemplo con los servidores de datos, de alarmas, de históricos, de interface hombre-máquina, etc. Una vez que los datos de planta se hayan procesado, se puede transferir la información a otras aplicaciones de software, tales como hojas de cálculo o bases de datos. Esto es lo que podríamos denominar gestión de datos, lo que nos permite analizar eventos, alarmas, emergencias, etc., ocurridos durante la producción [2]. En la figura a continuación se puede observar una aproximación gráfica de la estructura de una aplicación de software de un sistema SCADA.

Figura 1.8. Arquitectura general de software SCADA.

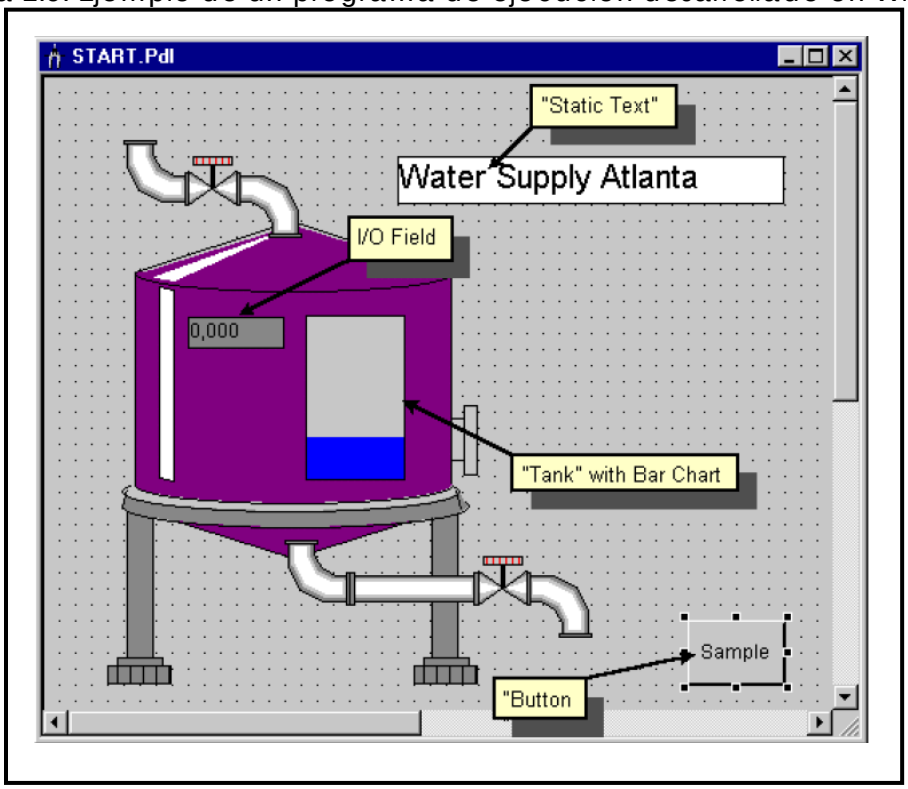


Fuente: Sistemas de visualización industrial [2]

El software SCADA está dividido entre programa de desarrollo y el programa de ejecución o aplicativo:

- El programa de desarrollo tiene herramientas que le permiten al usuario diseñar sus ventanas de aplicación, con sus respectivas características (textos, dibujos, colores, propiedades de los objetos, etc.) y que estarán estructuradas en función de los procesos que vaya a controlar el sistema SCADA [2].
- El programa de ejecución permite correr la aplicación diseñada con el programa de desarrollo y es el elemento de software que va a estar gestionando todo el sistema SCADA mientras se encuentre en uso [2].

Figura 1.9. Ejemplo de un programa de ejecución desarrollado en WinCC.



Fuente: Sistemas de visualización industrial [2]

Como se puede apreciar a lo largo de este capítulo la implementación de un sistema SCADA requiere del cuidado en detalle de cada nivel a ser desarrollado y a pesar que la mayoría de sistemas instalados en la industria son soluciones de un solo fabricante, estas son realizadas con estándares bien conocidos, por lo tanto se podría obtener un sistema SCADA bien instalado y completamente funcional sin la necesidad de atarse a un proveedor y además a un costo más económico.

2. TECNOLOGÍAS DE ÁREA EXTENDIDA PARA EL ACCESO SCADA.

Un ritmo constante de crecimiento es siempre un objetivo de una empresa y expandirse por otras localidades es el resultado lógico de esta expansión. A nivel industrial este crecimiento es siempre controlado y monitoreado por un sistema SCADA en conjunto con herramientas administrativas que permitan conocer en detalle los parámetros de producción o los resultados de los procesos desarrollados, de tal manera, que mientras la producción se lleva a cabo en la planta industrial de la empresa la gestión de los resultados es ejecutada en las oficinas administrativas fuera de la planta o inclusive en otra ciudad o país. Es así que el sistema SCADA alcanza las proporciones de una red de área extendida y por lo tanto es necesario considerar el problema del medio de acceso que interconectará las diferentes localidades para su implementación. A continuación se describe los principales métodos de acceso físico que se encuentran disponibles en la actualidad como base en las tecnologías de las comunicaciones.

2.1. Medios Alámbricos.

2.1.1. Dial Up.

Una conexión de Dial Up es una forma barata de acceso a una red de área amplia en la que el cliente utiliza un módem de línea para llamar, a través de la red telefónica conmutada, a un servidor de acceso (por ejemplo PPP) y el protocolo TCP/IP para establecer un enlace módem-a-módem, que permite entonces que se enrute la conexión. Esta conexión es principalmente utilizada para el acceso a Internet aunque también es implementada en ocasiones para soluciones de remotización de sistemas. La desventaja de este tipo de conexión es que es lenta comparada con las conexiones de tipo DSL.

La conexión de Dial-Up resulta factible en la mayor parte del planeta, ya que las Redes Telefónicas Conmutadas están globalmente extendidas. Esta conexión es utilizada en zonas rurales o en áreas muy remotas donde las conexiones de banda ancha son imposibles por falta de infraestructura (la baja demanda de este tipo de servicios en estos lugares hace que su instalación sea poco rentable y que no se halle entre las prioridades de las empresas de telecomunicaciones). Esta forma de conexión suele realizarse a través de una llamada local y normalmente requiere algo de tiempo para establecer una sesión de datos.

Las conexiones por línea conmutada tienen en general una velocidad máxima teórica de 56 kbit/s (con el protocolo V. 92); de forma neta 53 kbit/s. Sin embargo, en la práctica, la velocidad media de transferencia suele ser de 10 kbit/s. Además, si hay ruido en la línea telefónica la tasa de transferencia disminuye. Las conexiones por línea conmutada tienen, por lo general, una latencia superior a los 200 milisegundos o más, lo cual hace difícil o casi imposible realizar transacciones que demanden gran ancho de banda, como la video – conferencia, pero puede representar una solución válida para sistemas que requieran transmitir pocos bits en intervalos de tiempo largos, como por ejemplo en pequeños sistemas SCADA.

Las conexiones de Dial Up nacieron con la creación del módem (MOdulador / DEmodulador), el cual permitía a las grandes empresas dar soluciones de conexión WAN entre sus sucursales y por lo tanto estos equipos eran de carácter propietario, pero a finales de los años 80 la ITU empezó a estandarizar las comunicaciones entre los equipos terminales de datos (DTE, por sus siglas en inglés de Data Terminal Equipment) y los equipos de comunicación de datos (DCE, por sus siglas en inglés de Data Comunication Equipment).

A finales de los 80's la Unión Internacional de Telecomunicaciones (UIT) empezó a realizar las llamadas recomendaciones V-series que estandarizarían luego las

comunicaciones que se realicen por medio de los MODEM's de línea Dial Up entre los equipos DCE y DTE.

2.1.2. XDSL

DSL es una tecnología que utiliza módems sobre un par de cobre trenzado, originalmente usado para las líneas telefónicas, para transmitir datos de banda ancha tales como datos multimedia o de video para los suscriptores. El término xDSL cubre un número de formas similares de tecnologías DSL como son: ADSL, SDSL, HDSL, HDSL-2, G.SHDSL, IDSL y VDSL.

xDSL ha captado la atención de muchos proveedores de servicios de transporte de datos, debido al amplio ancho de banda que esta tecnología ha llegado a manejar y por el beneficio que representa ya tener implementada la infraestructura del medio de acceso (par trenzado de cobre) para el servicio y sin mayores cambios en ella.
Los servicios xDSL son enlaces dedicados y usan un acceso punto a punto, sobre el par de cobre trenzado de última milla de la red de telefonía pública, entre proveedor de servicios de red de datos y el cliente o suscriptor. En la actualidad la mayoría de las implementaciones de esta tecnología son ADSL, principalmente dedicados hacia los clientes domiciliarios para la navegación en Internet.

2.1.2.1. ADSL (Asymmetric Digital Subscriber Line)

La tecnología ADSL es asimétrica en cuanto a la medida de ancho de banda de subida y bajada de la información, de esta manera se permite designar más tráfico de bajada en el total de ancho de banda disponible, es decir el tráfico desde la oficina

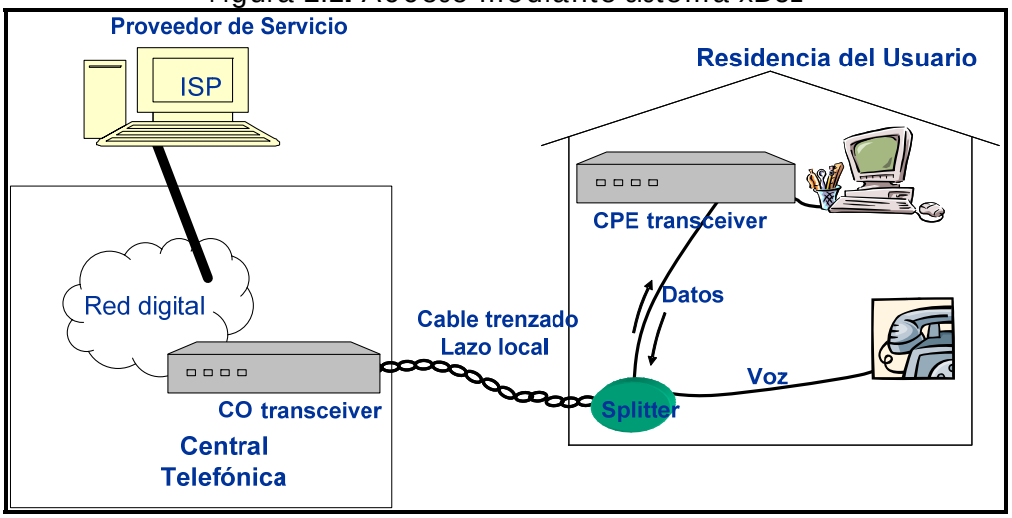
central hacia la premisa del cliente, siendo así consecuente con el comportamiento característico del tráfico de Internet.

Esta característica combinada con el método de acceso permanentemente en línea (elimina la necesidad del marcado) hacen de ADSL una tecnología ideal para usuarios de Internet o de Intranets con amplias disponibilidades en cuanto a aplicaciones multimedia, de video en demanda o de acceso a LAN's remotas. Estos usuarios comúnmente reciben mucha más información de la que envían.

ADSL transmite más de 6 Mbps en bajada hacia el suscriptor y hasta 1 Mbps en subida lo cual representa como 50 veces más la velocidad de transmisión que su antecesora la tecnología dial-up y sin la necesidad de nuevo cableado o de nueva infraestructura en el medio de acceso, de tal manera que ADSL literalmente ha transformado la red pública limitada a la transmisión de voz, texto y gráficos de baja resolución en una red más poderosa capaz de transmitir video y cualquier tipo de información multimedia.

Un enlace ADSL conecta un módem ADSL a cada extremo del par trenzado de cobre de la línea telefónica, creando tres canales de transmisión de información: Un canal de alta velocidad en sentido de bajada, un canal de dúplex de media velocidad y el canal de servicio básico de telefonía. El canal de telefonía tradicional esta divido de los canales de transmisión de datos por un spliter que básicamente contiene filtros, para que de esta manera se pueda asegurar que el canal de telefonía no se interrumpa cuando se mantiene la transmisión de datos, inclusive si ADSL falla. El canal de alta velocidad va desde 1.5 Mbps a 9Mbps mientras que el de media velocidad puede tener desde 16 a 640 Kbps. Cada canal puede ser multiplexado para obtener canales de menor velocidad en caso de que el usuario desee contratar una velocidad menor a la disponible.

Figura 2.1. Acceso mediante sistema xDSL



Fuente: Redes de acceso basadas en xDSL [18]

2.1.2.2. HDSL (High bit rate DSL)

El estándar HDSL es un enlace DSL síncrono de cuatro hilos con una tasa de transmisión de datos de 784 Kbps sobre cada par trenzado de cobre para conseguir un T1 y con tasa de transmisión de 1168 kbps para un E1.

HDSL se volvió popular porque es la mejor forma de proveer un E1 o un T1 sobre un par de cobre para los clientes corporativos en una red de datos. Además de la ventaja del tiempo de instalación que esto supone en un sistema HDSL no se manejan repetidores como en un sistema tradicional AMI (Alternative Mask Inversión) utilizado originalmente con este servicio.

2.1.2.3. SDSL (Symmetric Digital Suscriber Line)

SDSL es una versión HDSL con tasa de datos adaptiva y al igual que HDSL es simétrica. SDSL soporta solamente datos digitales en una unica línea (par decobre) y no soporta llamadas analógicas. Puede trasmitir hasta 1,54 Mbps de transmisión o puede ser configurado para ofrecer un variable rango de ancho de banda.

La característica simétrica que SDSL ofrece, combinada con al acceso permanente, la hace una tecnología favorable para su uso en redes WAN con una moderada tasa de transmisión de datos y representa una cómoda alternativa para líneas dedicadas T1 o E1.

2.1.2.4. VDSL (Very high data rate Digital Suscriber Line)

VDSL transmite datos a altas velocidades dependientes de las distancias de las líneas telefónicas de par de cobre. La máxima tasa de bajada considerada es de 51 a 55 Mbps sobre líneas de hasta 300 m. de longitud y de hasta 13 Mbps en enlaces de 1500 m. En cuanto a las tasas de subida, dentro de un modelo asimétrico, como el de ADSL, se puede obtener velocidades de 1,6 a 2,3 Mbps.

2.2. Medios Inalámbricos.

2.2.1. CDMA.

Esta tecnología permite el enlace inalámbrico de voz y datos por medio de la modulación de espectro ensanchado (spread spectrum) y generalmente está implementada como medio de acceso por parte de las empresas de servicios

celulares para las comunicaciones de voz, pero ventajosamente en sus últimas evoluciones está tecnología presta las facilidades para la transmisión de datos.

El acceso inalámbrico CDMA trabaja en las bandas comerciales de celulares de 850, 1900, 2500 y recientemente se encuentra en incursión una nueva frecuencia de 450 MHz impulsada principalmente para prestar servicio de telefonía en amplias zonas, lo cual puede representar una ventaja para el caso de las zonas rurales en donde hay baja densidad poblacional en grandes espacios de tierra [20].

CDMA se basa en la separación del espectro, que en los medios de la transmisión digital es cuando la señal ocupa una banda de frecuencia que sea considerablemente más amplia que el mínimo requerido para la transmisión de datos por otras técnicas, esto se hace con el objeto de que la señal transmitida sea percibida por todos los receptores en la misma frecuencia y al mismo tiempo pero que la información sea marginada dependiendo del código que use al ser transmitida, es decir, los usuarios comparten la misma banda de frecuencia y cada señal es identificada por un código especial, que actúa como una clave reconocida por el transmisor y el receptor. La señal recibida es la suma de todas las señales "combinadas" y cada receptor debe clasificar e identificar las señales que le corresponden de las demás señales. Para hacer esto utiliza un código pseudoaleatorio que corresponde con el código transmitido.

La primera operación implica encontrar del código correcto, y así sincronizar el código local con el código entrante. Una vez ha ocurrido la sincronización, la correlación del código local y del código entrante permite a la información apropiada ser extraída y las otras señales ser rechazadas. También permite que dos señales idénticas que vienen de diversas fuentes, sean demoduladas y combinadas, de modo tal que se mejore la calidad de la conexión, por lo que es también una ventaja el uso simultáneo de varias fuentes (diversidad). Por este motivo, una de las principales características de la

tecnología CDMA es que hace prácticamente imposible que sea objeto de interferencias e interceptaciones, ofreciendo gran seguridad en las comunicaciones.

Existen dos maneras en las que se realiza el ensanchamiento de espectro de la señal a ser transmitida en CDMA. El ensanchamiento por Secuencia Directa (DSSS, Direct Sequence Spread Spectrum) y el ensanchamiento por Salto de Frecuencia (FHSS, Frequency Hoping Spread Spectrum), consiguiendo por cualquiera de las dos formas las ventajas que ofrece CDMA como son la resistencia frente al ruido y a las interferencias y la dificultad para que su señal sea interceptada.

2.2.1.1. DSSS (Espectro Ensanchado por Secuencia Directa).

En esta técnica se genera un patrón de bits redundante (señal de chip) para cada uno de los bits que componen la señal. Cuanto mayor sea esta señal, mayor será la resistencia de la señal a las interferencias. El estándar IEEE 802.11 recomienda un tamaño de 11 bits, pero el óptimo es de 100. En recepción es necesario realizar el proceso inverso para obtener la información original.

La secuencia de bits utilizada para modular los bits se conoce como secuencia de Barker (también llamado código de dispersión o Pseudoruido). Esta es una secuencia rápida diseñada para que aparezca aproximadamente la misma cantidad de 1's que de 0's. Por ejemplo: +1-1+1+1-1+1+1+1-1-1-1-1 (Donde -1 representa los 0's) Solo los receptores a los que el emisor haya enviado previamente la secuencia podrán recomponer la señal original, además, al sustituir cada bit de datos a transmitir, por una secuencia de 11 bits equivalente, aunque parte de la señal de transmisión se vea afectada por interferencias el receptor aún puede reconstruir fácilmente la información a partir de la señal recibida [20].

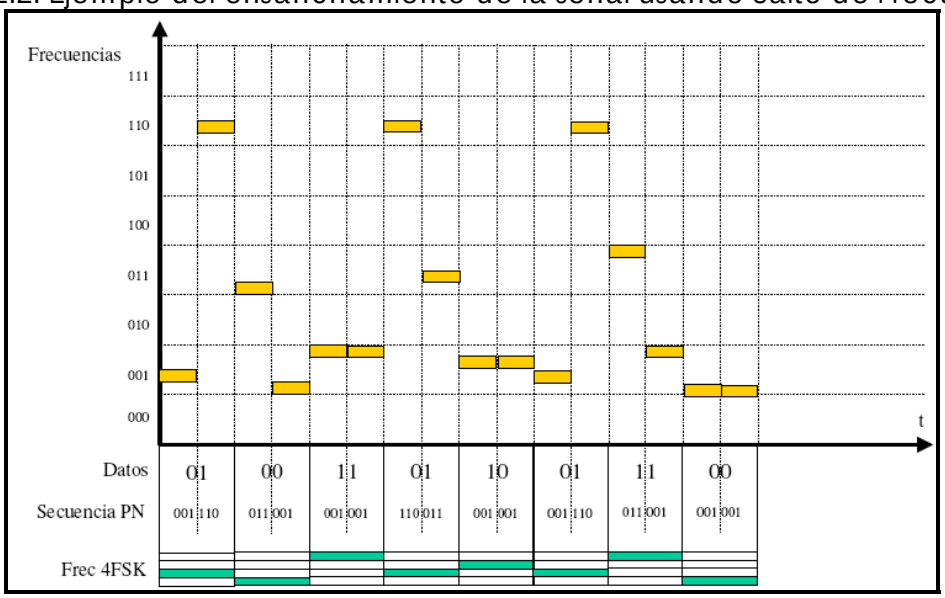
2.2.1.2. FHSS (Espectro ensanchado por salto de frecuencia).

La tecnología de espectro ensanchado por salto en frecuencia (FHSS) consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo llamada "dwell time" el cual es inferior a 400 ms. Pasado este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. De esta manera cada tramo de información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo.

El orden en los saltos en frecuencia se determina según una secuencia pseudoaleatoria almacenada en unas tablas, y que tanto el emisor y el receptor deben conocer. Si se mantiene la sincronización en los saltos de frecuencias se consigue que, aunque en el tiempo se cambie de canal físico, a nivel lógico se mantiene un solo canal por el que se realiza la comunicación. Esta técnica también utiliza la zona de los 2.4GHz, la cual se organiza en 79 canales con un ancho de banda de 1MHz cada uno. El número de saltos por segundo es regulado por cada país, así, por ejemplo, Estados Unidos fija una tasa mínima de saltas de 2.5 por segundo.

En el estándar IEEE 802.11, luego del ensanchamiento de la señal se utiliza la modulación en frecuencia FSK (Frequency Shift Keying), con una velocidad de 1Mbps ampliable a 2Mbps. En la revisión del estándar, la 802.11b, esta velocidad también ha aumentado a 11Mbps. La técnica FHSS sería equivalente a una multiplexación en frecuencia.

Figura 2.2. Ejemplo del ensanchamiento de la señal usando Salto de Frecuencia.



Fuente: Redes de acceso basadas en xDSL [18]

Hoy en día existen muchas variantes de CDMA que han surgido de su evolución, pero el CDMA original se conoce como CDMAOne bajo una marca registrada de Qualcomm. A CDMA se le caracteriza por su alta capacidad y celdas de radio pequeño, que emplea espectro extendido y un esquema de codificación especial y, lo mejor de todo es muy eficiente en potencia.

Características de CDMA

Información paquetizada. Las redes basadas en CDMA están construidas con el objetivo de realizar la transmisión de datos en formatos de paquetes, por lo general con protocolos basados en IP (Internet Protocol; protocolo de Internet). En otro tipo de redes se suele añadir equipo que soporte paquetes de datos y requiera también equipo terminal que lo soporte. El estándar CDMAOne ya incorpora en sus terminales los protocolos TCP/IP (Protocolo de control de transmision/Protocolo de Internet) y PPP (Protocolo punto a punto) [19].

Seguridad y privacidad. La técnica de espectro ensanchado ha sido utilizada ampliamente en aplicaciones militares, donde la seguridad de las conversaciones y protección de los datos son cuestiones de vital importancia. De igual manera, en un ambiente de negocios también son vitales los aspectos de seguridad y privacidad, es así que el actual estándar CDMA, diseñado con alrededor de 4.4 trillones de códigos, convierte a esta técnica de codificación en algo virtualmente imposible de capturar, descifrar o clonar por terceros sin autorización.

Control del nivel de potencia. El control de la potencia es otro de los beneficios que presentan los sistemas de CDMA. Empleando técnicas de procesamiento de señales, corrección de error, etc., CDMA supera el problema de la potencia con una serie de ciclos de retroalimentación. Con un control automático de la ganancia en las terminales y una supervisión constante del nivel de señal a ruido y tasas de error en las radio – bases, picos en el nivel de potencia son regulados con un complejo de circuitos electrónicos que ajusta la potencia a una razón de 800 veces en un segundo [19].

En una celda congestionada, la potencia de las terminales se elevaría creando una interferencia mutua. En el margen, las transmisiones de alta potencia inundarían las celdas vecinas donde éstas podrían ser tomadas por la radio base adyacente. En una celda de poca densidad, la potencia es tan baja que la celda se reduce efectivamente, transmitiendo sin interferencia hacia las celdas vecinas y mejorando el desempeño de las mismas. Este tipo de ajuste dinámico en el tamaño de las celdas es imposible en TDMA, pues en esta las celdas adyacentes utilizan diferentes frecuencias. Se ha comprobado en diversos estudios que CDMA es ciento de veces más eficiente en potencia que TDMA.

Bajo consumo de potencia y baterías más duraderas en las terminales. Debido al sistema de retroalimentación de CDMA que mantiene la potencia al más bajo nivel

permisible, las terminales consumen menos potencia y son más pequeñas, además de que las baterías de CDMA duran más tiempo que las de TDMA [19].

Amplia cobertura con pocas celdas. La señal de espectro ensanchado de CDMA provee gran cobertura en la industria inalámbrica, por lo que permite a los carriers la instalación de menos celdas para cubrir un área más extensa. Pocas celdas significan para los carriers mucho ahorro en infraestructura de radio-bases. Dependiendo de la carga del sistema y de la interferencia, la reducción de celdas es 50 por ciento menor en CDMA que en sistemas como GSM (sistema global para comunicaciones móviles), basado en TDMA [19].

Ancho de banda en demanda. El canal de 1.25 MHz de CDMA provee un recurso común a las terminales en un sistema de acuerdo con sus propias necesidades, como voz, fax datos u otras aplicaciones. En un tiempo dado, la porción de este ancho de banda que no utilice una terminal estará disponible para otro usuario. Debido a que CDMA utiliza una porción grande de espectro repartida entre varios usuarios, provee flexibilidad en el ancho de banda para permitir servicios en demanda. Bajo TDMA, donde los canales son fijos y pequeños, esto no es posible. En forma general está comprobado que CDMA es de tres a seis veces más eficiente en ancho de banda que TDMAc [19].

2.2.2. GPRS

GPRS (Por sus siglas en inglés de General Packet Radio Service), es una extensión de la tecnología de comunicaciones móviles GSM (Por sus siglas en inglés de Global System for Mobile Communications), diseñada con el objetivo de desarrollar las capacidades de transmisión de datos del usuario e información de señalización sobre la red que actualmente es utilizada para la transmisión de voz.

Características de GPRS

Las características de GPRS la hacen idónea para aplicaciones que van más allá del uso de la voz y que de forma global se conoce como Servicios Avanzados de Datos en Movilidad, con facilidades para la implementación en soluciones punto a punto y punto a multipunto, con soporte de protocolos de conmutación de paquetes como IP o X.25. A continuación se listan las particularidades de GPRS:

- GPRS es una mejora de GSM y define una arquitectura de red con:
  - Conmutación de paquetes.
  - Gestión de la movilidad.
  - Acceso radio.
  - Conexión a otras redes de datos fijas con IP, X.25, ATM, etc.

- En GPRS los usuarios están "permanentemente conectados"

- El terminal móvil se convierte en una ventana a Internet y a las intranets corporativas

- El tamaño de los paquetes de datos suele ser corto (típicamente entre 500 y 1000 octetos) y cada paquete es tratado como una entidad independiente.

- En GPRS, gracias a las velocidades que se alcanzan se puede realizar, además de los servicios básicos de telefonía móvil, consultas de la Web (HTTP), transferencia de archivos (FTP), transmisión de video comprimido, servicios de transmisión de datos punto a punto y punto a multipunto.

- En cuanto a seguridad, GPRS utiliza autenticación del abonado, confidencialidad de la identidad del usuario, confidencialidad de la información transmitida y el uso de una tarjeta SIM.

- Además, tiene cuatro niveles de codificación de radio cinco niveles de calidad de servicio (QoS)

- Puede utilizar más de una ranura de tiempo por trama TDMA, lo que permitiría velocidades de hasta 171,2 kbps (máximo teórico). En la práctica se usan como máximo 4 ranuras a 12 kbps c/u o sea 48 kbps.

2.2.3. IEEE 802.11x y Wi-Fi.

Las tecnologías 802.11x, comercialmente referidos con Wi-Fi son un conjunto de estándares desarrollados por un grupo de trabajo de la IEEE para las conexiones que se realicen en un entorno LAN (Local Area Network) de manera inalámbrica (WLAN). A continuación se detallan las mismas.

- 802.11: Estándar original del IEEE.
  - Estándar original del IEEE
  - Velocidad de hasta 2 Mbps.
  - Opera a una frecuencia de 2.4 GHz.
  - Puede tener interferencia con otros sistemas, como Bluetooth.
  - Usa modulación FHSS/DSSS.

- 802.11a:
  - Estándar de alta velocidad.
  - Soporta velocidades de hasta 54 Mbps.

  - Opera en la banda de los 5GHz.
  - Problemas de estandarización en Europa.
  - Usa modulación OFDM.

- 802.11b:
  - Conocido como Wi-Fi (Wireless Fidelity).
  - Soporta hasta 11 Mbps.
  - Compatible con el estándar 802.11 de modulación DSSS.
  - Opera en la frecuencia de 2.4 Gz.
  - Usa modulación DSSS.

- 802.11g:
  - Estándar de alta velocidad.
  - Soporta hasta 54Mbps
  - Compatible con el IEEE.
  - Opera en la frecuencia de 2.4 GHz.
  - Usa modulación OFDM/DSSS.

Actualmente hay más estándares que se encuentran en desarrollo que permitirán a Wi-Fi tener nuevos alcances como por ejemplo el estándar 802.11p que será usado por los vehículos en las autopistas para soportar a los llamados "Sistemas de Transporte Inteligente" para incrementar la seguridad de las vías.

Wi-Fi fue desarrollado inicialmente para ser usado por dispositivos móviles como computadores personales dentro de una LAN pero ahora es usado más frecuentemente por aplicaciones que van en crecimiento como son acceso a Internet y teléfonos de VoIP, juegos, etc. Una persona con un dispositivo Wi-Fi tal como una computadora, un teléfono o un PDA (Personal Digital Assitant) puede mantener conectividad cuando se encuentre dentro del área de cobertura de un access-point

(AP). Un AP inalámbrico conecta a un grupo de estaciones wireless de Wi-Fi de manera similar a la conexión que ofrece un hub dentro de una red LAN alambrada.

Una red típica de Wi-Fi puede tener uno o más AP con uno o más clientes inalámbricos que son reconocidos por el AP mediante el envío y reconocimiento de paquetes broadcast de muy corta duración que contienen información del SSID (Service Set Identifier) que representa el nombre de red. Wi-Fi también permite conectividad en modo punto a punto, el cual habilita a los dispositivos inalámbricos para conectarse entre ellos, esta conectividad es útil para el intercambio de información.

Estas tecnologías son usadas para el acceso y la interconexión de dispositivos de campo o de nivel de producción MES que puedan estar distribuidos a lo largo de una ciudad o para casos mayores, como por ejemplo, en los sistemas de captación de aguas para su potabilización y posterior distribución. En la implementación de los sistemas SCADA que mantienen centros de control repartidos por diferentes localidades es usual contratar sistemas de transporte de datos de operadoras bien conocidas que pueden interconectar los centros de control mediante redes de transporte SDH o Gigabit Ethernet con fibra óptica.

3. SEGURIDAD EN LOS SISTEMAS SCADA.

Históricamente los sistemas SCADA se han basado en entornos cerrados construidos alrededor de protocolos y sistemas propietarios, para aplicaciones especificas en muchos de los casos; los SCADA se han declarado sistemas seguros porqué estaban aislados del resto de la red corporativa, eran diseñados a medida y muy poca gente conocía como funcionaban en detalle. Con el tiempo las políticas de reducción de gastos, siempre presentes, provocaron que paulatinamente se haya ido optando por la estandarización de los protocolos y plataformas SCADA para facilitar la interoperabilidad entre distintas marcas, en los distintos niveles de operación de estos sistemas, generando así una competencia más intensa entre fabricantes y por ende abaratando los costos en la implementación SCADA. Esta tendencia de estandarización ha llevado a la mayoría de fabricantes a migrar hacia redes conocidas, como TCP/IP y plataformas PC, intentando aprovechar al máximo la infraestructura existente en las empresas [21].

Así, por un lado, SCADA ha dejado de ser un sistema desconocido y la excusa de que son seguros debido a que no están expuestos, o lo que se solía llamar como “seguridad a través de la oscuridad” ya no sirve, cualquiera que pueda adquirir el conocimiento sobre cómo está implementada la red podría aplicar técnicas de explotación e intrusión tradicionales sobre estas plataformas abiertas de hardware y software con vulnerabilidades heredadas de los viejos sistemas aislados SCADA [21].

Aunque en muchos entornos sigue existiendo la sensación de que la red SCADA es una red “cerrada” la realidad indica que cada vez tiene más interconexiones, tanto por necesidades de negocio (sistemas de gestión, ERP, toma de decisiones, etc.) como para reducir gastos, por ejemplo la unificación de la red de control con la red de usuarios, el mantenimiento remoto, la automatización del monitoreo, etcétera. En definitiva, se han ido eliminando aquellos puntos que hacían de SCADA un sistema

único, independiente e inviolable y las bases sobre las que construíamos los conceptos de seguridad en SCADA, dejando así al descubierto y con total vulnerabilidad las redes de las que dependemos para conseguir el mundo industrializado como lo conocemos hasta el momento.

3.1. Vulnerabilidades de los sistemas SCADA.

Los sistemas SCADA al haber sido diseñados como sistemas aislados y autónomos utilizaban redes con enlaces de datos que estaban netamente implementados para transmitir con alta confiabilidad y disponibilidad pero sin tener en cuenta su seguridad, además, estos sistemas estuvieron desarrollados con equipos de limitada capacidad de procesamiento, útiles únicamente para reportar datos de pocos bits o como actuadores, es así que la mayoría de las redes SCADA actuales carecen de dispositivos de seguridad como cortafuegos, mecanismos de cifrado o software antivirus. En los siguientes apartados se discutirá las vulnerabilidades propias que presentan los sistemas SCADA debido a sus características típicas.

3.1.1. Vulnerabilidades Técnicas

Hoy en día es bastante común que las redes SCADA estén mezcladas con las redes de las empresas sin ningún tipo de separación o control de acceso. En muchos casos, los ordenadores tienen dos tarjetas de red conectadas, por un lado a la red de la empresa y a la red SCADA por otro. Esto crea una puerta de enlace potencial entre ambas, ya que basta comprometer alguna máquina para poder acceder de una red a otra. Los atacantes no necesitan ser expertos en redes de control de procesos, basta con atacar una máquina de la red local de la empresa que tenga acceso a la red SCADA para poder causar daños.

Una carencia de estos sistemas, como se ha dicho anteriormente, es que no se han implementado medidas de seguridad básicas en ninguno de sus niveles, tales como cifrado, autenticación, almacenamiento de datos críticos en textos planos, redundancia e incluso hay implementaciones cuya pila TCP/IP es defectuosa, lo que las hace vulnerable a una variedad de ataques plenamente conocidos. Por ejemplo, los sistemas SCADA son muy sensibles a escaneos de red, por lo tanto es bastante arriesgado ejecutar un proceso de auditoría de seguridad ya que los resultados son impredecibles y van desde ralentización de la red hasta denegaciones de servicio, es decir que muchos de los controles de seguridad empleados en otro tipo de entornos no son directamente trasladables a los sistemas SCADA.

Una de las herramientas favoritas de los equipos de seguridad para realizar auditoría es el "escáner de puertos" el cual se convierte en nuestro peor enemigo si hablamos de redes SCADA, existen sistemas operativos que ejecutan procesos de la misma manera desde hace quince años, PLC con implementaciones de funcionalidades de red básicas o no estándar, etc. componentes que no están diseñados para lo imprevisto y que sucumbirán a un procedimiento "normal" de auditoría de seguridad. Así pues, es necesario innovar y desarrollar metodologías "no agresivas" para la revisión de seguridad de sistemas SCADA, principalmente en entornos de laboratorio para luego poder ser llevado a la práctica sin el riesgo de afectar ningún proceso.

Por otra parte, los sistemas que ya han sido implementados o adaptados con redes de comunicación nuevas y dedicadas para SCADA utilizan los protocolos actualizados para establecer un enlace entre los distintos niveles de control y monitoreo de los procesos. En estos casos se han ido presentando nuevos problemas de vulnerabilidad como el descubierto recientemente por la empresa de seguridad electrónica industrial DIGITAL BOND en un servidor de monitorización comercializado con el nombre de LiveData RTI que usa ICCP para su implementación, en este se presenta una

denegación del servicio cuando se hacen excesivas peticiones de conexión, dejando sin servicio al sistema por completo.

En sistemas SCADA implementados sobre redes WAN se suele presentar el problema de vulnerabilidades en la conexión de sus dispositivos de campo, que usualmente son los que se encuentran distribuidos a largas distancias del centro de mando. El medio por el que estas ubicaciones remotas se comunican con el resto de la infraestructura SCADA puede representar un problema de seguridad adicional: Packet Radio, VSAT, WiFi, etc. mecanismos de transmisión sin hilos que, sin una capa adicional de cifrado, pueden comprometer la confidencialidad de las comunicaciones. Con el paso del tiempo, los sistemas SCADA han evolucionado hacia plataformas comerciales y protocolos abiertos (Windows, TCP/IP, etc.), con lo que hay que añadir a las vulnerabilidades inherentes a SCADA los tipos de ataques tradicionales para estas plataformas (gusanos, vulnerabilidades en software comercial, etc).

3.1.2. Vulnerabilidades Culturales

Aunque las deficiencias de seguridad en software y hardware que se describen anteriormente hayan sido cubiertas por los fabricantes o ingenieros que implementan el sistema, existen varias vulnerabilidades de que no han sido publicadas o inclusive descubiertas, debido a que los sistemas no son probados exhaustivamente y menos aún si ya han sido implementados en su totalidad, bajo el concepto de que "si funciona, es mejor no tocar", en la mayoría de veces se confía en su aislamiento. Es en casos como estos en los que la vulnerabilidad de los sistemas SCADA pasa de ser un problema técnico a ser un problema de visión de los ingenieros a cargo.

El desarrollo que han tenido los SCADA en cuanto a seguridad no va de la mano con los protocolos que se han desplegado hasta ahora, con el objeto de la estandarizar las redes, debido básicamente a que el tema de la seguridad no había sido abordado

frontalmente hasta hace poco tiempo. Como se ha mencionado anteriormente la seguridad en estos sistemas se confía o confiaba en el hecho de que son redes que se encuentran aisladas del mundo exterior y si bien ese concepto era válido años atrás, hoy es obsoleto.

Para que un sistema mal protegido sea violado solo basta que alguien con un poco de información, sin tener la autorización necesaria, sienta la necesidad de ingresar a él y sin duda, en este aspecto, la mayoría de incidentes reportados actualmente provienen de fuentes internas que obtienen acceso mediante fallas simples como la falta de autenticación o la escasa separación de roles o perfiles en los aplicativos del sistema. Esta visibilidad total y disponible del sistema, unida a la falta de controles de autenticación y auditoria facilita los errores humanos además de hacer mucho más cómodas y sencillas las tareas de un atacante que quiere comprometer el sistema. Comprometer la unidad central o los aplicativos HMI le permiten tener una visión a alto nivel del proceso en el que quiere causar daños.

Por otro lado existe una gran cantidad de información disponible públicamente acerca de los componentes de la infraestructura SCADA (protocolos, unidades remotas, etc.) que permiten a un atacante convertirse en un experto SCADA para poder descubrir y explotar nuevos tipos de vulnerabilidades a más bajo nivel. Fabricantes e integradores, con la colaboración del cliente, suelen publicar detalles sobre proyectos de implantación exitosos, dejando a disposición pública datos de configuración y funcionamiento de carácter sensible y ciertamente interesante para un atacante.

Algunos de los componentes de la infraestructura SCADA, como los RTU o los PLC, suelen estar ubicados remotamente, físicamente aislados y situados a miles de kilómetros de la Unidad Central y ganar acceso físico a las instalaciones que albergan estos dispositivos remotos suele ser trivial y si bien físicamente se encuentran lejos de la unidad central, a nivel lógico tienen conectividad con el sistema SCADA (y

potencialmente con la red interna, los ERP, etc.), ofreciendo al atacante un punto de entrada a una red aparentemente aislada. Por lo tanto este representa una vulnerabilidad más en un entorno SCADA no protegido.

3.2. Esquemas de seguridad para los sistemas SCADA.

3.2.1. Arquitecturas de red para sistemas SCADA

Los sistemas SCADA tradicionalmente han estado aislados de la red corporativa y del acceso a internet. Siempre que sea posible es aconsejable mantener esta configuración, pero existen situaciones en que esta solución no es viable, como por ejemplo un SCADA que se despliegue sobre una red WAN y que tenga sus varios centros de control conectados por medio de la red corporativa estará destinado a mantenerse conectado con el resto de la empresa y probablemente al acceso a internet.

Cuando se tiene un sistema SCADA con algún tipo de enlace con las redes corporativas o de acceso a internet es necesario el uso de ciertas técnicas de aislamiento que aseguren la integridad e inviolabilidad del entorno de trabajo, en muchos de los casos es necesario migrar la arquitectura de red sobre la que se soporta el sistema hacia una que mantenga los estándares de seguridad y determinen una marcada división entre las redes. Con estas técnicas se busca minimizar las oportunidades para los atacantes externos o usuarios malintencionados.

Para mantener un esquema de seguridad práctico se recomienda el uso de cortafuegos (o Firewalls) y sistemas detectores de intrusos, IDS (por sus siglas de Intrusion Detection System). Además, se debe permitir la mínima cantidad de conexiones desde servidores u ordenadores externos hacia los dispositivos internos de la red SCADA, y todas aquellas permitidas deben estar debidamente documentadas y justificadas.

También se debe usar una infraestructura dedicada para procesos críticos de emergencia y que preferiblemente estén atendidos con un protocolo distinto al del resto de la red, como por ejemplo en un sistema de apagado general de seguridad o emergencia.

Otra práctica recomendada, bajo el esquema de mantener aisladas las redes SCADA del resto, es el uso de las llamadas zonas desmilitarizadas (DMZ), que lo que buscan es mantener a hosts o servidores que usualmente son accedidos por usuarios externos, fuera de la red principal. De tal manera que los equipos que sean ubicados en esta zona no tendrán acceso a ninguno de los equipos que están dentro de la LAN SCADA, pero si habrá flujo de información en el sentido contrario, así que los equipos que se encuentren en la zona desmilitarizada estarán disponibles para las diferentes redes.

Los servidores que almacenan los datos, recopilan información de la red SCADA y la almacenan para que esté disponible para consultas y reportes históricos, son comúnmente llamados Historian. En una configuración segura es recomendable que los servidores historian se ubiquen en una zona desmilitarizada localizada entre la red corporativa y la red SCADA, independiente de las dos. También es recomendable que se utilicen dos protocolos distintos para comunicarse con cada red. Un ejemplo de esto sería que utilicen alguna base de datos relacional para compartir la información en la red corporativa y un protocolo SCADA para recoger información desde esa red. Así se configuran reglas diferentes en el firewall y se minimiza el riesgo de incidentes.

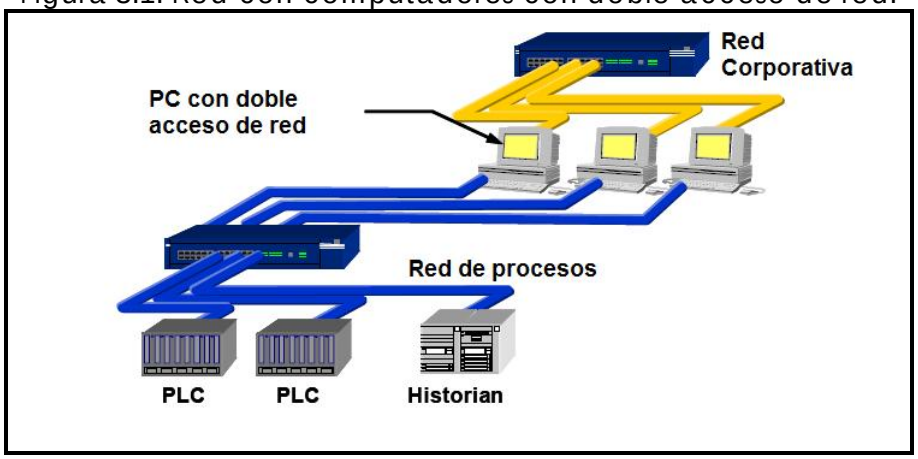
Otro factor de riesgo son las redes inalámbricas. Se debe evitar realizar tareas críticas usando este medio de conexión en los sistemas de control de procesos cuando sea posible. Es recomendable limitar el uso de estas redes para capturar datos solamente. En todo caso, es muy importante evitar conexiones no deseadas en la red inalámbrica usando todas las medidas disponibles.

En el 2005 fue realizada una investigación por el centro de coordinación de la seguridad de la infraestructura nacional del Reino Unido (NISCC, por sus siglas en inglés de National Infraestructure Security Coordination Centre) en la que se recogió la información del manejo de seguridad de industrias relacionadas con la producción eléctrica, alimentos, petróleo, productos químicos, a lo largo de Europa y Norteamérica. La información recolectada en forma de entrevistas personales, manuales de políticas de seguridad, reportes de auditoría de seguridad y literatura en productos de seguridad, arrojó como resultado a 8 arquitecturas recomendables para la implementación de seguridad en redes que tengan procesos industriales involucrados. Cada una de ellas es descrita a continuación:

3.2.1.1. Computadores con doble acceso a red.

Una solución de seguridad comúnmente propuesta es la instalación de dos interfaces de red en los computadores que tengan acceso a la red corporativa y a la red de control de procesos [23]. Esta solución es la más fácil de implementar y la menos costosa pero en términos de seguridad presenta un alto riesgo de intrusión por lo que es la menos recomendable. Su implementación podría ser útil en redes muy pequeñas con un nivel de seguridad mínimo. En la figura a continuación se muestra la implementación de una de red con computadores con doble acceso a red.

Figura 3.1. Red con computadores con doble acceso de red.

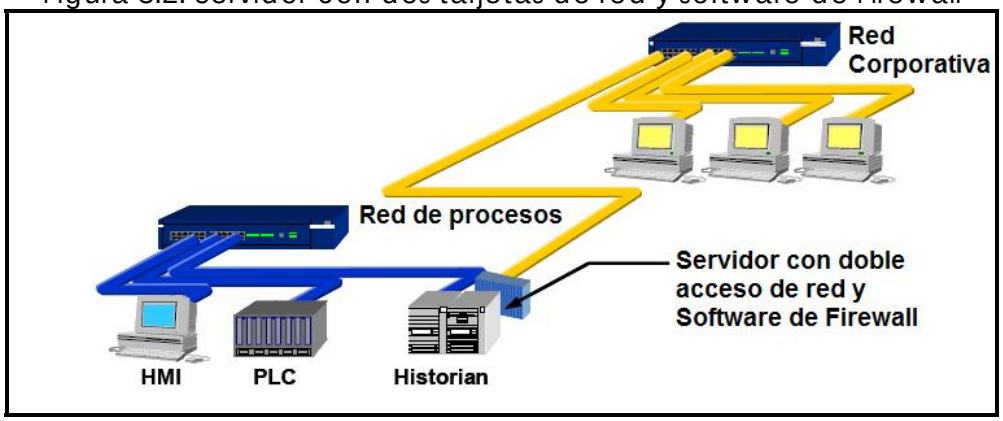


Fuente: NISCC [23]

3.2.1.2. Servidor con doble acceso de red y Software de Firewall

Una variación de la arquitectura previa es la instalación de un servidor que tenga un software de Firewall basado en hosts y con dos interfaces de red para el acceso a las distintas redes. Comúnmente este servidor funciona como el historian de la red SCADA a la vez que sirve para el acceso de las dos redes [23]. La idea es que el único tráfico compartido entre la red corporativa y la red SCADA sea los datos históricos de los eventos en los procesos controlados, así si se usa un firewall personal en cada máquina, que permita solo este tipo de datos, se podrá usar en el servidor un firewall de bajo presupuesto, consiguiendo un sistema de seguridad mejorado con bajos recursos. En la figura a continuación se muestra esta configuración de red.

Figura 3.2. Servidor con dos tarjetas de red y software de Firewall



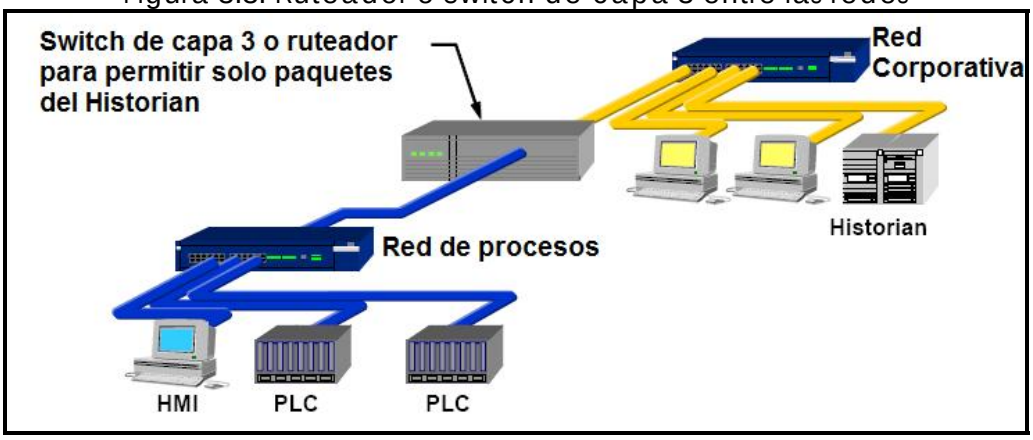
Fuente: NISCC [23]

En esta arquitectura se tiene las mismas vulnerabilidades de seguridad que en el caso anterior, lo que se consigue es mejorar la configuración de seguridad con el uso de los mismo equipos que en el caso anterior. El principal problema que se presentaría es el uso de la información compartida entre las redes, lo que representa un latente peligro en caso de que usuarios malintencionados de la red corporativa consiguiesen al acceso a través del servidor y logren manipular parámetros de los dispositivos de la red de procesos.

3.2.1.3. Ruteador o Switch de capa 3 entre las redes.

Es recomendado el uso de un ruteador o un switch de capa tres entre las redes corporativas y la red de procesos que contenga los filtros básicos para el control de tráfico entre ellas, que básicamente se limitaría al paso de paquetes con la información de los datos históricos para el historian. Muchos de estos dispositivos funcionan como “Firewalls Packetfilters” en esta configuración, es decir están implementados principalmente para limitar el paso a cierto tipo de paquetes y no desarrollan, como parte de su trabajo, la protección contra un ataque o una intrusión más sofisticada, como el escaneó de puertos, por ejemplo.

Figura 3.3. Ruteador o Switch de capa 3 entre las redes



Fuente: NISCC [23]

Este diseño de red es solo seguro en el caso de redes corporativas conocidas con bajos niveles de vulnerabilidades aunque por otro lado es conocido que ahora en el mercado se puede encontrar ruteadores con altas capacidades para implementación de firewalls, lo que representa un ahorro en su uso.

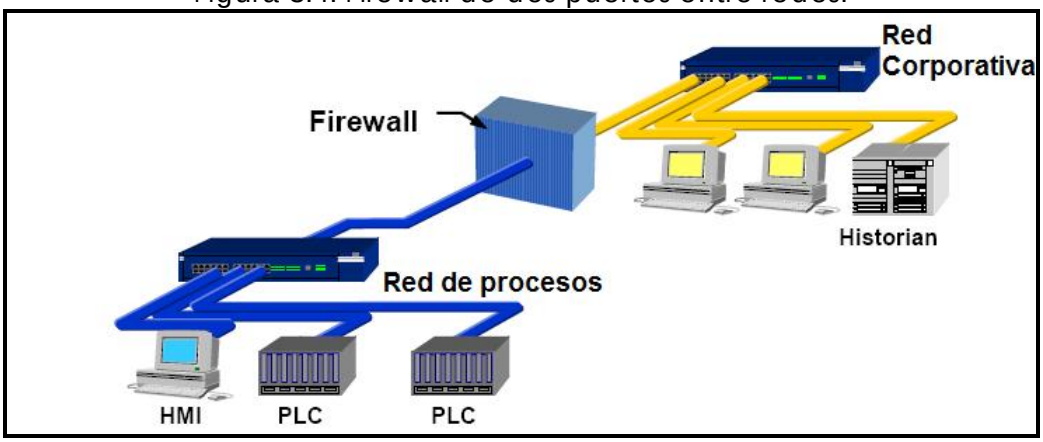
3.2.1.4. Firewall de dos puertos entre redes.

Un importante avance de seguridad puede ser logrado con la introducción de un firewall de dos puertos entre las redes corporativa y de control de procesos. La mayoría de Firewalls en el mercado hoy en día ofrecen como una característica básica la inspección para todos los paquetes TCP y UDP que cursen el firewall, además de una aplicación proxy para servicios de Internet, tales como FTP, HTTP y SNMP. Cuando estos firewalls son configurados con estrictas reglas es un hecho que se reduce en gran medida el riesgo de ataques hacia las redes de procesos en la seguridad SCADA [23].

Con esta arquitectura de red se presentan nuevos problemas que solucionar. El primero de ellos es determinar en qué red se instalarán los servidores que son compartidos,

como por ejemplo el historian. Si el historian reside en la red corporativa debe existir una regla en el firewall que permita al historian comunicarse con los dispositivos de campo que se encuentran en la red de procesos y ahí nace una vulnerabilidad para el caso en que usuarios malintencionados puedan acceder mediante suplantación de direcciones de IP (aparentando ser el historian) hacia la red de procesos. Para el caso en que el historian se ubique en la red de procesos se debe crear una regla en el firewall que permita el acceso de los hosts de la red corporativa hacia la red de procesos con lo que esta red queda aún más vulnerable e inclusive se correría el riesgo de la propagación de virus o gusanos hacia ella.

Figura 3.4. Firewall de dos puertos entre redes.



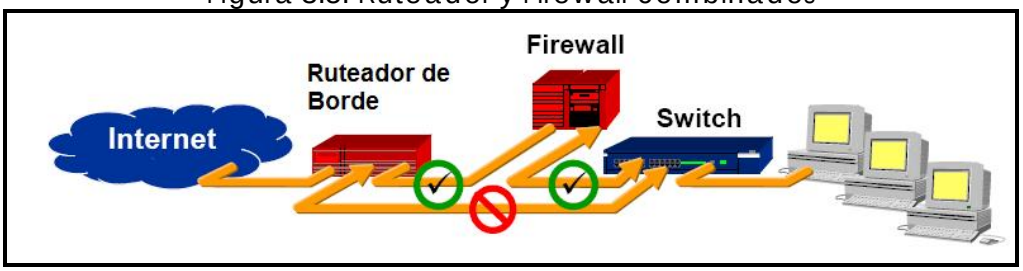
Fuente: NISCC [23]

3.2.1.5. Combinación de ruteador y firewall entre redes.

Un diseño de arquitectura un poco más sofisticado es el uso de un ruteador y un firewall combinados en el borde de la red, donde el ruteador se sitúa delante del firewall y ofrece servicios de filtrado de paquetes para los paquetes entrantes hacia el firewall,

mientras que este maneja los problemas más complejos mediante la inspección del estado de los paquetes y la utilización de técnicas de proxy [23].

Figura 3.5. Ruteador y Firewall combinados



Fuente: NISCC [23]

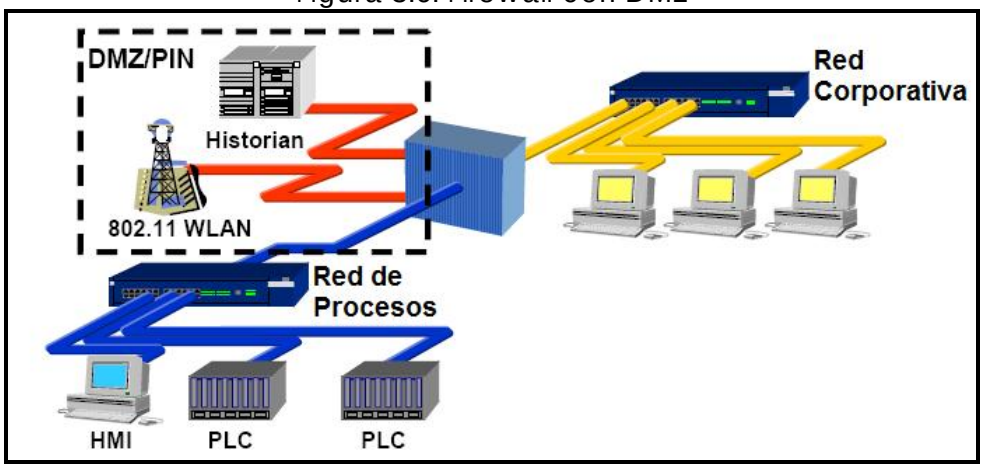
Este tipo de diseño es muy popular en las redes conectadas a internet debido que permite un rápido manejo y análisis del conjunto de paquetes entrantes por parte del ruteador, especialmente en el caso de ataques que provoquen denegación del servicio, y además reduce la carga de procesamiento de paquetes para el firewall. Esta configuración de red también ofrece defensa mejorada debido a que ahora hay dos dispositivos que el atacante tiene que superar para ingresar a la red.

Aunque esta arquitectura es muy popular en el mundo de las redes corporativas y en las tecnologías de la información, rara vez se encuentra se la encuentra en el mundo de las redes SCADA, debido al hecho de que la red corporativa y de control de procesos quedarían sujetas a la misma subred y cuando se utiliza un ruteador dentro de SCADA no es con fines de seguridad sino exclusivamente para separar las redes, evitando así mayores retardos en el manejo de la información.

3.2.1.6. Firewall con zona desmilitarizada (DMZ) entre redes

Una mejora importante que se ha desarrollado es el uso de firewalls con la facilidad de implementar zonas desmilitarizadas independientes de la red corporativa o de control de procesos. En una zona desmilitarizada se colocan los elementos de críticos de la red, como por ejemplo el historian o puede usarse otra zona para el acceso a elementos inalámbricos o remotos, que siempre suponen un punto vulnerable para la seguridad de la red. Las subredes creadas en zonas desmilitarizadas con el objetivo de manejar la información de los procesos que se llevan a cabo en el resto de la red a menudo son llamadas como redes de proceso de información o PIN (por sus siglas en inglés de Process Information Network) [23].

Figura 3.6. Firewall con DMZ



Fuente: NISCC [23]

Para crear una DMZ se requiere que el firewall tenga tres o más interfaces de red adicionales a los interfaces público y privado. En uno de ellos se conectaría la red corporativa, al segundo, la red SCADA y al tercero los dispositivos que sean inseguros o compartidos como el servidor historian o un AP (Access Point) inalámbrico. En el

interface privado del firewall puede ser utilizado para los servidores de la red corporativa.

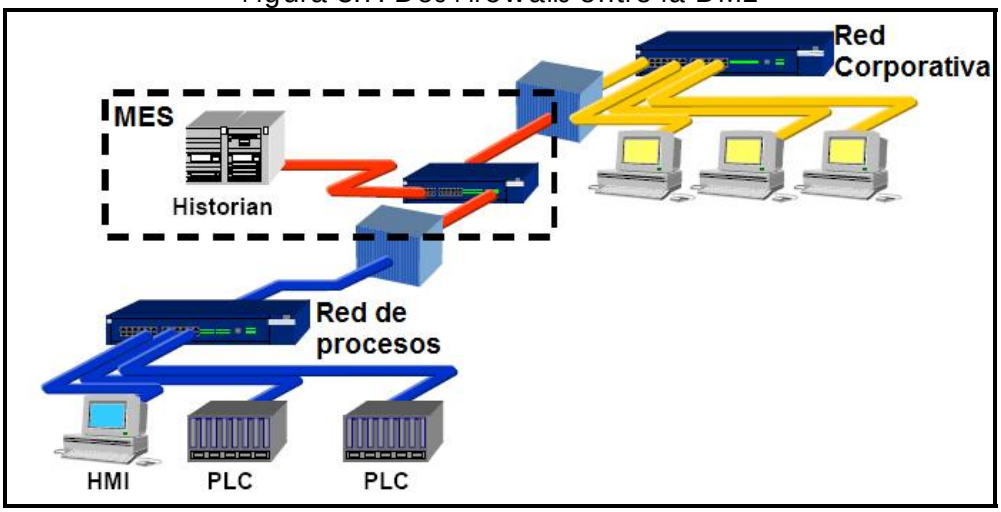
Con el uso de la DMZ no existe comunicación directa entre las redes corporativas y la red de procesos y cada una de ellas termina en la red DMZ. En los firewalls más sofisticados se puede implementar varias zonas desmilitarizadas y mediante el seteo de reglas en el software se puede determinar que tráfico es permitido entre las redes que se conecten a ellas.

La seguridad en esta configuración de red corre riesgo cuando un computador en la zona desmilitarizada está comprometido con alguna intrusión y puede ser usado para iniciar un ataque hacia la red de control de procesos. Este riesgo puede ser minimizado si setea como una de las reglas del firewall que el tráfico solo puede ser iniciado por dispositivos que residen en la red de control de procesos. Otro inconveniente en este tipo de arquitectura es el uso de reglas que en cierto punto se vuelven muy complejas, además que la implementación de un firewall con varios interfaces de red se vuelve muy costoso.

3.2.1.7. Dos firewalls entre la DMZ.

Una variación al caso anterior es el uso de una DMZ que tenga un par de firewalls posicionados entre la red de control de procesos y la red corporativa. Los servidores en común (tales como el historian) están situados entre los firewalls creando una subred en la DMZ que puede ser usada como un nivel MES (Manufacturing Execution System) del sistema SCADA. De manera similar al caso anterior el flujo de información es analizado cuando intenta ser compartido entre las redes pero en este caso el acceso a la red de procesos no se verá afectado por un servidor comprometido con la red corporativa [23].

Figura 3.7. Dos Firewalls entre la DMZ



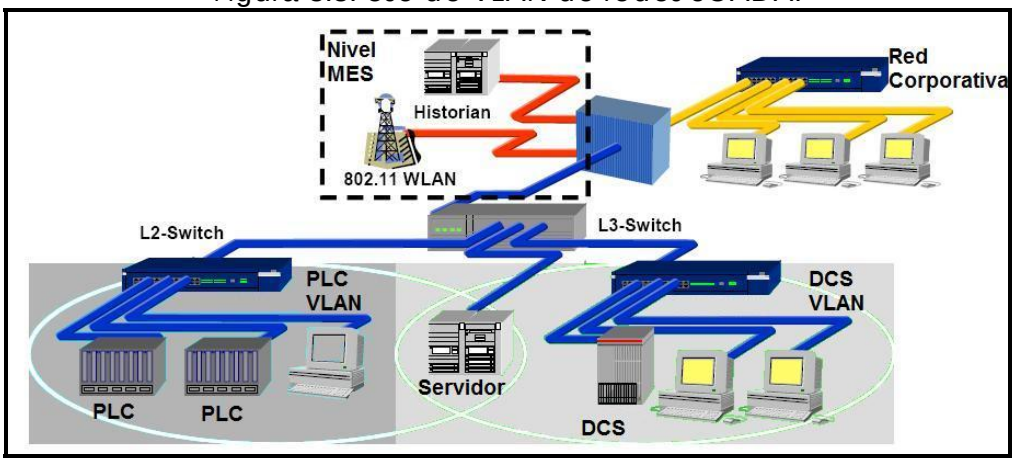
Fuente: NISCC [23]

Esta configuración permite que las subredes de procesos y corporativas tengan dispositivos responsables independientes y se pueda manejar cada una de ellas con diferentes reglas y administración permitiendo un mejor desempeño ya agilidad en su manejo. De hecho, este diseño ha sido recomendado por varios organismos de seguridad por sus ventajas en los estándares de seguridad e independencia entre redes que presenta. Una variación útil es el uso de un ruteador entre la red corporativa y el firewall hacia la DMZ, para cubrir posibles deficiencias de seguridad mediante el filtrado de paquetes. Esta configuración presenta una buena solución para casos que demanden altas prestaciones de seguridad o cuando se necesite una clara independencia en el manejo de las redes pero su principal desventaja es la complejidad en su manejo y el incremento en costo que esta representa.

3.2.1.8. Uso de VLAN's combinadas con un firewall.

Como se ha visto hasta ahora las redes SCADA han sido tratadas como entidades independientes tratando de aislarlas del resto y de mantenerlas bien comunicadas dentro de ellas mismas, sin embargo, hay ciertos casos en los que existen áreas funcionales o celdas en donde no es necesario una comunicación interna o se requiere una separación. Siguiendo en la línea de las arquitecturas anteriormente presentadas se puede conseguir una solución similar para este tipo de configuraciones, mediante el uso de redes virtuales VLAN (Virtual LAN) dentro de las mismas subredes, como se puede apreciar en la figura a continuación.

Figura 3.8. Uso de VLAN de redes SCADA.



Fuente: NISCC [23]

Un Switch de capa 3 o un ruteador se encarga de dividir de manera física la red de control de procesos y mediante el uso de switches se configura las VLAN's para lograr conectividad dependiendo de las funciones designadas a cada área. El ruteador se encarga de filtrar los paquetes entre las subredes virtuales. Las VLAN's previenen la propagación del tráfico no deseado a través de toda la red, así se puede dividir el

tráfico que utiliza la red de ejecución de procesos o PLC VLAN, de la red de control de procesos o DCS (por sus siglas en inglés de Distributed Control System), mientras que la red destinada a ejecutar tareas de programación de manufactura (MES) se encuentra en la zona desmilitarizada y puede también compartir tráfico con la red corporativa, mediante el firewall. En la figura anterior se puede apreciar esta disposición.

Se puede utilizar variaciones a esta configuración de red para permitir la implementación de niveles adicionales propios de los sistemas SCADA, como por ejemplo en la zona desmilitarizada se puede usar el servidor historian junto con una red de gestión y planeamiento de recursos o ERP (por sus siglas en inglés de Enterprise Resource Planning), y se puede crear, por otra parte, una VLAN con equipos que se trabajen en la extensión de una red WAN y conformen una red MES y otra para los elementos de control (DCS) con los dispositivos de campo.

Dentro de estas ocho configuraciones de red presentadas se obtiene cierto un nivel de ventajas asociadas en cada una de ellas, de tal manera que se ha analizado a cada arquitectura en función de la seguridad, escalabilidad y facilidad de administración y se ha resumido este análisis en una tabla con una valoración de cada característica del 1 al 5, correspondiendo el 1 al nivel de calificación más bajo.

Tabla 3.1. Estimación de la valoración de las características de cada una de las arquitecturas descritas.

Arquitectura	Seguridad	Administración	Escalabilidad
PC con doble acceso de red	1	2	1
Servidor con doble acceso de red y software de Firewall	2	1	1
Ruteador o Switch de capa 3 entre las redes	2	2	4
Firewall con dos puertos	3	5	4
Combinación de ruteador y firewall entre redes	3.5	3	4
Firewall con DMZ entre redes	4	4.5	4
Dos firewalls entre la DMZ	5	3	3.5
VLAN combinadas con firewall	4.5	3	5

Fuente: NISCC [23]

El conjunto de las prácticas de seguridad citadas anteriormente resultan útiles pero sin embargo no representan un método infalible de seguridad debido a que es posible que algún código malicioso u otro tipo de ataque atraviesen las distintas zonas de la red y logren penetrar en ella hasta el nivel de control de procesos y afecten su funcionamiento, principalmente por el hecho de que la mayoría de Firewalls e IDS no están diseñados adecuadamente para manejarse en el entorno SCADA y no son óptimos para manejar sus protocolos más comunes o también introducen una latencia al sistema afectando a procesos con tiempos críticos de operación en tiempo real; Estas situaciones no muy usuales en otros entornos de redes de datos resultan vitales para los procesos en los sistemas SCADA y para hacer más crítico el asunto, existe muy poca información disponible acerca de cómo exactamente los Firewalls o IDS deben funcionar en arquitecturas, configuraciones y manejos SCADA. En los párrafos a continuación se define algunos parámetros generales bajo los cuales deberían funcionar los dispositivos de seguridad dentro de un sistema SCADA para hacer de este un sistema confiable.

3.3. Características en servidores y equipos.

3.3.1. Firewalls.

Este dispositivo es un foco de seguridad para cualquier tipo de red de datos y por lo tanto requiere dedicada atención, no solo para su puesta en funcionamiento sino también para su consecuente operación, manejo y monitoreo de sucesos, además de ser necesaria una constante actualización para mantener sus protecciones vigentes. La complejidad de sus tareas no debería ser subestimada pero desafortunadamente en las redes SCADA lo son y en muchos casos ni siquiera se piensa en la posibilidad de la instalación de uno de ellos.

Por otra parte, actualmente los fabricantes de firewalls están enfocados en la seguridad para el acceso a internet y aplicativos que usan protocolos propios de sistemas corporativos descuidando, de esta forma, a los protocolos que se desempeñan en el medio industrial, tales como MODBUS, PROFIBUS, DNP3, etc. Y como resultado se obtiene que muy probablemente estos firewalls no se encuentren en la capacidad de filtrar los paquetes SCADA, principalmente en la capa de aplicación y la única opción disponible es el filtrado en función de la dirección de red con lo que el firewall quedaría limitado a funcionar como un ruteador. Es decir, si se tuviera un firewall diseñado para redes SCADA se tendría, por ejemplo en una red que funcione con MODBUS, la opción de bloquear los comandos de escritura hacia los dispositivos de campo desde la zona DMZ y permitir solo los de lectura (de acuerdo a las arquitecturas 7 u 8 descritas en el apartado 3.2.1.).

Cabe recalcar que existe una solución de software de código abierto para funcionar como firewall de una red MODBUS bajo el kernel de Linux desarrollado por Matthew Franz y Venkat Pothamsetty de Cisco Systems Critical Infraestructure Assurance Group

(CIAG), que se encuentra disponible de manera gratuita en internet en la dirección http://modbusfw.sourceforge.net/

3.3.2. Servidor de datos Historian.

Este servidor se implementa en computadores con altas prestaciones para almacenamiento, consultas y procesamiento de datos, inclusive en algunas ocasiones es instalado con un sistema de arreglo de discos con capacidades de "mirroring" (sistema mediante el cual se mantiene una réplica exacta de los discos de almacenamiento para asegurar la disponibilidad de los datos en caso de fallas), lo cual es recomendable. Además estas máquinas suelen estar conectadas con un buen canal de comunicaciones para mantenerse disponible para toda la red, tanto a nivel corporativo como de control de procesos.

La ubicación de este servidor dentro de la red tiene importantes implicancias sobre su estructura de seguridad. Como se puede notar de lo descrito en los apartados anteriores de este capítulo, la existencia de servidores compartidos entre las redes corporativa y de procesos, tales como el historian, puede tener un impacto significativo en el diseño y configuración del firewall. En sistemas con un diseño separado en tres zonas la ubicación de este servidor es relativamente simple pero en sistemas con dos zonas el diseño de seguridad se convierte en algo un poco más complejo por el hecho de que se tiene que decidir en cuál de las subredes se ubicará el servidor historian.

Al colocar el servidor historian en el lado de la subred corporativa con el firewall a su ingreso significa que un buen número de protocolos inseguros, como el MODBUS/TCP, pueden pasar a través del firewall y que todo los reportes de los dispositivos de control hacia el historian están expuestos para la red corporativa y por ende para usuarios maliciosos. Por otro lado, al poner el historian en el lado de la red de control de procesos significa que los protocolos típicos de una red corporativa, como HTTP o SQL,

tendrán completo acceso hacia ella y está quedará expuesta nuevamente a usuarios malintencionados que deseen ingresar desde la red corporativa haciendo uso de estos protocolos.

La mejor solución disponible y recomendable es evitar los sistemas que tengan su red separada en dos zonas y en su lugar usar sistemas de tres zonas con el uso del historian en la parte desmilitarizada [23]. Inclusive esta solución puede representar un problema si se tiene una gran cantidad de accesos de los usuarios corporativos con consultas de datos hacia el historian lo cual demandaría altas capacidades de procesamiento de parte del firewall. Una solución sugerida puede ser el uso de un servidor recolector de datos en la parte de control y un servidor espejo a este conectado hacia la red corporativa para las consultas de usuarios, por supuesto que esto requiere un camino dedicado a través del firewall para permitir la comunicación de los servidores, pero si es realizado correctamente el riesgo es mínimo.

3.3.3. Dispositivos de red.

La interconexión entre las distintas zonas y los distintos elementos dentro de cada una de las zonas está a cargo de los dispositivos de red, mediante estos se controla el tráfico de datos, por esta razón, ellos representan un importante factor a considerar en la seguridad del sistema. Si bien el firewall se encarga de seleccionar los datos que pasaran a través de la red, de acuerdo con las reglas configuradas, los dispositivos de red, como ruteadores o switches, pueden realizar un filtrado básico de los paquetes además de su encaminamiento.

En cada una de las configuraciones descritas en los apartados anteriores los ruteadores pueden y deberían ser usados con listas de acceso para filtrar en una primera instancia los paquetes que intenten ingresar con acceso a puertos que no estén habilitados. También mediante el uso de NAT (Network Access Translation) se verificaría que solo las

máquinas autorizadas puedan pasar paquetes entre la red corporativa y la red de control de procesos. Además uno de los ruteadores será el encargado de interconectar al sistema SCADA con Internet y tendrá que admitir o denegar los accesos remotos por lo que la configuración de enrutamiento en este debe ser muy cuidadosa y un filtrado de paquetes también sería útil.

En el caso de los switches sus características principales deben ser básicamente las de un puente entre las máquinas locales para la mayoría de las configuraciones de red antes descritas pero en el último de los casos, en el que se plantea la realización de VPN's entre las subredes se necesita que sean switches administrables que faciliten esta implementación. Los usuarios que accedan remotamente deberán formar parte de una de las VPN's de tal manera que en uno de los switches de la red se debe habilitar esta opción de acceso.

Tanto en el uso de switches como de ruteadores, cuando se acceda de manera remota se tiene que dar dos niveles de autenticación. El usuario remoto primero obtiene el acceso hacia la red corporativa y luego mediante el firewall, hacia la red de control de procesos. Se puede usar una VPN con acceso vía Dial-Up para llegar a la red corporativa y en el caso de empresas que no permitan el paso a través del firewall hacia la red de control de procesos se puede usar una nueva VPN hacia este destino.

3.4. Acciones de seguridad para los sistemas SCADA.

3.4.1. Políticas y procedimientos

La implementación de las políticas que se adopten en la empresa para mantener protegidos al sistema SCADA, en conjunto con la red corporativa, radica en la disposición de la topología de la red escogida y el tratamiento que tengan los paquetes que ingresan a la red por parte de las reglas establecidas en el firewall. Una

configuración básica del firewall es denegar todos los ingresos a los puertos permitiendo solo a aquellos protocolos que vayan a ser utilizados en el sistema. Esto funciona sin problema excepto por el hecho de que muchos de los protocolos usados en SCADA tienen versiones con fallas de seguridad, es decir, son inseguros y por ende necesitan especial atención.

Una vez que la arquitectura de la red se haya establecido y el firewall sea ubicado empieza el trabajo de determinar exactamente que tráfico se quiere permitir para que circule hacia el sistema. La premisa de todas las empresas es denegar todo el tráfico y habilitar solamente los puertos que permitan el tráfico de los protocolos utilizados por el sistema, pero el problema va más allá, cuando fallas de seguridad pasan a través de los protocolos utilizados, como por ejemplo en el servidor historian se puede tener una base de datos que atienda peticiones SQL (Structure Query language) desde los computadores de la red corporativa, pero desafortunadamente SQL es también utilizado por el gusano Slammer para efectuar ataques, de esta manera si se habilita el tráfico para estas peticiones también se habilitaría una puerta de entrada para este gusano. Por otro lado en los protocolos más utilizados en las redes SCADA, como MODBUS/TCP, Ethernet Industrial/IP o ICCP se han ido descubriendo "huecos" de seguridad en sus estructuras de transporte de datos y esto sumado al hecho de que los firewalls comerciales actuales no han sido diseñados para analizar el tráfico típico de una red SCADA, resulta en un significante riesgo en la seguridad de que preocuparse en estas redes.
Para evitar algunos de los problemas que se puedan presentar a nivel de transporte de datos en los protocolos se establecen algunas estrategias que permitan prevenir, detectar y defenderse de acciones no deseadas:

- Mediante el establecimiento de derechos y jerarquías de acceso que permitan limitar el ingreso de usuarios hacia los puntos neurálgicos de la red y un registro de cuando alguno de ellos ha ingresado y los cambios que ha realizado.

- Con la encriptación de datos que se emiten desde las estaciones remotas hacia los nodos centrales o viceversa, de por lo menos dos niveles de autenticación.
- Por medio del filtrado de los paquetes entrantes analizando su cabecera para determinar si su origen es conocido o no. Muchos sistemas SCADA podrían trabajar con protocolos para el transporte de datos en TCP/IP o en UDP/IP, de tal manera que en estos casos se debería filtrar cualquier otro tipo de tráfico entrante.
- Con caminos de acceso predeterminados dedicados para cierto tipo de transacciones. Lo cual se puede realizar mediante VPN's como en la última estructura de red planteada en el apartado 3.2.1.8.
- Mediante programas de vigilancia de otros programas que son ejecutados y/o realizan transacciones de datos a través de la red como un antivirus.
- Estableciendo protocolos entre las redes de control y DMZ distintos a los que se establezcan entre la red corporativa y DMZ, de tal manera que si existe algún tipo de intento de algún usuario malicioso, de pasar a través de la red desmilitarizada, esta sea bloqueada de facto.
- La red de control de procesos no debería tener ningún tipo de acceso desde o hacia Internet, inclusive no debería existir algún tipo de conexión hacia internet a pesar de que no se use una red desmilitarizada o algún tipo de firewall para el acceso.

Además de estas reglas generales, útiles y prioritarias a ser implementadas, en un sistema SCADA típico que combine las redes corporativas con la red de control de procesos, se debe establecer las reglas que el firewall aplicará a cada uno de los protocolos permitidos. Las necesidades y mejores prácticas a implementarse varían significativamente entre las empresas para cualquier protocolo dado y deberían ser analizadas en base a ella. A nivel industrial se conocen algunos estándares que funcionan a manera de plantilla para el análisis de cada protocolo utilizado en la industria.

Uno de los protocolos más útiles en la implementación de los sistemas SCADA es SNMP (Simple Network Management Protocol). Usado para servicios de reporte del estado de red entre dispositivos tales como ruteadores, swtiches, PLC, etc. A pesar de ser extremadamente útil en su servicio este protocolo es completamente débil en cuestión de seguridad, las versiones 1 y 2 usan claves de acceso sin encriptación para la lectura y escritura de dispositivos, en algunos casos inclusive las claves son bien conocidas y no pueden ser cambiadas. La versión 3 ha resuelto estos problemas y es considerablemente más seguro pero su uso es todavía limitado. Además las implementaciones SNMP en dispositivos embebidos han mostrado serios defectos en muchas instancias, de esta manera los comandos SNMP, desde y hacia la red de control de procesos deberían ser prohibidos si no se implementa una red de gerenciamiento segura.

Los sistemas SCADA al estar desarrollados en conjunto con redes empresariales están sujetos a la utilización del protocolo NAT (Network Address Translation), mediante el cual se puede hacer uso de direcciones IP privadas dentro de la red y publicar solo un número limitado de direcciones mediante el dispositivo de borde de la red. Este protocolo fue creado con la intención de reducir el número de direcciones IP necesarias para reconocer los dispositivos en las redes a nivel mundial. Actualmente NAT es promovido como una característica de seguridad debido a que el tráfico que ingresa a la red aparentemente termina en el dispositivo de entrada hacia ella, de tal manera que NAT funciona también para camuflar la identidad de los hosts de la red al mundo exterior. Si un dispositivo dentro de la red tiene asignada una dirección IP privada, entonces el ruteador no debería permitir el paso directo del tráfico que trata de ingresar desde Internet, la única forma de comunicar a este determinado host es mediante la conexión NAT.

Utilizar NAT como una técnica de seguridad puede tener consecuencias negativas en ciertos casos como el incremento de la dificultad para validar la seguridad del set de reglas del firewall debido a la naturaleza dinámica de las conexiones abiertas y las

combinaciones puerto/dirección IP que utiliza el firewall para realizar la "traducción" de direcciones. Además ciertos protocolos son desentramados por NAT por la falta de direccionamiento directo. Por ejemplo el protocolo OPC (OLE for Process Control) requiere un software adicional que inserte ciertos campos cuando pasa a través de NAT. De igual manera algunos protocolos como Fieldbus o EtherNet industrial/IP presentan problemas por el hecho de que el tráfico multicast en el que están basados para ofrecer completamente sus servicios no es soportado cuando se trabaja con NAT.

Los dispositivos de gestión en las redes SCADA representan un punto neurálgico para estos sistemas de tal manera que se deben tener bien en cuenta las recomendaciones que en este capítulo se plantean y si bien pueden existir alternativas válidas, en el desarrollo de este texto se ha pretendido plantear todas las disponibles para una implementación segura SCADA. Además de la arquitectura escogida no se debe pasar por alto las políticas de seguridad para así garantizar en un último nivel la inviolabilidad de la red.

4. IMPLEMENTACIÓN DE UN SISTEMA SCADA PROTOTIPO.

En este capítulo se desarrolla la descripción de un sistema de monitoreo remoto que consta de elementos de campo, un medio de transmisión y un software de gestión. No se abarca el nivel de planeamiento empresarial E.R.P. para mantener la simplicidad del ejemplo. El prototipo supone realizar el monitoreo de una estación de trabajo remota de la que se requiere conocer el estado de los parámetros que la mantienen funcionando correctamente y la actuación sobre algunos de ellos.

4.1. Descripción del prototipo.

El prototipo está dispuesto para realizar la adquisición de los parámetros de:

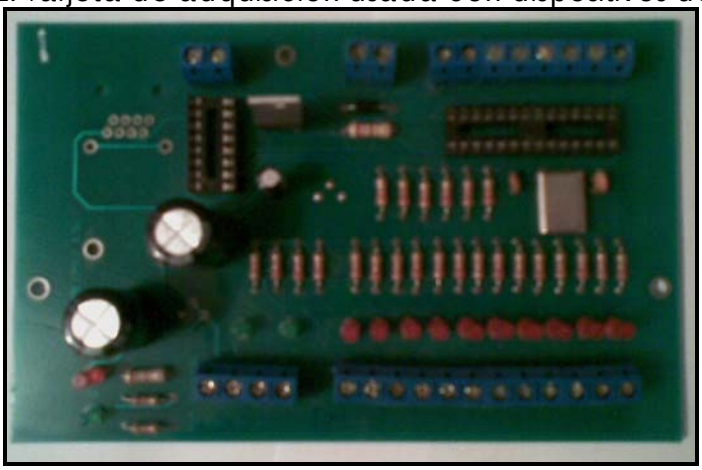
- Nivel de voltaje de alimentación de los equipos ahí instalados,
- nivel de voltaje de las baterías de respaldo,
- estado del sistema de alimentación de energía,
- estado de la puerta de acceso al lugar y ventanas y,
- sensado de los dispositivos de seguridad.

Para realizar estas tareas el sistema consta de los siguientes dispositivos de campo:

- Entradas digitales para sensar los estados de tipo on/off como puertas y ventanas.
- Entradas analógicas para sensar los niveles de alimentación de voltaje en las baterías y energía de la red.
- Salidas digitales para los actuadores en caso de que se quiera realizar el cambio del ingreso de alimentación.

Todo esto es desarrollado a nivel de dispositivos de campo mediante una tarjeta de adquisición de datos desarrollada para el efecto. En la figura a continuación se muestra la imagen de la tarjeta electrónica utilizada para este fin.

Figura 4.1. Tarjeta de adquisición usada con dispositivos de campo

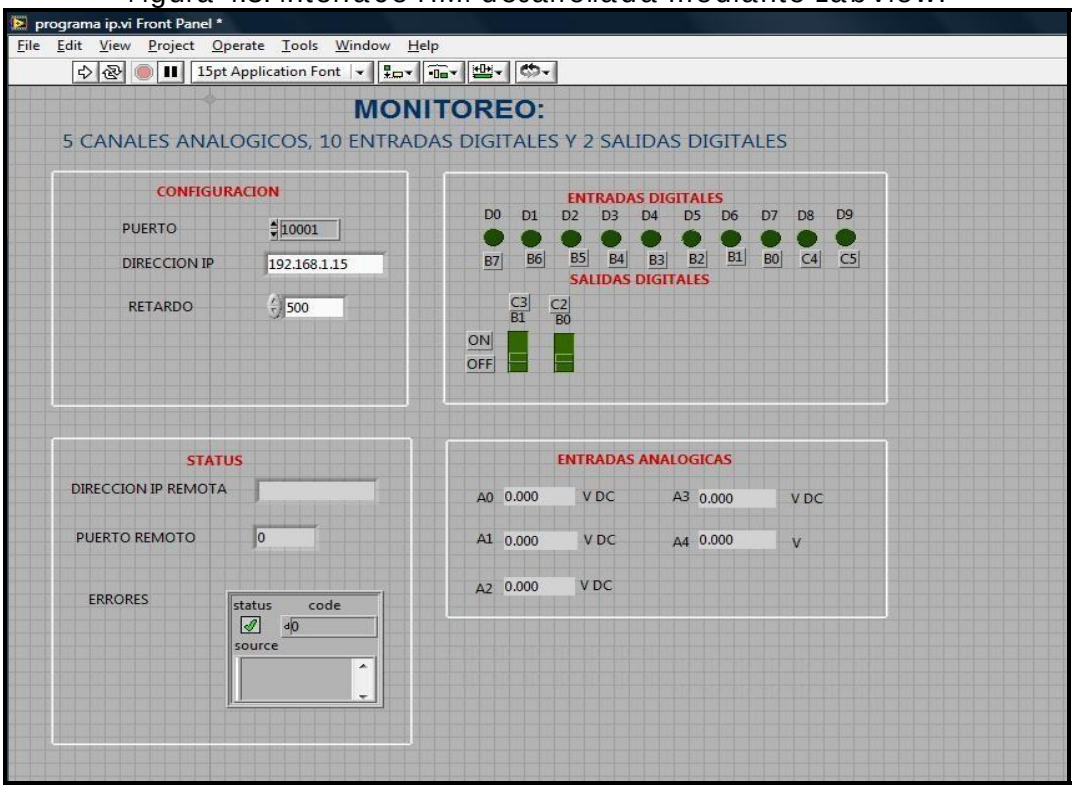


Para llevar a cabo la remotización del sistema se realiza la comunicación entre la adquisición de datos y el centro de control mediante el protocolo UDP/IP transmitiendo sobre un medio Ethernet. Los datos adquiridos y comandos que recibe la tarjeta de son transmitidos por un adaptador de red Ethernet con especificaciones industriales. El interface de red se comunica con los dispositivos de campo mediante un bus RS-232 para adquirir los datos sensados. En la figura a continuación se puede apreciar el interface de red con su salida RS-232 utilizada para la conversión del medio de transporte.

Figura 4.2. Interface de red con conversión de medio Ethernet a RS-232

El control del sistema es efectuado mediante una interface programada en el programa LabView, que es una herramienta de desarrollo sacada al mercado por National Instruments, El interface HMI incluye cuadros de texto en donde se especifica las direcciones IP de los dispositivos de campo instalados con los cuales se va a mantener comunicación. En la figura a continuación se muestra la captura de una pantalla del programa en modo de ejecución.

Figura 4.3. Interface HMI desarrollada mediante LabView.



Este sistema prototipo muestra a escala como se desarrollaría un SCADA en la práctica, con cada uno de sus niveles de implementación, a este hay que agregarle el detalle de los sistemas de seguridad, que fácilmente puede ser llevada a cabo en una red empresarial gracias a que transmite sus datos por un medio Ethernet y utiliza como protocolo de transporte a UDP, para soportar el acceso en tiempo real.

5. CONCLUSIONES Y RECOMENDACIONES.

- La evolución de la tecnología ha proveído el crecimiento y mejora de los procesos industriales y por ende los sistemas SCADA necesarios para mantener dicho crecimiento, controlado, han ido evolucionando exponencialmente por lo que ahora estos sistemas presentan gran complejidad. Por lo tanto es necesario prestar dedicado estudio y atención a su implementación en cada uno de sus niveles para no dejar falencias en su desarrollo.

- A pesar de que en la industria actualmente se encuentran sistemas realizados a medida con soluciones propietarias, es necesario buscar la migración de estos sistemas hacia estándares abiertos que permitan una fácil evolución y mejora de los procesos automáticos.

- La implementación de los medios de comunicación que soporten el transporte de datos en los sistemas SCADA tiene que ser escogido en función del área que ellos abarquen y qué nivel de la planta en especifico se tenga por objetivo, así por ejemplo el nivel de campo se podrá realizarlo con protocolos que funcionen en las capas bajas del modelo OSI mientras que la gestión y el gerenciamiento con protocolos que lleguen hasta los niveles de presentación en OSI.

- Los sistemas SCADA que ocupen más de una localidad en sus desempeños pueden ser interconectados mediante redes de grandes proveedores de transporte de datos siempre y cuando la comunicación juegue un papel predominantemente a nivel de gestión y gerenciamiento de las empresas pero no cuando las distintas localidades dependan una de la otra para llevar a cabo los procesos de producción, ya que en este caso los datos a transmitir tendrán muy poco “payload” en las tramas por lo que se puede estar contratando recursos innecesarios. En este caso se debe utilizar medios de transporte de más bajo nivel en el modelo OSI y que por lo general son facturados por cantidad de

Bytes transmitidos más que por anchos de banda en Kbps. Como por ejemplo tecnologías como GSM o GPRS a mano de operadoras móviles.

- Los medios usados entre los niveles de campo y control de procesos deben mantener canales confiables y si es posible con redundancia en el transporte, debido a que los protocolos usados para mantener el monitoreo y gestión de los sistemas SCADA funcionan en tiempo real y la retransmisión de paquetes debe ser mínima o en su defecto nula.

- Las pautas que se indican para seguir en cuestión de seguridad deberían ser consideradas como primordiales y no dejar de ser desarrolladas bajo ningún concepto caso contrario la red es solo tan útil como podría ser una computadora completamente infectada de virus, ya que está no durara en su funcionamiento ni lo que se tarde en recuperar la inversión de su realización.

- Cualquier sistema SCADA desarrollado como solución propietaria debe acogerse a los estándares conocidos y recomendados para cada caso y nivel de operación inclusive mitigando cuestiones administrativas como la falta presupuesto, porque si no, cuando crezca la red se puede requerir ampliar el sistema y lo que fue alguna vez una solución se convertiría en un impedimento.

6. BIBLIOGRAFÍA.

- [1] Wikipedia. SCADA. 2008. Disponible en World Wide Web: http://es.wikipedia.org/wiki/SCADA.
- [2] Universidad de Cataluña. Sistemas de visualización industrial. 2006.
- [3] Ruiz Olaya, Andrés Felipe. Implementación de una red MODBUS/TCP. Universidad del Valle, Facultad de Ingeniería. Santiago de Cali. 2002.
- [4] Introduction to MODBUS, Technical Tutorial. 2002. Disponible en World Wide Web: http://www.sena.com/download/tutorial/tech_Modbus_v1r0c0.pdf
- [5] Siemmens. Catálogo IK-PI 2005, Industrial Communication, Comunicación industrial para Automation and drivers. 2005.
- [6] PROFIBUS, Automatización Industrial. Disponible en World Wide Web: http://www.disa.bi.ehu.es/spanish/ftp/material_asignaturas/Fundamentos%20de%20Automatizaci%F3n%20Industrial/Comunicaciones%20y%20Supervisi%F3n/PROFIBUS.pdf
- [7] Romero, Diego M. Introducción a Ethernet Industrial, Algunos Conceptos. IEEE, Sección Argentina. 2005.
- [8] Gorenberg, Andrés. Profinet: El nuevo estándar de comunicación de las plantas industriales. Revista Electroindustria, publicación 3 de mayo de 2007. 2005. Disponible en World Wide Web: http://www.emb.cl/electroindustria/articulo.mv?xid=216&rank=1
- [9] Wikipedia. PROFINET. 2008. Disponible en World Wide Web: http://en.wikipedia.org/wiki/PROFINET_IO.
- [10] Triangle MicroWorks Inc, Raleigh. DNP3 Overview. www.TriangleMicroWorks.com. February, 2002.
- [11] DNP Users Group. A DNP3 Protocol Primer, Revision A. www.dnp.org. 2005.
- [12] Coats, Jim. DNP3 Protocol AGA/GTI SCADA Security Meeting. DNP Users Group. www.dnp.org. August, 2002.

- [13] Narváez, Andres. Aplicación de los enlaces ICCP en el intercambio de información entre los centros de control en tiempo real. Centro Nacional de Control Energía, CENACE. [s.a.].
- [14] LeMay, Michael. SCADA Protocols. Overview of TASE.2/ICCP. [s.a.]. Disponible en World Wide Web: http://seclab.uiuc.edu/docs/iccp-intro.pdf.
- [15] AS-International Association. Elementos para tomar decisiones, AS-Interface. www.as-interface.net. 2006.
- [16] Bordóns, Alba, Carlos. Tecnología del control, Sensores, Acondicionamiento de señal, Actuadores. 2000. Disponible en World Wide Web: http://www.esi2.us.es/~bordons/Sensores.pdf.
- [17] Coiffi, John. Silverman, Peter. Starr, Thomas. Understanding Digital Suscriber Line. Prentice Hall PTR. First Edition. 1999.
- [18] Galarza, Cecilia. Redes de Acceso Basadas en Tecnologías xDSL. Universidad del Azuay, Maestría de Telemática. 2005
- [18] Universidad del Azuay. Redes de Acceso Basadas en Tecnologías xDSL. Dra. Cecilia Galarza. 2005.
- [19] Mobile Cellular Telecommunications, Analog and Digital Systems. William C. Y. Lee. McGraw-Hill. Second Edition. 1995.
- Murguet, Roberto. El Acceso Radio Celular, las comunicaciones móviles. Universidad de Azuay.
- [20] Universidad del Azuay, Maestría en Telemática. El acceso Radio Celular, las comunicaciones móviles. Roberto Murguet. 2004.
- [21] NeutralBit. Introducción a la seguridad en sistemas SCADA. www.neutralbit.com. 2006.
- [22] Smith, Steven S. The SCADA Security Challenge: The race is on. 2006.
- [23] Byres, Eric. Carter, Joel. Karsch, John. Good practice guide on firewall deployment for SCADA and Process Control Networks. NISCC, National Infrastructure Security Co-ordinate centre. 2005.
- [24] C. Salema. Microwave radio links: from theory to design. Wiley-Interscience, cop. 2003.