UNIVERSIDAD DE BELGRANO

Las tesinas de Belgrano

Facultad de Ingeniería y Tecnología Informática
Licenciatura en Licenciatura en Sistemas de Información

Aplicaciones de software para control de procesos de automatización industrial con dispositivos móviles

Nº 161 **Gabriel Alejandro Miños**

Tutor: Carlos Said

Departamento de Investigación
Abril 2005

Contenido

Fundamentos del problema

El planteo de la necesidad de distribuir la información

Introducción

En la actualidad la mayoría de los procesos industriales automatizados conectados a sistemas SCADA (Supervisión Control y Adquisición de Datos por sus siglas en inglés de Supervisory Control And Data Acquisition) utilizan una arquitectura tradicional (ver 'Arquitectura tradicional' más adelante en éste capítulo) para la conexión de las estaciones de visualización. Esta arquitectura suele estar atada a las prestaciones que el sistema SCADA podía ofrecer como posibilidades de conexión en sus inicios.

Durante los últimos años los sistemas SCADA fueron cambiando sus prestaciones de conectividad entre estaciones de consulta por los servicios de interconexión que brindan los sistemas operativos actuales.

La introducción de equipos PC (Computadora Personal) con sistema operativo Windows empleadas como estaciones de visualización, ha impulsado más aún la tendencia de relegar en los servicios de interconexión del sistema operativo la tarea de distribuir la información que el sistema SCADA adquiere.

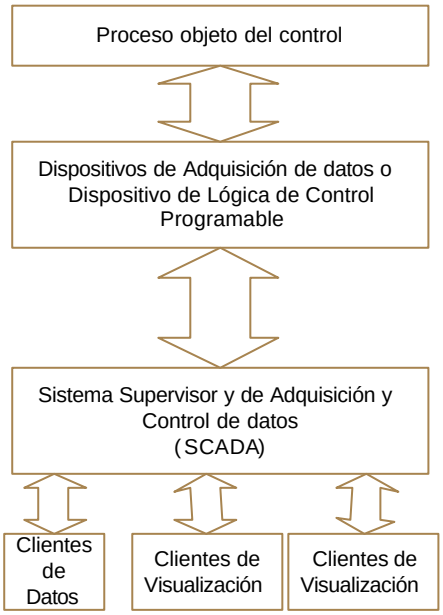
Así, hoy en día la mayoría de los sistemas SCADA utilizan TCP/ IP como protocolo de comunicación entre las estaciones de consulta de los datos, en lugar de protocolos propietarios.

Si bien las topologías que permiten los sistemas SCADA se adecuaron a las prestaciones de los sistemas operativos actuales, éstas no han variado mucho respecto a las que proponían en sus inicios.

Esquemáticamente un sistema SCADA conectado a un proceso automatizado consta de las siguientes partes:

- Proceso Objeto del control: Es el proceso que se desea supervisar. En consecuencia el origen de los datos que se requiere colectar y distribuir.
- Adquisición de Datos: Son un conjunto de instrumentos de medición dotados de alguna interfase de comunicación que permita su interconexión.
- SCADA: Combinación de hardware y software que permita la colección y visualización de los datos proporcionados por los instrumentos.

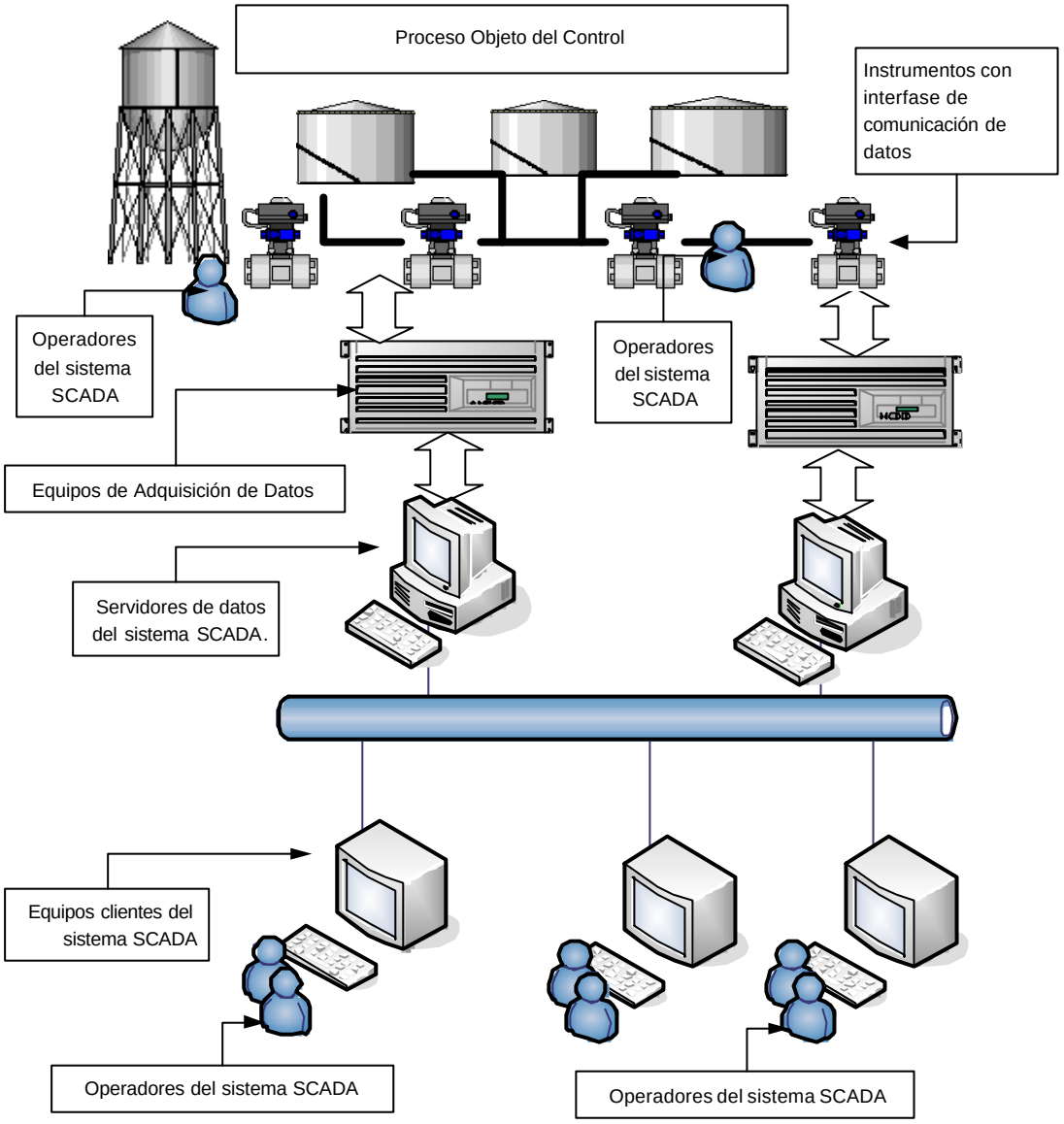
Clientes: Conjunto de aplicaciones que utilizan los datos obtenidos por el sistema SCADA.



Arquitectura tradicional

Históricamente los sistemas SCADA presentan un equipo que, conectado físicamente a los dispositivos de adquisición de datos, actúa como servidor para sus clientes interconectados a través de una red.

El siguiente esquema expone la topología tradicional de un sistema SCADA conectado a un proceso industrial automatizado.



Sin embargo, esta arquitectura presenta una serie de oportunidades de mejora relacionadas con la naturaleza de cada proceso industrial.

Los siguientes párrafos explican en más detalle cada una de estas partes a medida que se plantea una solución alternativa a la arquitectura tradicional de los sistemas SCADA.

Origen de la información

En un proceso de producción automatizado intervienen numerosas variables de proceso que afectan el resultado final del mismo. Dependiendo del proceso que se observe, la naturaleza de estas variables cambia notablemente.

Por ejemplo, en la producción de aluminio las variables más importantes están relacionadas con la tensión y corrientes de la cuba donde se realiza la electrólisis. En la producción de sustancias alimenticias, éstas pueden hacer referencia a temperaturas vinculadas a una etapa del proceso de pasteurización. En la producción de textiles pueden hacer referencias a velocidades de motores que manipulan los tejidos. En el proceso de extracción de petróleo es crítica la velocidad, junto con la fuerza y torque a la que son sometidos los equipos de extracción. En el transporte de gas y petróleo la presión de los gases y fluidos a lo largo de las cañerías resulta de vital importancia para evitar accidentes fatales y desastres. Para la industria de provisión de gas, la medición de la composición química del gas forma parte de los controles que se realizan para garantizar la calidad del producto. Como ejemplos más genéricos se pueden citar la medición de

niveles de tanques de almacenamiento final e intermedio o el peso de los transportes – camiones, trenes, contenedores, etc. - que distribuyen materias primas.

De los ejemplos anteriormente citados se observa que cada proceso tiene sus propias variables que resultan ser de importancia para el ciclo completo de producción. También se observa que el comportamiento de las variables esta íntimamente relacionado con la naturaleza del objeto sobre el cual se realiza la medición. Esto último esta relacionado con el intervalo de tiempo en el cual la magnitud de una variable pueda sufrir una modificación.

Podemos citar como ejemplo visualizador que el nivel de un tanque de un millón de litros de un fluido dado es poco probable que se altere en el lapso de un minuto. Sin embargo, las variaciones de corriente sobre un interruptor pueden observase en fracciones de segundo.

De ahí que cada proceso tenga sus propias reglas para la observación de las variaciones que sufren las variables relacionadas con él.

La adquisición de los datos

El proceso de adquisición de datos comienza con la implementación de instrumentos de medición que dispongan de alguna interfase para datos con un protocolo determinado. Los diseños y especificaciones quedan determinados por el fabricante del instrumento, el cual puede optar por una solución estándar de la industria o proveer al equipo con algún esquema y protocolo propietario.

De ahí que el equipo PC que se utilice para adquirir datos de estos instrumentos deba ser, por un lado, lo suficientemente flexible para poder adaptarse a esquemas propietarios y por el otro, deba proveer soporte para todos, o la mayoría, de los estándares de comunicación de la industria.

Surge, entonces, el concepto de aplicación controladora de comunicaciones la cual tiene como función única la de interpretar los datos que proveen los instrumentos y ponerlos a disposición de la aplicación que se encargará de recolectarlos y visualizarlos en las pantallas de los equipos PC de los usuarios.

Antes de poder manipular los datos provistos por el controlador de comunicaciones es necesario crear una estructura intermedia en la que puedan definirse las características del dato que se desea recolectar. Por características del dato podemos interpretar, entre otros, a la unidad de medida que representa esa información, rangos entre los cuales es válido el dato y la velocidad a la cual interesa observar las variaciones del mismo. Esta estructura recibe el nombre de «Base de Datos de Proceso» o PDB por sus siglas en ingles.

La PDB actúa entonces como repositorio de toda la información que proviene de los distintos controladores de comunicación, si los hubiese, y administra la comunicación con ellos. Entonces la colección de datos para su posterior tratamiento se realiza a partir de los datos que estén disponibles en dicha base de datos de proceso.

La adquisición de datos tiene dos grandes divisiones en lo que respecta al manejo de la información. Una es la colección de datos históricos y la otra es la visualización de datos en tiempo real.

El conjunto de aplicaciones formado por los controladores de comunicaciones, la base de datos de proceso, el sistema de colección de datos históricos y las aplicaciones de visualización de datos, recibe el nombre de «Aplicaciones de supervisión y adquisición de datos» o SCADA, por sus siglas en inglés.

El presente trabajo apunta solamente al análisis de la problemática de la visualización de datos en tiempo real provistos por una aplicación SCADA.

El manejo de la información

Por definición un SCADA basado en PC es una aplicación basada en un programa para PC que es utilizado para visualizar todos los datos que son necesarios para los operadores, ingenieros y administradores de planta de un proceso determinado, para permitir tomar decisiones en tiempo real considerando controlar y optimizar el proceso de producción.

Los datos disponibles en la base de datos de proceso reflejan, entonces, la realidad tomada por los instrumentos de medición. Estos datos son expuestos frente a los usuarios, en los equipos PC designados para visualización, a través de una interfase denominada «Interfase Máquina-Humano» o HMI, por sus siglas en inglés.

La interfase HMI se diseña acorde a las necesidades y requerimientos de los usuarios. Generalmente incluyen:

- Gráficos de tendencias: Gráficos de variables en función del tiempo. En la práctica los valores graficados de las variables corresponden a las mediciones obtenidas de los instrumentos por el sistema durante un corto período de tiempo.
- Datos de tiempo real: Valores numéricos que reflejan la realidad de los valores del proceso obtenidos por los instrumentos de medición.

- Operación y comando: Según las atribuciones permitidas a la aplicación SCADA sobre el proceso objeto, puede proveerse a los operadores con funciones que actúen sobre ciertos valores del proceso, logrando así una operación sobre éste. Así mismo, se provee la funcionalidad de comandar determinados equipos que intervienen en la ejecución del proceso, como ser arranques y paradas sobre motores, apertura y cierre de válvulas, etc.
- Mímico: Es un esquema gráfico que refleja los datos en forma clara y fácil de entender. El citado mímico por lo general, responde a un esquema o plano de las instalaciones en donde se lleva a cabo el proceso sobre el cual se están tomando datos, de manera de reflejar una visión cercana a la realidad de las instalaciones y la interacción de sus partes.

La aplicación SCADA provee a los usuarios la habilidad de obtener información precisa en tiempo real, y distribuye dicha información a los lugares apropiados dentro del esquema de operación del proceso, permitiendo crear mejoras en él.

La distribución de la información

En la mayoría de las instalaciones se designa un puesto, denominado centro de control, el cual concentra toda la información colectada por la aplicación SCADA. Generalmente este puesto consta de varias estaciones de trabajo para los diversos operadores que intervienen en el control y la supervisión del proceso.

También se designan estaciones aledañas en lugares estratégicos del ciclo de producción para asistir a los operadores de dicho ciclo. Si bien es posible acceder a toda la información del SCADA desde estas estaciones, se designan como puestos de consulta y supervisión de una parte determinada del proceso.

La interfase gráfica disponible en estas estaciones permite que los operadores visualicen y consulten información en forma rápida y efectiva para que ellos puedan tomar decisiones acerca de variaciones en las variables de proceso. Dependiendo de la naturaleza del proceso, estas acciones pueden ser correctivas o simplemente informativas del resultado final de un ciclo de producción.

Pero si bien estas estaciones están mas cerca de los operadores especializados, facilitando al acceso a la información, el operador debe acercarse físicamente a la estación para consultar por los datos que necesita para realizar una tarea.

El planteo más común es el caso de las operaciones de mantenimiento, donde los operadores de mantenimiento deben conocer información del equipo sobre el que van a trabajar. No solo información histórica de él, como horas de funcionamiento, fecha de mantenimientos anteriores, información estadística de fallas o procedimientos de reparación, sino también información en tiempo real del instrumento. Por ejemplo, para verificar que los datos que obtiene el SCADA son precisos respecto de las mediciones reales, el operador mide en el lugar adecuado con instrumentos calibrados y luego compara con la medición obtenida en las pantallas de visualización.

Esta metodología de trabajo se extiende también a las tareas rutinarias de supervisión y control de los instrumentos de proceso, sin esperar a los ciclos de mantenimiento preventivo estipulados.

La necesidad no resuelta

De lo antes expuesto se visualiza la necesidad de contar con algún dispositivo que permita al usuario llevar la información de la aplicación SCADA a donde sea necesario, en lugar de tener que ir a consultar la información a un lugar previamente determinado y, por lo general, fijo e inamovible.

Llegamos así hasta el planteo del uso de dispositivos de mano, denominados dispositivos móviles, para poder llevar la información recolectada por la aplicación SCADA hasta el punto donde resulta de mayor utilidad, la mano de quien debe tomar las decisiones que pueden modificar el resultado final de un ciclo de producción.

Estos dispositivos podrían reconocer el instrumento sobre el cual el operador va a trabajar y presentar en la pantalla la información que este necesite, en lugar de tener que espera por ella o consultar, telefónicamente o por radio, a otro operador que se encuentre frente a una estación de visualización.

La solución propuesta

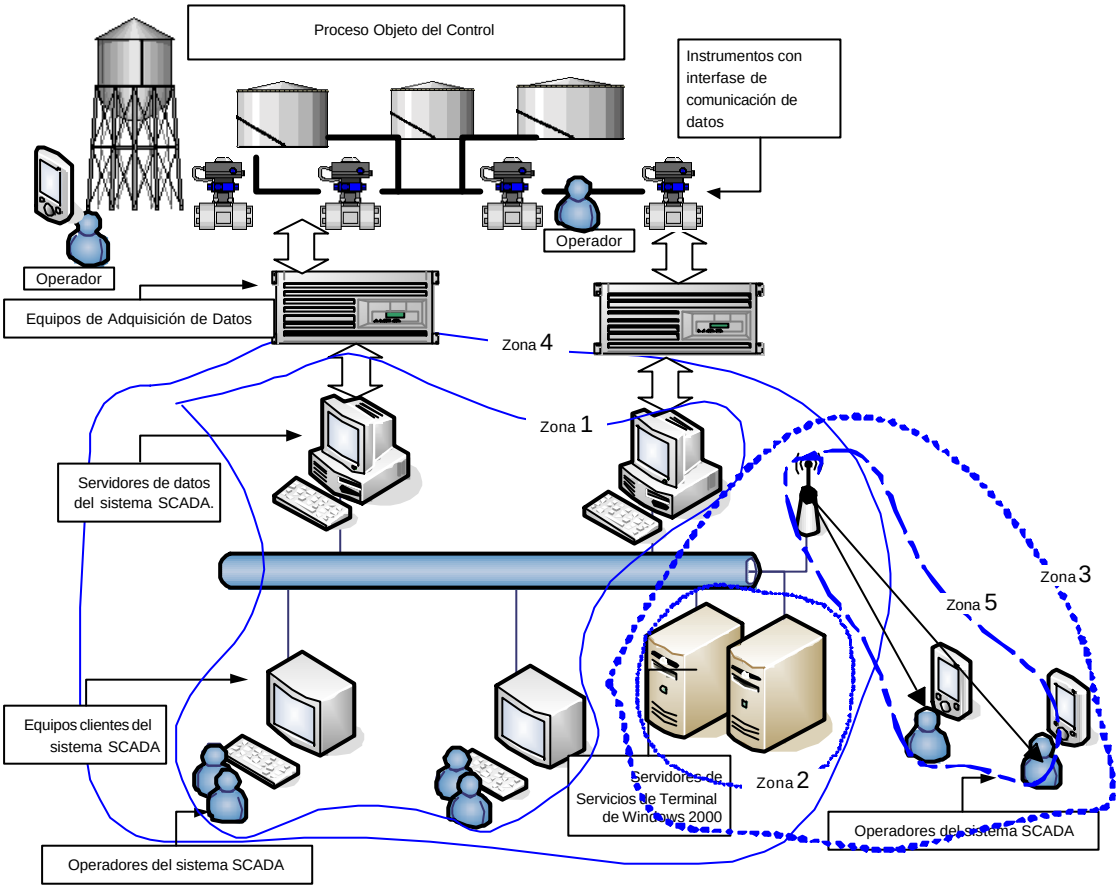
La implementación propone el agregado de dispositivos móviles que actúan como equipos terminales de los datos que obtiene el SCADA al sistema de control actual. Estos dispositivos acompañarían las tares diarias del operador, transformándose en una herramienta mas de trabajo para poder operar y supervisar el proceso.

Inicialmente empleados como equipos de visualización, con el tiempo irán ganando terreno en la operación y comando del proceso, a medida que se hagan más comunes y fortalezcan las opciones de seguridad informática respecto a la autenticación de usuarios y controles de acceso.

La integración de estos dispositivos a la red de visualización del SCADA implica la combinación de

variadas tecnologías disponibles hoy día en el mercado. Pero la cuidadosa selección de éstas necesita de un detallado conocimiento del funcionamiento y sus especificaciones, de manera de poder cumplir con las necesidades de distribución de información planteadas.

En forma genérica, y sin entrar en detalles, se propone para lograr alcanzar las necesidades de distribución de información el uso de dispositivos móviles basados en PocketPC o Windows CE, los cuales formarán parte de la red de las estaciones SCADA empleando redes de tecnología inalámbrica.



La solución propuesta gráficamente puede ser descompuesta para su comprensión y análisis en diferentes zonas. Cada una de ellas se presenta en el gráfico delimitada por una línea de puntos con un nombre asociado a ella (Ej: Zona de análisis 1; Zona de análisis 2).

Cada capítulo que desarrollamos a continuación profundiza en el detalle de la arquitectura y funcionalidad de cada zona.

Zona	Capítulo	Descripción
Zona 1	Aplicación SCADA.	Zona de aplicación del sistema SCADA relacionada al proceso que se controla.
Zona 2	Servicios de Terminal.	Análisis de la funcionalidad de los Servicios de Terminal de Windows 2000
Zona 3	Protocolo RDP 5.0	Análisis del protocolo RDP versión 5.0 utilizado por los Servicios de Terminal de Windows 2000.
Zona 4	Aplicación en los Servicios de Terminal.	Análisis de las aplicaciones empleadas en los Servicios de Terminal
Zona 5	Redes inalámbricas y dispositivos de mano.	Factores relacionados con la construcción de redes inalámbricas.

Finalmente en el capítulo «Conclusión final» presento una visión integradora, luego de haber realizado el análisis y descomposición de la topología propuesta.

Análisis de una aplicación SCADA

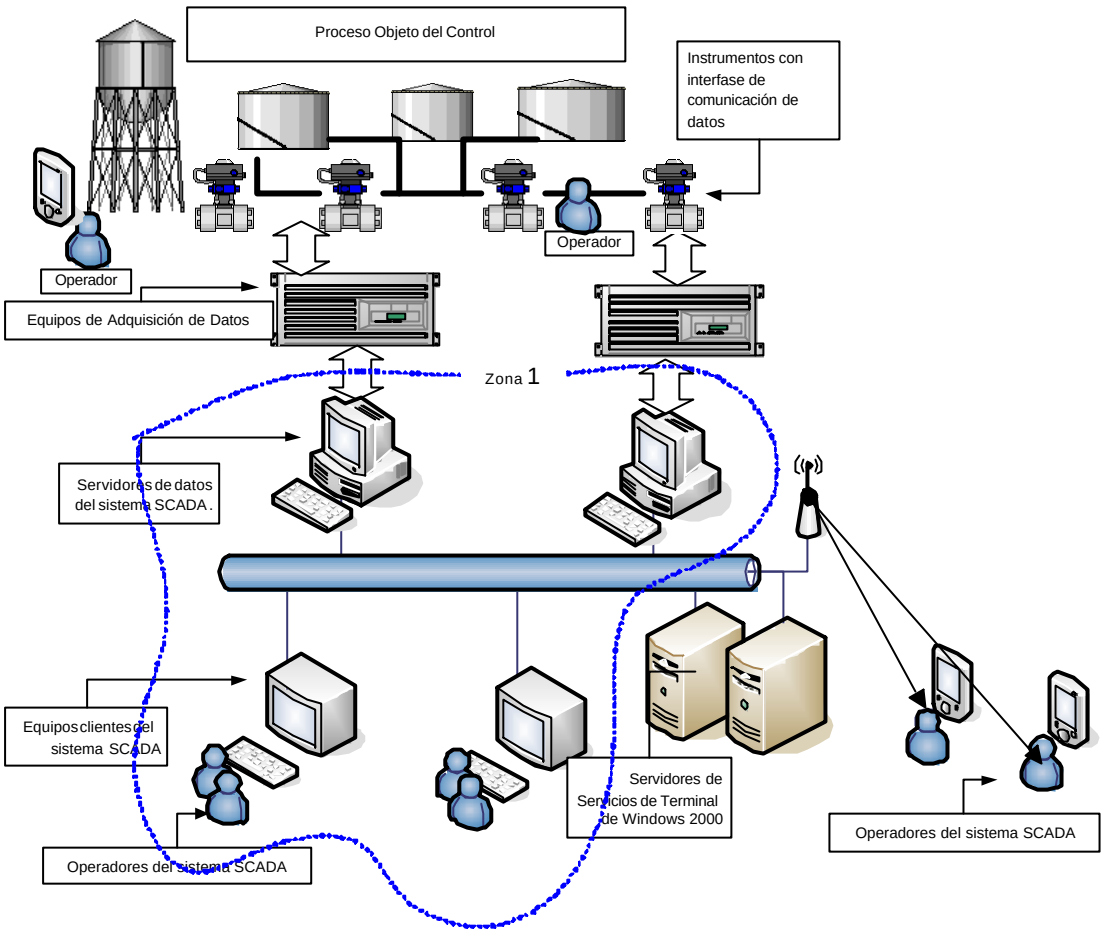
Descripción de los componentes más comunes en una aplicación SCADA

Introducción

La solución propuesta comienza con el análisis de una aplicación de control basada en un sistema SCADA conectado a un proceso industrial automatizado.

El SCADA, entonces, se encarga de colectar los datos del proceso objeto y luego distribuye la información acorde a sus prestaciones.

En este capítulo se desarrolla en forma más profunda el proceso de adquisición y manipulación de la información, como así también las alternativas de distribución de la misma acorde al producto seleccionado.



Proceso objeto de la aplicación

Las aplicaciones SCADA son usadas para monitorear y controlar de forma remota una planta y su equipamiento. El campo de aplicación de los SCADAs es muy extenso y cubre áreas como la distribución de electricidad, el seguimiento de oleoductos, plantas de tratamientos de aguas, control de inundaciones y automatización de fábricas, entre otros.

El origen de los datos que adquiere y manipula el SCADA esta íntimamente relacionado con la naturaleza del proceso objeto de la aplicación. Cada proceso tiene claros y definidos parámetros que deben ser controlados a lo largo de todo el proceso de producción o ejecución.

Generalmente son utilizados determinados equipos eléctricos o electrónicos que transforman las magnitudes físicas o químicas de dichos parámetros en señales eléctricas para que puedan ser interpretadas por componentes electrónicos. Estos dispositivos reciben el nombre de transductores. Así existen transductores de presión, de temperatura, de peso, de luz, de velocidad, de fuerza, entre otros.

Estos transductores son conectados a dispositivos de lógica de control programable, conocidos como PLC, los cuales son los encargados de administrar y controlar el flujo de datos que proveen los transductores y así llevar adelante la lógica de ejecución que reclame el proceso objeto que se debe controlar.

Cada PLC esta formado entonces por un conjunto de señales que recibe del proceso objeto, una lógica de control que administra los datos y les da sentido a éstos, un conjunto de interfaces para poder actuar sobre el proceso que se controla; por ejemplo accionar una válvula, arrancar o detener un motor eléctrico, entre otros; y una o varias interfaces que permitan comunicar los datos obtenidos a otros equipos PLC.

De ésta manera se pueden vincular varios equipos PLC para que en conjunto logren controlar procesos que requieren el seguimiento de varios miles de parámetros o puntos de control.

Las interfaces de comunicación de estos PLC suelen respetar protocolos estándares aceptados por la industria para establecer sus comunicaciones. Sin embargo, nada impide que cada fabricante diseñe su propio protocolo para comunicar su equipo PLC con otro dispositivo similar.

Una vez mas, cada proceso relacionado con la industria a la que pertenece, ha elegido con el transcurso

del tiempo, su protocolo preferido. Y es bastante común que los fabricantes de equipos PLC y equipos de comunicaciones se amolden a estos protocolos.

Como ejemplo mas comunes podemos citar:

- MODBUS: Es el protocolo serial de facto de la industria de instrumentos para mediciones industriales. Es un protocolo de mensajes de la capa de aplicación, posicionado en el nivel 7 del modelo OSI, que provee comunicación tipo cliente y servidor entre distintos instrumentos conectados a un bus de comunicaciones.
- DNP3: Es un protocolo basado en el estándar del International Electrotechnical Commission (IEC) Technical Committee 57, Working Group 03 diseñado para aplicaciones de telecontrol y aceptado mayormente en la industria de control de plantas de transporte y generación de energía eléctrica.

Generalmente toda la información recolectada por los equipos PLC es llevada a un Centro de Control, donde se logra obtener una visión más generalizada del proceso en su conjunto, su evolución en el tiempo, y estado actual. También se espera colectar información histórica de las variables observadas con el fin de generar registros de los factores que pudieron influir en el proceso objeto y hasta predecir sus comportamientos en el futuro.

El Centro de Control suele contar con una red de equipos PC interconectados entre sí, y a su vez a los equipos PLC, de manera de poder distribuir la información del proceso objeto a los distintos operadores del mismo. Estos usuarios del sistema suelen estar agrupados según su grado de responsabilidad para con el proceso y cada uno de éstos tiene necesidades distintas de información que el sistema en su conjunto debe proporcionar. En la mayoría de las aplicaciones suele haber niveles de «Operador», «Supervisor», «Administrador» e «Ingeniería».

Interfaces y protocolos de comunicación

Para poder tomar la información disponible en los equipos PLC la aplicación SCADA debe poder entender, interpretar y relacionarse con la forma de comunicación de los equipos PLC. Esto es, su protocolo de comunicación.

En una arquitectura basada en PC las alternativas para interfaces son dos: Agregar una placa interfaz de diseño propietario a la PC o utilizar un puerto de comunicaciones estándar tipo RS-232.

Interfaz propietaria

La decisión de emplear una interfaz propietaria está determinada por la sugerencia o imposición del fabricante del equipo al cual se requiera conectarse.

Puede ser que el fabricante sugiera la utilización de un dispositivo propietario para comunicación, con el fin de lograr mejores prestaciones en la comunicación o asegurar ciertas tasas de transferencia de información.

También es posible que el fabricante sólo provea un método de comunicaciones propietario el cual debe respetarse para cumplir con la garantía de servicio del equipo.

Interfaz estándar

En el caso de que la interfaz de comunicaciones recaiga en un estándar de la industria tipo RS-232 se emplean los puertos de comunicación tradicionales en un equipo PC. El uso total o parcial de las bondades de la norma depende nuevamente de las posibilidades provistas por el fabricante del equipo al cual se necesite conectar.

La demanda por alta velocidad en las comunicaciones ha llevado a varios fabricantes a utilizar el estándar Ethernet 802.3 como interfaz entre sus equipos o con equipos PC. Si bien es posible compartir una red Ethernet de oficina con una de equipos PLC, ésta práctica no es recomendada, ya que una rede de oficina con numerosos equipos y considerable tráfico, podría afectar la velocidad y el desempeño de las comunicaciones con los equipos PLC.

Protocolos de comunicación

Los protocolos de comunicación entre los equipos PLC y las aplicaciones SCADA basadas en arquitectura PC suelen estar desarrollados por o en conjunto con el fabricante del equipo PLC. Por lo que no es necesario realizar adaptaciones o modificaciones mayores.

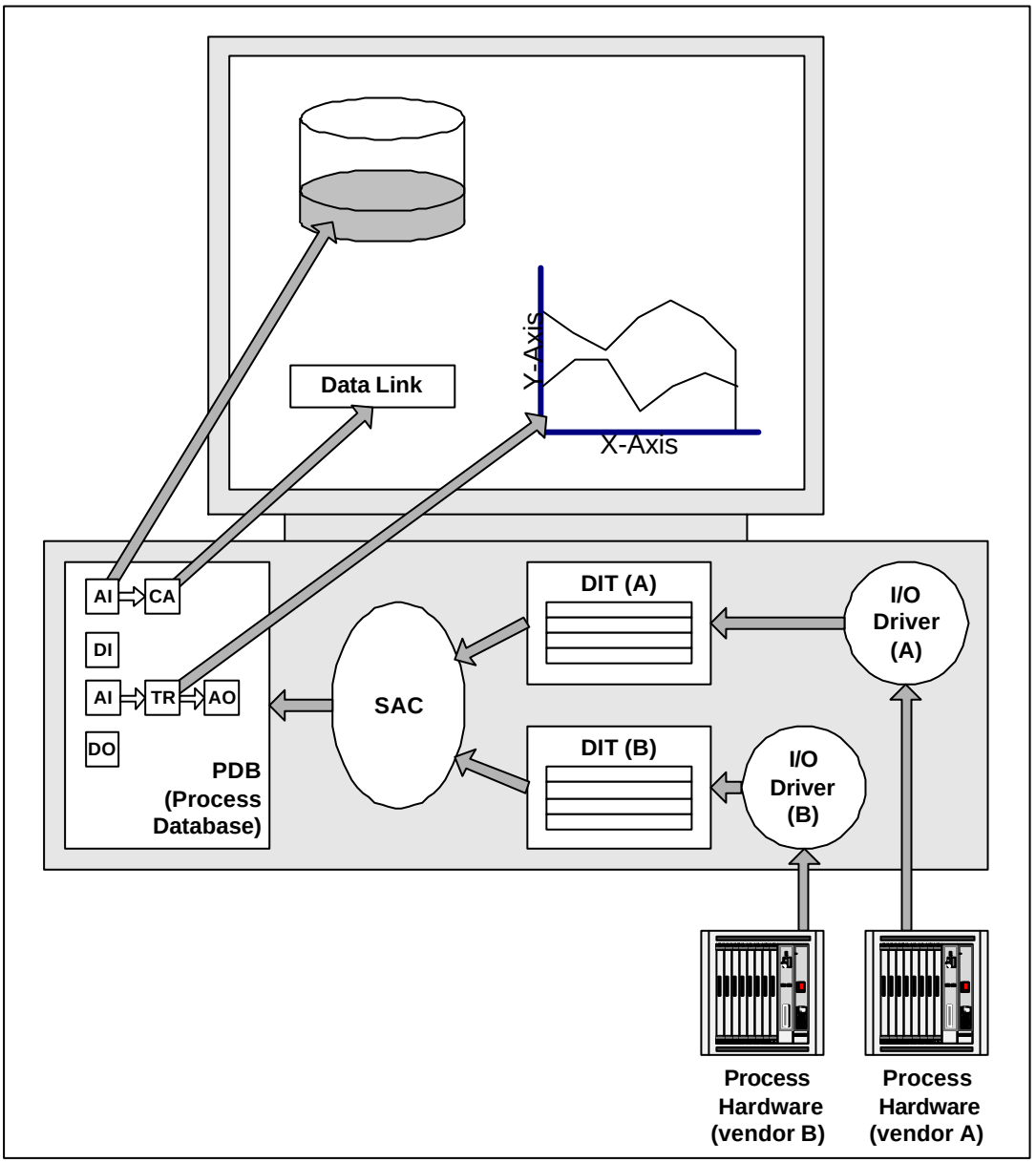
El interprete del protocolo del equipo PLC suele ser un programa para PC denominado controlador de comunicaciones. Éste se encarga de administrar la comunicación entre la aplicación SCADA y el equipo PLC.

Generalmente una aplicación SCADA puede intercambiar información con varios controladores de comunicaciones, permitiendo mezclar en una sola aplicación diversos modelos de equipos PLC aún de distintas marcas y fabricantes.

Existen hoy día varios centenares de controladores de comunicaciones para distintos equipos PLC y diversas aplicaciones SCADA basadas en arquitectura PC. Sin embargo, la industria trata de migrar a un nuevo estándar de comunicaciones, impulsado por empresas de primera línea como General Electric, Intellution, Microsoft entre otras, denominado OPC; por sus siglas en Ingles «OLE for Process Control».

Arquitectura de una aplicación SCADA basada en PC

Para el análisis de la arquitectura de una aplicación SCADA basada en la plataforma PC, estudiaremos el caso del paquete de desarrollo para aplicaciones SCADA de la firma norteamericana Intellution. Dicho paquete de desarrollo lleva el nombre «iFix» y esta desarrollado para ser ejecutado en un sistema operativo Microsoft Windows NT versión 4.0, Microsoft Windows 2000 o Microsoft Windows XP Pro, exclusivamente hasta el momento.



Esquema genérico de una aplicación SCADA .

En el esquema se observa una arquitectura básica para un modelo de adquisición y visualización de datos.

Comenzando por los dispositivos de control, los datos llegan a los Controladores de comunicaciones (I/O Driver) y son tratados en un esquema propietario denominado Tabla Imagen del Controlador (DIT – Driver Image Table) donde esperan ser procesados por el Sistema de Control y Alarmas (SAC).

Los puntos de control (Tag) definidos en la base de datos se identifican por el tipo de datos que adquieren. Así, DO implica un dato digital de salida, AI un dato analógico de entrada, DI un dato digital de entrada, y así con el resto de los tags.

La visualización se logra relacionando un objeto dentro del gráfico de operación con uno o varios de los valores de los tags previamente definidos.

A continuación se explican en mayor detalle cada una de las partes y su importancia en el funcionamiento conjunto de la aplicación.

Controladores de comunicaciones

El punto de entrada de datos para la aplicación es el controlador de comunicaciones asociado al protocolo del equipo PLC del cual se desea obtener datos. En particular existe una limitación de hasta ocho controladores simultáneos conectados a una aplicación SCADA. Esto no quiere decir que esta limitado a ocho equipos PLC, sino a ocho protocolos de equipos PLC. Entonces cada controlador de comunicaciones puede estar conectado a varios equipos PLC, siempre y cuando manejen el mismo protocolo.

Repositorio de información de tiempo real

Se entiende por información de tiempo real a los datos más recientes obtenidos por el equipo PLC que fueron entregados por el controlador de comunicaciones. Dado que es posible tomar mediciones del proceso objeto a tasas en el orden de las centésimas de segundo ésta es considerada como de «tiempo real».

El repositorio de la información de tiempo real obtenida de los controladores es una estructura residente en la memoria de la PC denominada PDB, por sus siglas en Ingles «Process Data Base».

La PDB es asistida por tareas periódicas de búsqueda de nuevos datos, que se encargan de interrogar a los controladores de comunicaciones por ciertos puntos de control previamente definidos en el diseño de la aplicación SCADA. Los valores de éstos puntos de control son almacenados en variables o ítems de datos denominados TAGs o genéricamente «puntos».

Los puntos de una PDB forman una estructura de datos relacionados con el tipo de datos que van a almacenar. Genéricamente la estructura alberga información del punto de control, como ser:

- Controlador de comunicaciones: identificación del controlador de comunicaciones del cual provienen los datos.
- Límites: rango de validez de las mediciones esperadas.
- Unidades de ingeniería en la cual se representa la magnitud.
- Intervalo de verificación: período al cual se espera que el dato varíe.
- Límites de alarma: rango entre los cuales las variaciones de la medición representan un comportamiento normal. Fuera de estos límites se considera una condición que debe ser observada, por lo que se genera una alarma relacionada con el punto de control. Generalmente existen cinco tipos de alarmas que identifican problemas en el proceso, a saber:
- Alarma HiHi: condición de alarma por valor muy alto en el rango estipulado para la medición. Implica una condición crítica para el punto de control en su relación con el proceso.
- Alarma Hi: condición de alarma por valor alto en el rango estipulado para la medición. Implica una condición de atención, pero no crítica para el proceso.
- Alarma Lo: condición de alarma por valor bajo en el rango estipulado para la medición. Implica una condición de atención, pero no crítica para el proceso.
- Alarma LoLo: condición de alarma por valor muy bajo en el rango estipulado para la medición. Implica una condición crítica para el punto de control en su relación con el proceso.
- Alarma ROC (Rate Of Change): indica que el valor sufre variaciones en su magnitud que superan las expectativas de funcionamiento normal. Implica una anomalía en el proceso o en los instrumentos.
- Valor de la última medición obtenida muñida de la fecha y hora de la misma.

Esta estructura de datos es puesta a disposición de otros componentes de la arquitectura de la aplicación SCADA para que pueda establecerse una relación entre los puntos de control, tomarse alguna decisión relacionada a un evento determinado o simplemente mostrar el dato en una representación gráfica.

Sub sistema de alarmas

Una de las tareas principales de una aplicación SCADA, una vez establecidos los parámetros normales

de funcionamiento para las variables de proceso o puntos de control, es notificar a los usuarios del sistema acerca de desviaciones en los parámetros del proceso.

El sistema realiza estas notificaciones generando un tipo especial de mensaje denominado «Alarma».

Una alarma es una condición de un punto de la PDB el cual ha sobrepasado los límites prefijados para su rango normal de funcionamiento.

Por su naturaleza esta condición requiere: la notificación al usuario del sistema y luego el reconocimiento de él sobre la misma. De ésta manera el sistema se asegura que alguna persona ha sido correctamente informada de la situación anómala y se espera la corrección de la situación en el corto plazo.

Estas notificaciones, al igual que los reconocimientos, son realizados por indicaciones en las pantallas de los operadores, pero también se dejan asentados en archivos de auditoría de actividades.

Los usuarios interactúan con el sistema para notificarse y reconocer las alarmas mediante gráficos animados que muestran la condición detectada de manera que sea simple y claro para el operador en que punto de control se produce el desvío y cuál es su factor de incidencia en el proceso completo.

De esto se desprende que las alarmas no son necesariamente críticas. Como ejemplo podemos citar el siguiente caso: la detección de una puerta abierta en un depósito de cajas de alimento para gallinas no necesariamente requiere de una acción inmediata. Por el contrario, la detección de una puerta abierta en un depósito de substancias radioactivas seguramente requiera una acción correctiva urgente. La naturaleza de cada proceso objeto es el que determina la criticidad de las alarmas.

Entonces el SCADA posee la habilidad de clasificar las alarmas según su prioridad en tres niveles principales: Alto, Medio y Bajo. En consecuencia el SCADA reacciona acorde a la prioridad de las alarmas.

De igual manera los usuarios del sistema son notificados de las alarmas que requieran su intervención. Si volvemos al caso de los niveles «Operador» y «Supervisor», un usuario «Supervisor» no será notificado de las alarmas de prioridad baja, pero sí de las de alta y media; mientras que un usuario «Operador» será notificado de todas las alarmas relacionadas con el proceso que él debe operar.

Almacenamiento de datos históricos

Para poder llevar un control detallado y preciso de un proceso es necesario observar su evolución en el tiempo.

Para tal fin la aplicación SCADA cuenta con la habilidad de guardar datos cronológicamente ordenados al sólo fin de recrear una situación pasada en un tiempo futuro.

El almacenamiento se realiza en una base de datos relacional estándar de mercado o en un archivo de estructura propietaria, brindando éste último el mejor desempeño al momento del almacenamiento. Sin embargo, se provee una interfaz ODBC para poder realizar consultas a los datos ya almacenados empleando sentencias del estándar SQL desde alguna aplicación externa al SCADA.

Se utilizan algoritmos de compresión de datos y de interpolación matemática para optimizar el lugar empleado para guardar datos. Se logra así una estructura compacta de datos donde se disminuye la cantidad de valores almacenados, optimizando el tiempo de acceso a los datos guardados y no malgastar el espacio del medio utilizado.

Visualización en pantalla

Como medio interactivo con el usuario del sistema, el SCADA emplea la salida de monitor de la PC para presentar la información obtenida de los equipos PLC, los mensajes de alarmas, las gráficas de tendencias de las variables del proceso objeto y valores estadísticos que afectan al mismo.

Esta información se organiza en vistas dependientes y jerárquicas diseñadas y ordenadas por el desarrollador de la aplicación. Estas reflejan el proceso objeto en un todo conjunto, como así también en vistas detalladas de determinadas etapas del proceso.

El tipo y el grado de información presentada en cada vista dependen del usuario que se encuentre frente al sistema. Por esto, el sistema debe administrar una suerte de perfiles de usuario para proveer a cada uno de ellos la información que le fue asignada por el desarrollador del sistema, o incluso permitir la personalización de sus vistas.

Las vistas deben, incluso, estar restringidas a ciertos usuarios para asegurar la confidencialidad de la información sensible.

De aquí se desprende que la aplicación SCADA debe ser capaz de administrar un sistema de validación de usuarios para el acceso a las vistas y otras operaciones. Por lo general esta tarea se realiza en conjunto con el sistema operativo de manera que sea posible administrar, en forma central y con políticas claras y robustas, el acceso a la información.

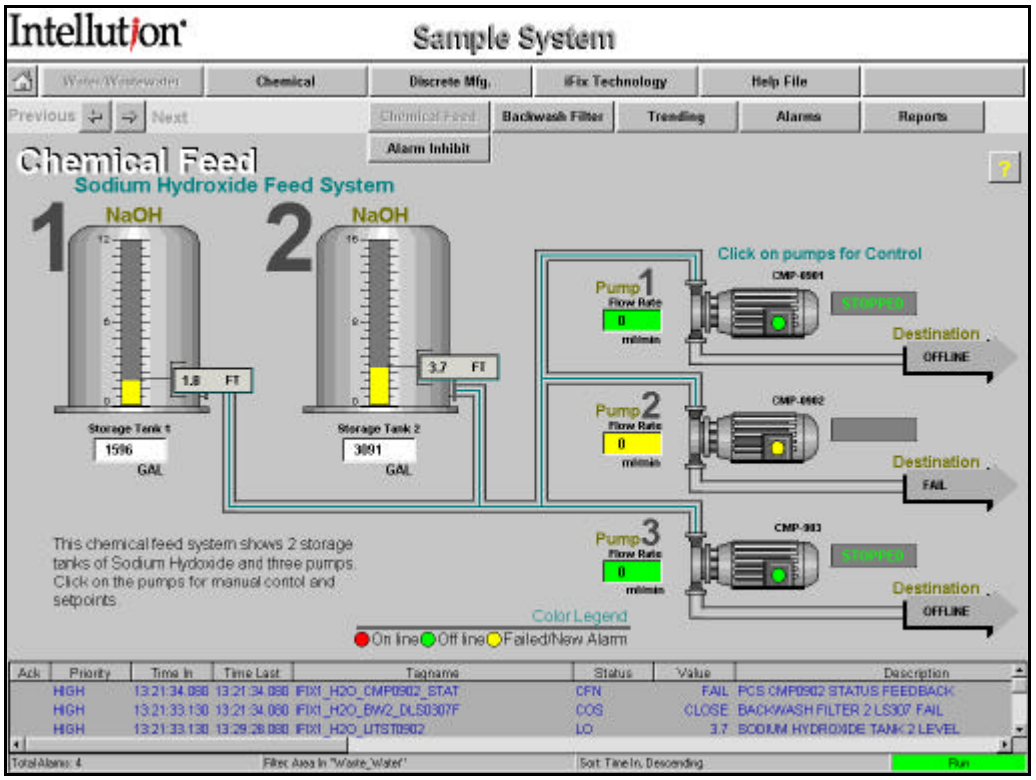
En un enfoque práctico, se utilizan las cuentas de usuario que se emplean para iniciar la sesión de usuario en el entorno Windows, para realizar la validación del usuario frente a la aplicación SCADA. Esto

minimiza las tareas de administración de las cuentas de usuario y permite el control de las cuentas mediante una política central de acceso.

En el diseño de la vistas se emplean técnicas de desarrollo de gráficos relacionados con las artes visuales y las costumbres de los usuarios del entorno Windows. Así se crean animaciones coloridas de las distintas etapas del proceso como así también gráficos de datos en forma de tendencias, juntamente con cajas de diálogo con estilo Windows para interactuar con el usuario.

Suelen emplearse tecnologías de ultima generación para realizar vistas lo más realistas posibles. Estas abarcan la inclusión de fotografías, archivos de secuencias de video, video en tiempo real, planos de Autocad y objetos ActiveX entre otros.

En el caso de que la vista contemple la modificación de algún parámetro sensible del proceso por parte del operador, se suele solicitar una confirmación de la acción por parte de éste. Ya sea mediante el uso de firma electrónica o algún método de identificación confiable, trazable y auditable en el tiempo.



Pantalla de ejemplo de visualización de un control de proceso

Programación de tareas

Dependiendo de la naturaleza del sistema SCADA es deseable que el mismo reaccione frente a ciertas circunstancias del proceso objeto, denominadas éstas eventos, y realice alguna tarea previamente definida por el diseñador y acordada con los propietarios del sistema.

Estas tareas responden a un esquema de programación basada en la detección de los eventos del sistema objeto, o bien en el cumplimiento de un intervalo de tiempo determinado.

Eventos como la detección de una falla, alcanzar un número determinado de alarmas o situaciones anómalas, o el cumplimiento de una secuencia determinada suelen disparar una notificación sobre tal evento, de manera tal que el personal responsable sea debidamente notificado y así, tal vez, tomar alguna acción correctiva o simplemente ser notificado.

Por otro lado, el SCADA también debe realizar tareas basadas en la detección de un intervalo de tiempo. La detección del fin de un turno de producción tal vez debe generar un informe de estado durante el turno. Generalmente la detección del fin de una semana suele generar un informe con las novedades semanales. Así otro tanto de ejemplos que dependen de la naturaleza del proceso objeto.

Para cumplir con estos requerimientos el SCADA cuenta con una aplicación complementaria destinada a la detección de eventos y programación de tareas. Esta aplicación es configurada por el desarrollador del sistema SCADA para cumplir con los requerimientos hacia el SCADA. Esta aplicación se ejecuta en conjun-

to con el SCADA y tiene la habilidad de interactuar con la PDB para poder detectar eventos basados en condiciones del proceso. También posee la posibilidad de programar la detección de eventos basados en intervalos de tiempo a través de una interfaz donde se puede seleccionar la fecha y hora de un evento, el nombre del día de la semana que se debe efectuar una tarea o el número de día del mes en el cual deba ejecutar una acción.

También tiene acceso a determinadas librerías del sistema operativo para poder reaccionar a ciertas deficiencias del equipo PC en su conjunto, tales como falta de espacio en disco, desconexiones de red, etc.

Para la acción frente al evento se cuenta con una serie de funciones que contemplan la mayoría de las funciones más habituales en una aplicación SCADA o se dispone de un entorno de programación Visual Basic para Aplicaciones de Microsoft para personalizar la funcionalidad requerida.

Generación de informes

Dentro de las finalidades más comunes de un sistema SCADA se encuentra la generación de informes del estado actual, historia y proyecciones de los valores más críticos para el éxito del proceso objeto.

Para lograr tal fin el SCADA debe contar con la posibilidad de acceder a sus datos de tiempo real, trabajar con datos colectados para propósitos de análisis históricos y proveer herramientas que permitan presentar el resultado del análisis a una interfaz determinada.

Esta interfaz puede ser el mismo monitor donde el operador interactúa con el sistema SCADA, puede ser también una impresora de papel, de manera de obtener un informe escrito o gráfico del análisis requerido o puede tratarse de una aplicación externa al SCADA que necesite nutrirse de la información del sistema para procesarla hacia otros niveles del sistema de gestión de información en su conjunto.

Para la generación de informes en pantalla la herramienta de visualización suele contar con objetos de características gráficas orientadas a la gráfica de valores en función del tiempo, en todas sus variantes y combinaciones más comunes, o incluso gráficos de confrontación de variables (gráficos tipo XY). También suele disponerse de gráficos tradicionalmente estadísticos, si es que es función del SCADA generar este tipo de información.

En la generación de informes gráficos suele relegarse la tarea de presentación de la información en aplicaciones de mercado ampliamente aceptadas para tales fines. Tal es el caso de la herramienta Crystal Reports de Seagate o Microsoft Excel de Microsoft. Estas herramientas facilitan la manipulación de la información posterior a la generación del informe.

Para la presentación de información de informes o resumen a otra aplicación suele relegarse en tecnologías de uso masivo para tales fines. Es posible conectar el SCADA a una interfase del tipo ODBC (Open DataBase Conectivity) para transferir la información a un sistema de base de datos relacional.

Mediante el empleo de técnicas de programación en Visual Basic para Aplicaciones es posible conectar el SCADA a la interfaz de Automación de una aplicación (OLE Automation) para intercambiar información o solicitar alguna acción determinada a la aplicación destino.

La combinación de estas opciones suele generar un robusto sistema de informes donde la aplicación SCADA sea capaz de generar un informe en una planilla tipo Excel y luego enviarla como anexo de un mensaje de correo a determinados destinatarios con el fin de cumplir los requisitos de distribución de informes.

Integración con otras aplicaciones

De igual manera que se espera que el SCADA transfiera los datos obtenidos del proceso objeto a otra aplicación, es deseable que éste tome datos de aplicaciones externas y los vuelque al proceso o simplemente los muestre al operador del sistema.

Tal es el caso del manejo de la producción mediante recetas. Éstas suelen involucrar varios parámetros que el SCADA debe controlar, pero que varían según el proceso que el SCADA esté realizando. El concepto de receta es el mismo que una receta de cocina. Ciertos procesos ordenados durante determinados períodos de tiempo.

Entonces el SCADA debe poder tomar esta información de recetas, generalmente almacenada en sistemas de bases de datos relacionales, y aplicarla a las variables del proceso objeto que éste controla. Se utilizan las mismas técnicas antes mencionadas, como ODBC y OLE Automation.

Para la visualización suele emplearse la inserción de objetos de tecnología ActiveX, con procedimientos definidos, en la pantalla de manera de presentar al operador la información necesaria.

Generación de registros de actividades

Al sólo fin de auditar el comportamiento del sistema y las acciones llevadas a cabo con el SCADA, se requiere la generación de un registro de auditoría donde queden asentadas todas las operaciones críticas

para el sistema más las que los propietarios del sistema hayan determinado como tales.

Por operaciones críticas se entienden los arranques y paradas de los equipos PC como así también el registro de los operadores sobre el sistema, fallas de comunicación con los instrumentos de medición entre otras.

Estructura de red

Una aplicación SCADA debe poder distribuir su información a los distintos puestos de operación designados para operar el proceso objeto. A tal fin se requiere una estructura de red que sea capaz de contemplar las necesidades actuales y contemple la capacidad de adaptación al cambio que el sistema en su conjunto sufrirá en los próximos años.

Es de esperar que la aplicación SCADA basada en Microsoft Windows utilice el estándar TCP/IP para establecer sus comunicaciones.

Así cada estación de operación del SCADA dispone de una dirección IP, conformando en su totalidad una red de equipos bajo el conjunto de protocolos TCP/IP, que puede aplicarse sobre una red de fácil construcción y mantenimiento.

Si bien es recomendable separar los tendidos físicos de redes, de manera de tener una red física para los productos de oficina y servicios del sistema operativo utilizados en los equipos PC, y otra para el uso exclusivo de la aplicación SCADA, nada impide que ésta comparta la misma red física simplificando así el tendido eléctrico de la misma y facilitando su crecimiento.

El modelo de red empleado por la firma desarrolladora de la aplicación SCADA se basa en la filosofía cliente y servidor. Donde el nodo cliente establece una sesión de red con el nodo servidor para el intercambio de datos. Esta sesión puede ser permanente mientras el nodo esté activo, o puede requerir ser desconectada según las necesidades de información del nodo cliente.

Así se establece una jerarquía entre nodos relacionada con el papel que cumplen dentro de la red. Existen los nodos «Servidores SCADA» que son los nodos SCADA que están físicamente conectados a los equipos PLC y tiene acceso a los instrumentos de medición, y los nodos «Clientes SCADA» que necesitan conectarse a un nodo «Servidor SCADA» para poder obtener datos del proceso.

Una arquitectura de red simple para un SCADA involucra a un «Servidor SCADA» y uno o varios «Clientes SCADA» distribuidos en los puestos de operación. Así se logra distribuir la información a los lugares necesarios, como ser puestos de operación, supervisión, mantenimiento, ingeniería, etc.

En la práctica suele haber varios «Servidores SCADA» con varios «Clientes SCADA» cada unos de ellos. De hecho, un «Cliente SCADA» puede actuar como cliente para mas de un «Servidor SCADA». También es posible que un «Servidor SCADA» actúe como «Cliente SCADA» de otro «Servidor SCADA» conformando así una gran red de «Clientes y Servidores SCADA» según lo requieran las necesidades de información para el proceso objeto, y la naturaleza propia del proceso en cuestión.

Distribución geográfica del sistema SCADA

Determinada por las características del proceso objeto, la distribución geográfica del sistema SCADA en su conjunto obedece a las necesidades de información de los propietarios del sistema y de sus operadores, sin dejar de lado un criterio lógico y de conveniencia.

Asimismo, la complejidad del proceso implicará requerir de uno o varios equipos PLC o interfaces con los instrumentos de medición, que deberán ser conectados a los equipos PC del sistema de supervisión. En consecuencia el SCADA deberá ser lo suficientemente flexible para cubrir las necesidades de control de un proceso objeto simple y local, hasta las de uno de complejidad elevada donde los equipos de medición se encuentren separados por grandes distancias. Pero, aún así, debe observar el proceso como un sólo sistema el cual debe ser controlado por el SCADA.

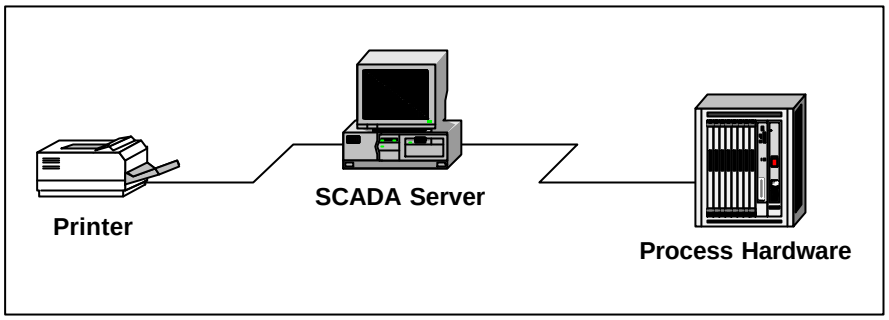
De la observación de éstas necesidades surgen distintos modelos de distribución geográfica que pueden ser resumidos en los siguientes tipos para su estudio.

Modelo local con una sola estación

Este modelo responde a la necesidad de emplear el sistema SCADA para la supervisión de un proceso objeto de baja complejidad donde los datos colectados del mismo residen en un equipo que centraliza la operación. Si se requiere de una interfase de visualización se usará el mismo equipo PC donde se ejecuta el sistema SCADA.

En este esquema el SCADA actúa como tal mientras cumple el papel de estación de visualización para los operadores. Esto implica que los usuarios deben acercase físicamente al equipo PC para poder interactuar con el sistema SCADA, analizar o requerir informes, como así también notificarse del estado de actividad del mismo.

Generalmente esta formado por un equipo PC conectado físicamente al equipo PLC o a la interfase con los instrumentos. Es posible utilizar medios de comunicación que incluyan enlaces de radio o telefónicos para conectar el equipo PC con los instrumentos. Pero dicho esquema obedece a los requerimientos de los instrumentos y sus protocolos y no afecta ni condiciona la funcionalidad del sistema SCADA instalado en los equipos PC.



Esquema geográfico local de un SCADA con una estación

Modelo local con varias estaciones de supervisión

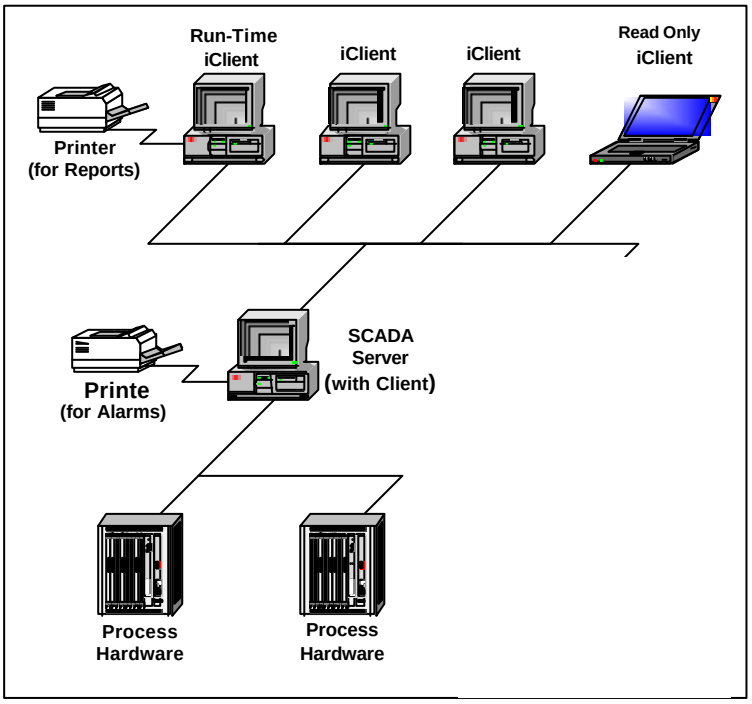
Este modelo contempla la posibilidad de que varios operadores puedan consultar la información disponible y operar el SCADA desde varias estaciones de trabajo simultáneamente.

Destinado principalmente para trabajar con procesos de una complejidad mayor que el anterior, en el cual el proceso objeto requiere de la supervisón de varios operadores para su funcionamiento, el modelo requiere de un equipo PC que se conecta físicamente con el equipo PLC o la interfase con los instrumentos y actúa como servidor de datos para otras estaciones que visualizarán los datos previamente obtenidos por éste. Estas estaciones reciben el nombre de Clientes y actúan como equipos terminales de datos.

Las funcionalidades disponibles en los equipos clientes son las mismas que las del equipo servidor. Es decir, se pueden visualizar los datos de igual manera, operar con los valores del proceso para modificarlos, requerir informes, analizar datos históricos previos, etc.

El hecho de que haya estaciones de trabajo simultáneas implica que el sistema SCADA debe llevar un control de las acciones que se llevan a cabo en cada estación. Surge así la necesidad de la identificación de los operadores del sistema que se encuentran operando el SCADA en cada una de las estaciones de manera que pueda auditarse las acciones realizadas por los operadores en su conjunto y que afectan al funcionamiento de todo el sistema.

En este esquema pueden conectarse hasta 100 equipos clientes que toman datos de un solo equipo servidor utilizando la facilidad de conexión en red que provee el sistema SCADA.



Esquema geográfico local con varias estaciones clientes

En el esquema se identifica un nodo denominado «SCADA Server with Client» que actúa como servidor de datos para la aplicación SCADA. Así mismo, éste nodo tiene la habilidad de mostrar información gráfica permitiendo el uso de éste equipo como nodo de visualización y operación de la aplicación.

Los nodos en la parte superior del esquema actúa todos como clientes de ambos servidores SCADA. Su diferencia en la nomenclatura responde al modo de licenciamiento de los mismos según lo determina el fabricante.

Modelo distribuido en una red local

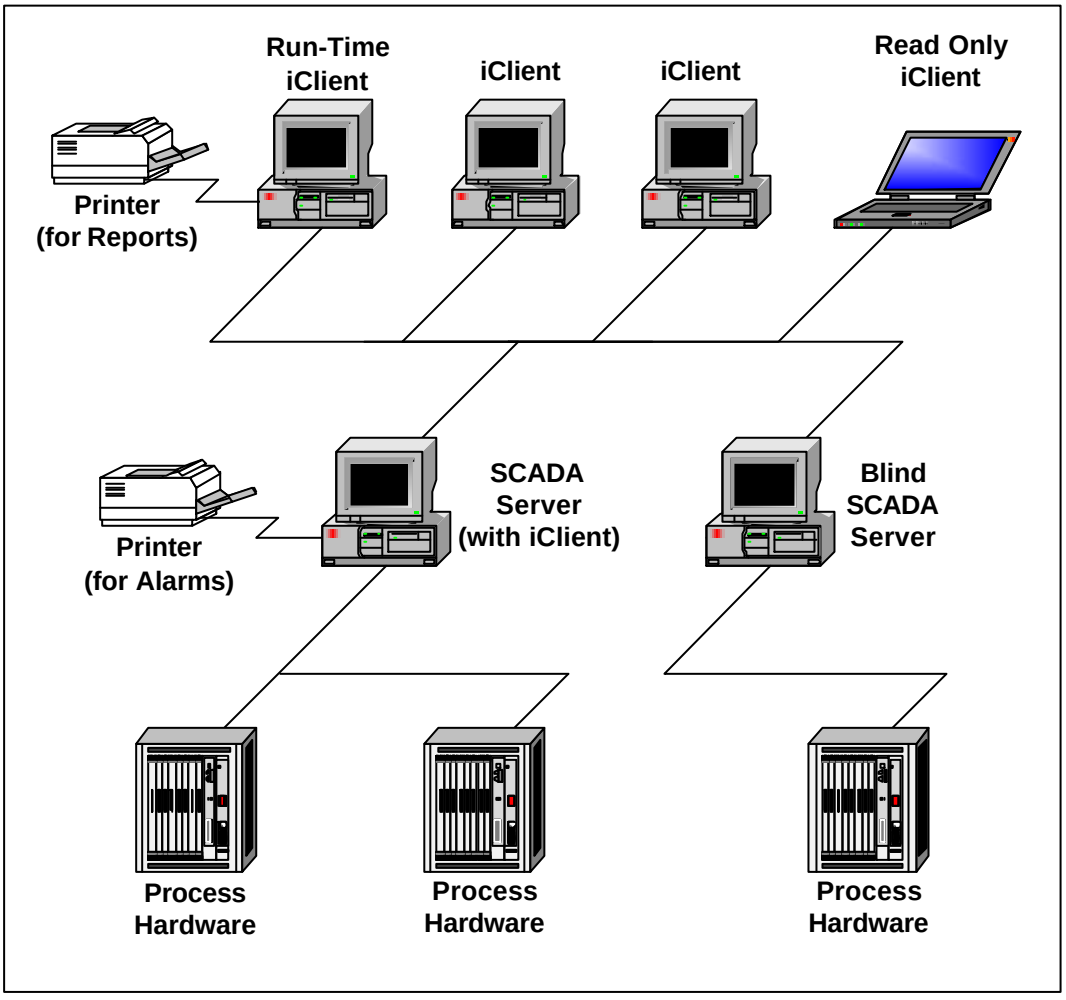
El modelo se aplica cuando el proceso objeto esta separado en unidades de proceso o etapas de proceso. Cada etapa del proceso posee un grado de supervisión casi independiente de la otra, pero no ajena a éstas.

Pueden esquematizarse entonces un modelo donde se coloca un nodo SCADA servidor de datos por cada etapa del proceso. Si bien cada servidor actúa en forma autónoma es posible que cierta información de estado sea distribuida entre los nodos servidores SCADA de manera tal que todos posean información relativa al proceso en el que participan, pero que no necesariamente proviene de la etapa de proceso en la cual están involucradas.

Como estaciones de supervisión pueden también colocarse nodos de visualización que sean capaces de mostrar información general del proceso o detallada de cada etapa.

Es de esperar que los informes generados por este tipo de esquema SCADA agrupen información de todas las etapas controladas por el SCADA y que éste sea capaz de tomar decisiones basadas en la información de etapas anteriores o posteriores.

La disposición geográfica de las estaciones de trabajo, tanto servidores como clientes, suele seguir el modelo lógico del proceso objeto. Así mismo la lógica de navegación de pantallas en las estaciones esta relacionada con el orden de las etapas de proceso y responden al modelo lógico del proceso y sus etapas.



Esquema distribuido en una red LAN

En el esquema se identifican dos nodos actuando como servidores SCADA, los cuales están conectados físicamente al hardware de proceso. El nodo denominado como «SCADA Server with iClient» actúa como servidor de datos y cliente al mismo tiempo, permitiendo el uso de este nodo como estación de operación. Por el contrario, el nodo denominado como «Blind SCADA Server», sólo proporciona datos a otros nodos. No hay aplicación de visualización en éste y, por consiguiente, no puede ser usado como estación de operación.

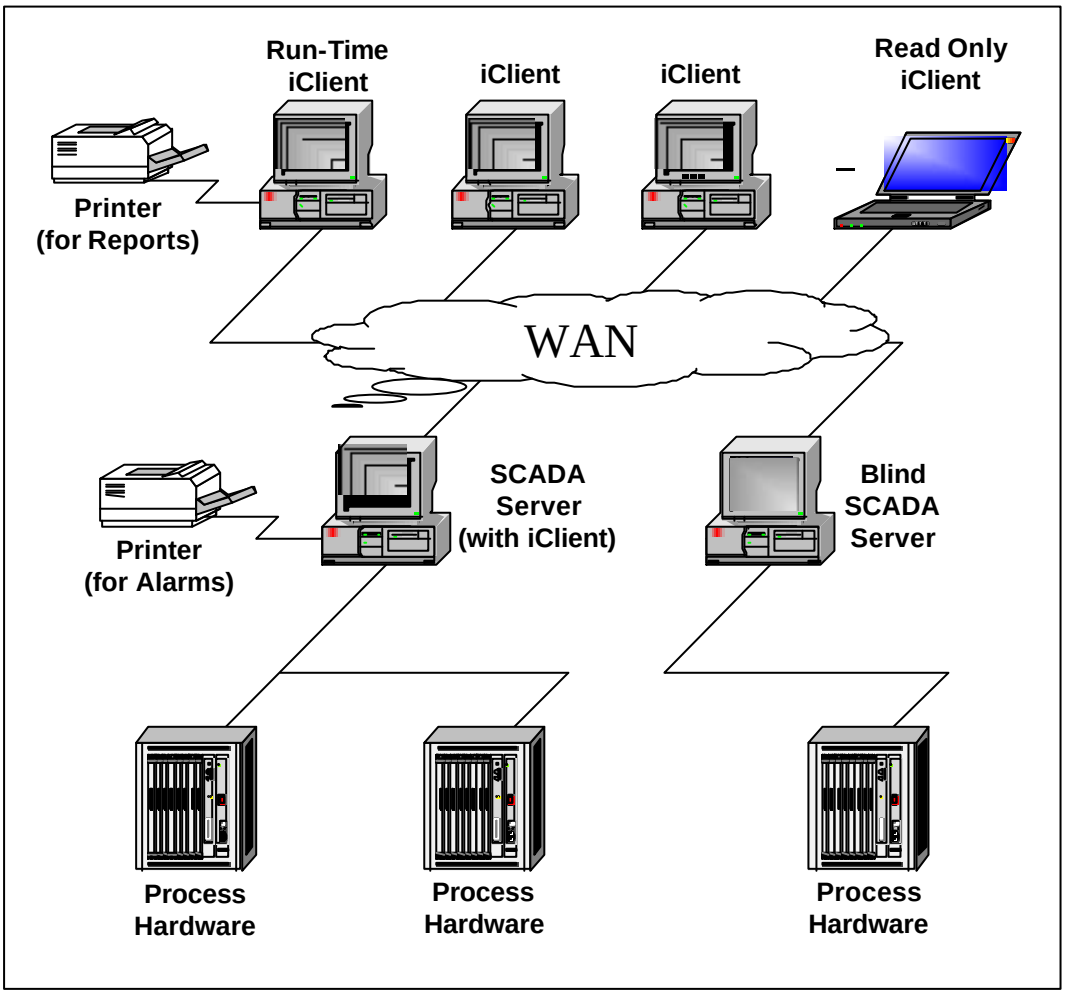
Los nodos en la parte superior del esquema actúa todos como clientes de ambos servidores SCADA. Su diferencia en la nomenclatura responde al modo de licenciamiento de los mismos según lo determina el fabricante.

Modelo distribuido en una red amplia (WAN)

Similar al esquema anterior, éste modelo contempla la posibilidad de que las distintas etapas del proceso se encuentran geográficamente distantes. Entonces se utilizan los recursos provistos por la red WAN existente para la interconexión de los nodos SCADA tanto servidores como clientes.

En la actualidad la implementación de VPNs (Red Privada Virtual) permite implementar sistemas SCADA que utilizan la Internet como medio de comunicación entre estaciones clientes y servidores.

En este caso la distribución geográfica responde a la naturaleza del proceso, la geografía donde el proceso reside, la ubicación de los usuarios y operadores, todo esto relacionado con la envergadura del proceso.



Esquema distribuido en una red WAN

Servicios de Terminal

Introducción a los Servicios de Terminal incluidos en Microsoft Windows 2000

Introducción

Frente a la necesidad de llevar una interfase gráfica de una aplicación SCADA a un dispositivo móvil, para que el usuario pueda interactuar con éste mientras aprovecha los beneficios de la libertad de movimiento y así hacer más productiva su tarea, se plantea la dicotomía de emplear una aplicación de mercado o enfrentar un desarrollo propietario.

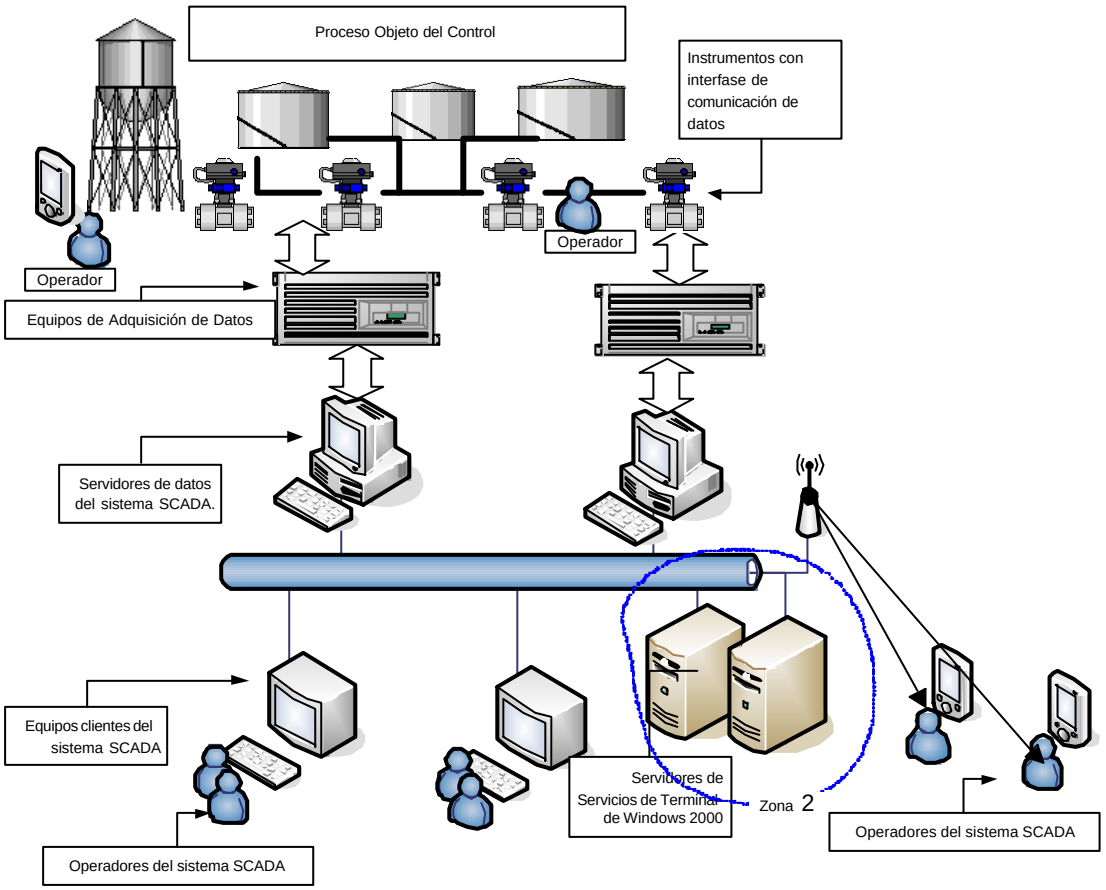
Muchas veces la elección, influenciada por las propias limitaciones de la herramienta de desarrollo de aplicaciones SCADA elegida para efectuar el control y la supervisión del proceso objeto, se inclina notoriamente hacia el largo camino de un desarrollo propio.

En particular, la herramienta de desarrollo de aplicaciones SCADA presentada en éste escrito, puede satisfacer tanto las necesidades de conectividad e integración de un desarrollo propietario, como las exigencias de calidad y diseño de una aplicación certificada para los Servicios de Terminal de Microsoft Windows 2000.

Sin embargo la decisión tomada no se apoya en la oferta de la supuesta seguridad de una certificación o la promesa de una rápida implementación, sino en la posibilidad de aprovechar las bondades que los Servicios de Terminal de Microsoft Windows ofrecen.

De esta forma, pasa a ser importante el grado de compromiso y cumplimiento que la herramienta de desarrollo de aplicaciones SCADA seleccionada pueda argumentar, defender y presentar como distintivo frente a sus competidores para correr en éste entorno operativo.

En la solución propuesta los Servicios de Terminal de Microsoft Windows 2000 actúan como nexo de la interfase gráfica de la aplicación SCADA presentada en los dispositivos móviles y los servidores de datos SCADA.



Los siguientes párrafos explayan brevemente las consideraciones y prestaciones más importantes de los Servicios de Terminal de Microsoft Windows 2000 que hacen de ésta oferta la solución más conveniente para la aplicación propuesta.

Descripción de los Servicios de Terminal de Windows 2000

Los Servicios de Terminal de Microsoft proveen acceso a Microsoft Windows 2000 y las más recientes aplicaciones basadas en Windows para computadoras clientes. También provee acceso a los escritorios de Windows y las aplicaciones instaladas en el servidor desde cualquier lugar usando los clientes soportados.

Esta herramienta incluida en Windows 2000 Server resulta más que útil para los administradores de tecnología de la información y de los sistemas de información que quieran aumentar la flexibilidad en las implementaciones de las aplicaciones, controlar el costo de la administración de computadoras o administrar remotamente los recursos de red

Los Servicios de Terminal corriendo sobre un servidor Windows 2000 permite que la ejecución de aplicaciones cliente, el procesamiento de datos, y el almacenamiento de datos ocurra en el servidor en lugar de en el equipo cliente. Éste provee acceso remoto a un escritorio de Windows del servidor utilizando un programa de emulación de terminal.

El programa de emulación de terminal puede ejecutarse en un numeroso grupo de equipos clientes, como ser computadoras personales, equipos portátiles basados en Windows CE.

El término Terminal basada en Windows (WBT, por su siglas en Ingles de Windows based Terminal) ampliamente describe una clase de equipos terminales livianos que pueden obtener acceso a servidores ejecutando sistemas operativos multiusuarios tipo Windows, como los servicios de terminal de Windows 2000.

Con los Servicios de Terminal, el programa de emulación de terminal envía sólo las pulsaciones sobre el teclado y los movimientos del ratón del equipos cliente al servidor. El servidor de Terminales realiza toda la manipulación de datos en forma local y la devuelve a la pantalla del equipo cliente.

Este modo de trabajo permite el control remoto de servidores y centraliza la administración de aplicaciones, mientras que minimiza el ancho de banda utilizado entre el equipo cliente y el servidor.

Los usuarios obtiene acceso a los Servicios de Terminal utilizando cualquier conexión que use el protocolo Transmission Control Protocol / Internet Protocol (TCP / IP) incluyendo Servicio de Acceso Remoto (RAS), Ethernet, Internet, redes inalámbricas, redes de área amplia (WAN) o redes privadas virtuales (VPN). Entonces la experiencia del usuario es sólo limitada por las características del vínculo mas débil en la conexión.

El servicio de terminal es una opción incluida en Windows 2000 que puede funcionar en uno de los dos siguientes modos:

Administración Remota

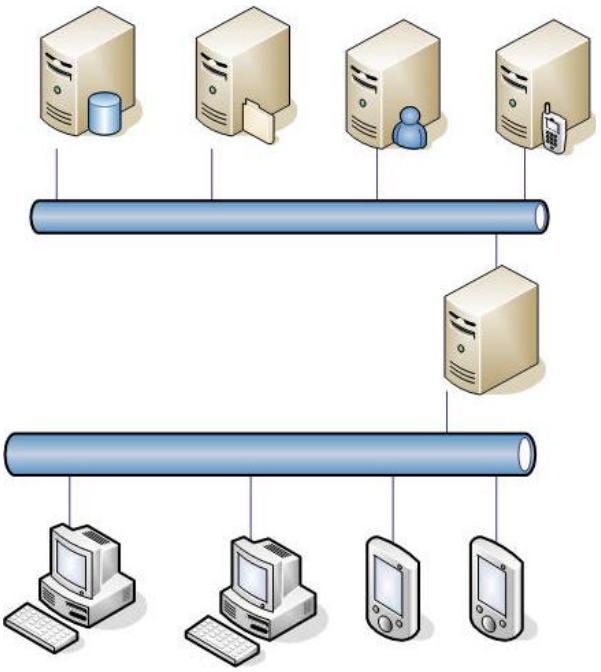
La administración remota da a los administradores de red y administradores de sistemas una poderosa herramienta para administrar a cada servidor Windows 2000 sobre una conexión TCP / IP existente. Es posible administrar los recursos compartidos de impresión y de archivos, editar el registro de Windows de otra computadora en la red, así como también ejecutar cualquier tarea como si uno estuviera sentada en la consola del servidor.

En el modo Administración Remota sólo instala los componentes de administración remota de los Servicios de Terminal sin instalar los componentes para compartir aplicaciones. Esto significa que puede utilizarse el modo de administración remota en servidores de aplicaciones de misión crítica con muy poca carga extra de trabajo.

Servidor de Aplicaciones

En modo servidor de aplicaciones es posible implementar y administrar las aplicaciones desde una ubicación central, ahorrando así tiempos de administración e implementación como los esfuerzos requeridos para el mantenimiento y la actualización.

Luego que una aplicación es instalada en el servidor de terminales varios clientes pueden conectarse al servidor, utilizando RAS, LAN, WAN, utilizando varios tipos diferentes de equipos clientes para acceder a la aplicación.



Esquema de Servicios de Terminal como servidor de aplicaciones

Implementación de los Servicios de Terminal de Microsoft

De los distintos escenarios que pueden aplicarse en la implementación de los Servicios de Terminal de Microsoft el escenario de un escritorio de Windows central es el mas conveniente para el estudio del sistema en cuestión.

La implementación de un escritorio central de Windows se logra cargando un escritorio de aplicación en un servidor Windows 2000 con los servicios de Terminal activados en modo Servidor de Aplicaciones.

Cada computadora cliente tiene una única y simple aplicación que permite la emulación de cada escritorio de Windows de cada usuario del servidor mientras que las aplicaciones de usuario están realmente ejecutándose en el servidor.

En este escenario los usuarios pueden ejecutar un conjunto controlado de aplicaciones estandarizadas aún desde sitios remotos o usando equipos propietarios, mientras que el sistema de seguridad es el encargado de proveer los accesos de usuario adecuados a los clientes.

Consideraciones para la implantación de la aplicación

Para la implantación de la aplicación en un entorno de Servicios de Terminal es necesario observar los requerimientos de la aplicación. Algunas aplicaciones tienen características que pueden impedir su funcionamiento con Servicios de Terminal o pueden desempeñarse con muy bajo rendimiento. Por esta razón se debe instruir a los usuarios a instalar éste tipo de aplicación en forma local.

Específicamente es necesario identificar las aplicaciones que requieran algún hardware especial para correr, como ser lectores de códigos de barras o tarjetas. Es posible utilizar este tipo de dispositivos sólo si es posible conectar los dispositivos al equipo cliente de manera tal que éste sea reconocido como un periférico tipo teclado. Los dispositivos que se conectan al puerto paralelo o serial del equipo cliente no son actualmente reconocidos por clientes de Servicios de Terminal basados en el protocolo RDP (Remote Desktop Protocol).

Del mismo modo las aplicaciones Multimedia o aplicaciones que tiene trabajo gráfico muy pesado no corren bien bajo los Servicios de Terminal.

Por otro lado hay aplicaciones que requieren una instalación especial o la ejecución de algún código particular ejecución. Generalmente éstos códigos compensan la falta del Registro de Windows o el soporte de almacenamiento para múltiples usuarios. En algunos casos será necesario escribir código especial de ejecución para aplicaciones que no fueron desarrolladas para entornos multiusuarios.

Consideración de la red para el acceso a los Servicios de Terminal

Es necesario considerar la infraestructura de la red cuando se implementa un entorno de Servicios de Terminal. En la mayoría de los casos, esto involucra diseños generales para la red, pero en algunos casos

los Servicios de Terminal tienen sus consideraciones particulares. Por ejemplo, los Servicios de Terminal no pueden pasar la dirección IP de un cliente individual a una aplicación.

Aplicaciones multiusuario que requieren que cada usuario tenga una dirección IP única no trabajarán adecuadamente en un entorno básico de Servicio de Terminal porque cada usuario parece originar la sesión desde la misma dirección IP, la cual es la del servidor de Servicios de Terminal propiamente dicho.

Por ejemplo, algunos cortafuegos (Firewalls) y servidores propietarios usan la dirección IP del cliente para determinar opciones de seguridad y la ubicación física del cliente. Es necesario alterar el entorno de Servicios de Terminal o la aplicación para casos como éste.

Es importante notar que todos los usuarios compartirán las misma dirección IP para conectarse desde un determinado servidor de Servicios de Terminal. En aplicaciones que monopolicen este recurso provocaran interferencias con la operación normal del servidor.

Balance de carga de red y Servicios de Terminal

El balance de carga de red es usado para distribuir el trabajo entre dos o más servidores. El balance de carga representa entonces un grupo de servidores utilizando una misma dirección IP virtual, junto a un mecanismo para distribuir la carga de éstos en forma dinámica.

Esto es útil en entornos donde existen numerosos usuarios conectados para usar aplicaciones financieras o una base de datos donde preservar la sesión de usuario no resulta crítico. Debido a que un servidor con Servicios de Terminal no es apropiado para el trabajo en forma de «Cluster», el balance de cargas de red puede ser una solución suficiente para asistir a un gran grupo de usuarios.

Tradicionalmente la solución de balance de carga no puede garantizar que el usuario se reconectará al mismo servidor. En casos donde exista este escenario no suele haber datos relacionados con la sesión específica del usuario. Incluso puede optarse por no soportar la reconexión de los usuarios al mismo servidor para reducir requerimientos y mejorar la seguridad.

Alternativamente puede ser posible usar las facultades de ciertos tipos de balance de cargas para, periódicamente, reconectarse al mismo servidor de Servicios de Terminal preservando así la sesión de usuario.

Preservar la sesión de usuario no es análogo a preservar los datos de usuario. Es posible para esto manejar dos o más servidores de Servicios de Terminal de manera tal de permitir a los usuarios conectarse a cualquier servidor y tener acceso apropiado almacenando los datos relativos al usuario y sus perfiles de manera externa a los servidores de Servicio de Terminal. Entonces el servidor sólo busca en este lugar de almacenamiento común los perfiles del usuario y su información almacenada. De esta forma los usuarios tienen la misma experiencia independientemente de cual servidor se encuentre conectados.

El balance de carga de red utiliza el concepto de «afinidad de IP», el cual permite a un usuario con la misma dirección IP reconectarse al mismo equipo servidor si su sesión fue desconectada. Esto significa que el balance de carga de red puede ser usado si el usuario no ha cambiado de equipo cliente o cambiado de dirección IP.

Consideraciones para la seguridad

La seguridad es un componente esencial en el plan de implementación de los Servicios de Terminal. Además de las consideraciones habituales de seguridad indicadas durante la implementación de Windows 2000, la implementación de los Servicios de Terminal tiene consideraciones que son específicas para un entorno multiusuario, como ser sistema de archivos (FAT / NTFS), procedimientos de identificación y acceso, derechos de usuarios y administradores, encripción y otros.

Sistema de archivos NTFS

Dada la naturaleza multiusuario de los Servicios de Terminal, es altamente recomendable la utilización de el sistemas de archivos NTFS de Windows 2000 como el único sistema de archivos en el servidor, en lugar del sistema de archivos FAT (File Allocation Table).

FAT no ofrece seguridad a carpetas ni a usuarios, mientras que con NTFS es posible limitar subdirectorios a ciertos usuarios o grupos de usuarios.

Esto resulta de vital importancia en entornos multiusuario como los Servicios de Terminal. Sin la seguridad que provee NTFS cualquier usuario tendría acceso a cada directorio y archivo en el Servidor de Terminales.

Derechos de usuarios

Los Servicios de Terminal son distribuidos con un conjunto de permisos de usuario por defecto que pueden ser modificados para agregar seguridad. Para poder acceder a un servidor de Terminales un usuario

debe tener el derecho de acceso local en dicho equipo («Logon Locally»).

Por defecto un servidor de Terminal en modo Administración Remota solo garantiza ese derecho a los Administradores en ese equipo, mientras que uno en modo Aplicaciones Compartidas garantiza este derecho a todos los miembros del grupo Usuarios.

Como Windows 2000 incluye todos los usuarios del dominio en el grupo de Usuarios de una computadora que no sea un controlador de dominio, todos los usuarios del dominio estarán permitidos para acceder al servidor de Terminales ofreciendo Compartir Aplicaciones.

Los usuarios que tienen acceso a través de un protocolo como es RDP, y los que acceden interactivamente a un servidor con Servicios de Terminal son automáticamente incluidos en el grupo local predefinido como «Usuarios de Servicios de Terminal». Un usuario sólo pertenece a este grupo mientras accediendo interactivamente a un servidor de Terminal. Este grupo predefinido da a los administradores control sobre los recursos que los usuarios pueden acceder de los Servicios de Terminal.

Se debe evitar configurar los Servicios de Terminal en un controlador de dominio ya que cualquier política de derechos de usuario que se aplique a este servidor se aplicará a todos los controladores de dominio en el dominio. Por ejemplo, para usar los Servicios de Terminal los usuarios deben estar autorizados a acceder en forma local («Log on Locally»). Si el servidor que ejecuta los Servicios de Terminal es un controlador de dominio, los usuarios podrán acceder localmente a todos los controladores de dominio en el dominio del servidor de Servicios de Terminal.

Acceso automático

Dependiendo en como los usuarios usarán los Servicios de Terminal, tal vez deba dárseles acceso al sistema de archivos. Los usuarios que sólo necesitan acceso a un aplicación específica, como una base de datos, pueden ser dirigidos directamente a la aplicación en el inicio. Esta directiva puede también ser aplicada a un grupo de usuarios.

Según los requisitos, es posible permitir que los usuarios se conecten al servidor sin introducir su usuario y contraseña, implementándolo por usuario o por servidor. Debe utilizarse esta funcionalidad con cautela ya que cualquier usuario con un cliente de Servicios de Terminal instalado podrá conectarse a éste.

Cambios en el proceso de acceso

En las secuencias de comandos de acceso se debería considerar verificar por la presencia de las variables de control %CLIENTNAME% o %SESSIONNAME%. Estas variables de entorno son específicas de los Servicios de Terminal y sólo aparecen en un entorno de usuario cuando éste se conecta a un servidor de Servicios de Terminal, tanto en modo de Administración Remota como en modo Servidor de Aplicaciones.

Encriptación

Existen tres niveles de encriptación para asignar a la transferencia de datos entre el servidor de Servicios de Terminal y el equipo cliente. Sin embargo los más altos niveles de encriptación están disponibles sólo en Norteamérica.

Bajo nivel de encriptación

Aplicando un bajo nivel de encriptación el tráfico desde el cliente hacia el servidor es encriptado usando el algoritmo RC4 y una clave de 56 bits (40 bits para clientes que utilicen RDP v 4.0), mientras que el tráfico desde el servidor hacia el cliente no es encriptado. El bajo nivel de encriptación protege los datos sensibles como una contraseña y datos de aplicación. Los datos enviados desde el servidor hacia los clientes es refrescado en pantalla, el cual es difícil de interceptar aún sin encriptación.

Nivel de encriptación mediano

Utilizando un nivel de encriptación mediano el tráfico en ambas direcciones es encriptado usando al algoritmo RC4 y una clave de 56 bits (40 bits para clientes que utilicen RDP v 4.0).

Alto nivel de encriptación

Con este nivel de encriptación el tráfico en ambas direcciones es sujeto a encriptación usando el algoritmo RC4 y una clave de 128 bits en la versión para Norteamérica de los Servicios de Terminal. En la versión de exportación de Servicios de Terminal la encriptación alta usa RC4 y una clave de 56 bits (40 bits para clientes que utilicen RDP v 4.0).

Consideraciones adicionales acerca de la seguridad

Cuando se planifica la seguridad para los Servicios de Terminal, se deben considerar los siguientes

aspectos:

Tarjetas Inteligentes (Smart Cards)

El acceso interactivo de Windows 2000 tiene la habilidad de autenticar a un usuario con la red de Directorio Activo usando un certificado X.509 versión 3 almacenado en una tarjeta inteligente junto con la clave privada. Sin embargo esta prestación no esta disponible a los usuarios que se identifican a los Servicios de Terminal. Esto también aplica a otros dispositivos de autenticación basados en hardware propietario.

Seguridad en redes y comunicaciones

El Acceso Remoto no limita a los usuarios a acceder a los Servicios de Terminal. Por consiguiente si un usuario establece un vínculo por MODEM o vinculo VPN a Internet todos los usuarios usando Servicios de Terminal ganan acceso a este vínculo.

Servicios de información sobre Servicios de Terminal

Es necesario deshabilitar la conexión anónima al servicio de transferencia de archivos FTP para prevenir el acceso inseguro al sistema de archivos.

Acceso

Los Servicios de Terminal pueden proveer a los usuarios remotos acceso a aplicaciones que normalmente serian inestables de otro modo dado el bajo rendimiento ofrecido por los servicios de discado o redes amplias (WAN) de baja velocidad.

La información de la pantalla, el dispositivo ratón y del teclado enviado por los Servicios de Terminal emplean típicamente menos recursos de red que una aplicación que deba ser bajada y luego ejecutad en forma local en la computadora del usuario remoto.

Acceso a los Servicios de Terminal usando Internet

Los usuarios pueden utilizar las ventajas del protocolo de túnel nivel 2 (L2TP) o el protocolo de túnel punto a punto (PPTP) para conseguir acceso a los Servicios de Terminal sobre Internet. Usando encriptación ambas opciones de túnel proveen acceso seguro a una red privada a usuarios operando sobre un medio público.

Estos protocolos son recomendados por la seguridad que éstos proveen, pero los Servicios de Terminal pueden ser accedidos por cualquier implementación de TCP/IP.

Cortafuegos (Firewalls)

Si la organización utiliza una implementación de cortafuegos para seguridad, se debe contemplar que el puerto 3389 debe permanecer abierto para permitir la conexión del protocolo RDP entre los clientes y el servidor.

Para lograr mejores resultado se recomienda la utilización de cortafuegos que utilicen la autenticación basada en el usuario. Un cortafuegos que garantiza acceso basado en la dirección IP permite el acceso de usuarios si la dirección del servidor de Servicios de Terminal ha sido garantizada en el cortafuegos.

Protocolo RDP versión 5.0

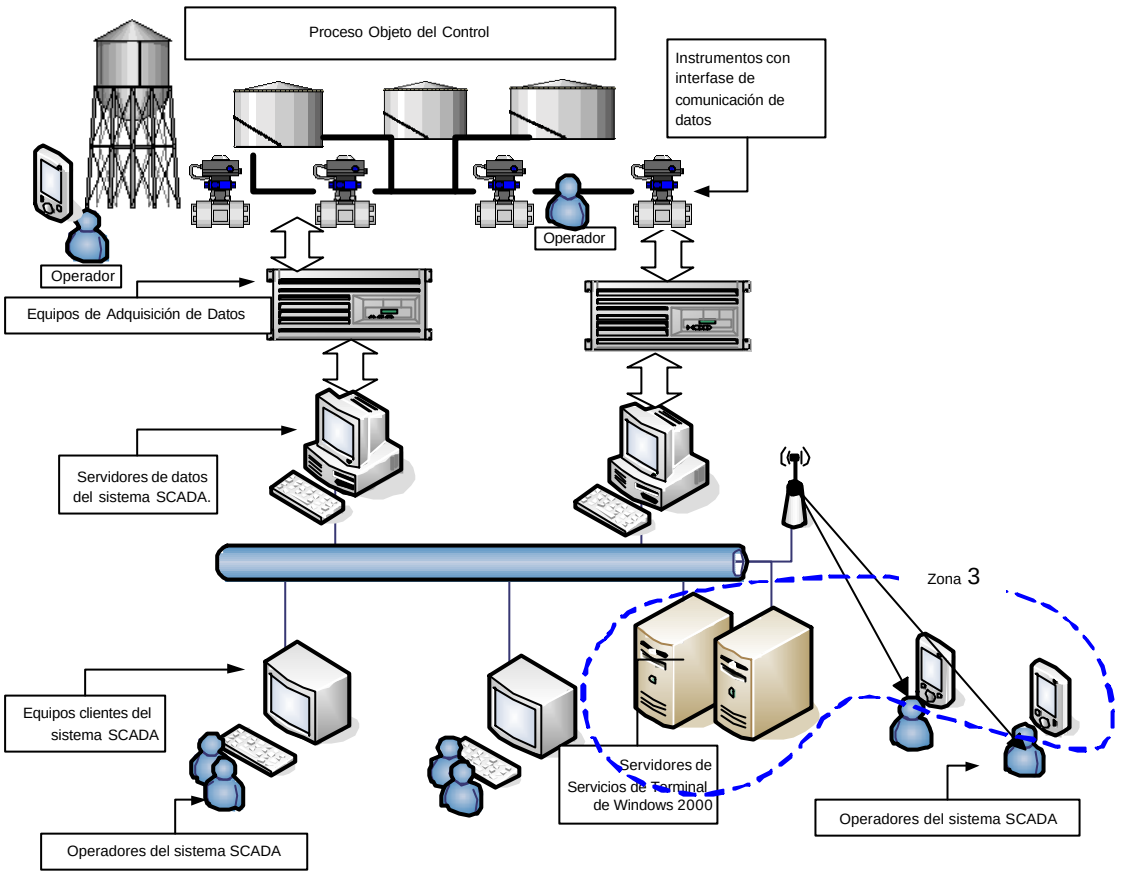
Introducción al protocolo RDP (Remote Desktop Protocol) versión 5.0 empleado en los Servicios de Terminal de Microsoft Windows 2000

Introducción

El empleo de los Servicios de Terminal de Microsoft Windows 2000 como plataforma operativa para la implementación de una aplicación SCADA con dispositivos móviles como la presentada, está fundamentado en las prestaciones de servicio alcanzadas por la combinación de las tecnologías seleccionadas.

En particular el uso de los Servicios de Terminal de Microsoft Windows 2000 sobresale por el uso del protocolo RDP versión 5.0. Éste se encarga de la interacción con el usuario, tanto desde el punto de vista de la presentación gráfica de la información del SCADA, como así también de las respuestas y acciones ejecutadas por el operador hacia la aplicación.

En la solución propuesta RDP versión 5.0 es empleado como protocolo de aplicación entre los dispositivos móviles y el servidor de Servicios de Terminal.



Las siguientes características de RDP versión 5.0 son las que mejor argumentan el empleo de los Servicios de Terminal de Microsoft Windows 2000 como la opción más conveniente para el desarrollo de la implementación.

Características sobresalientes de RDP versión 5.0

Arquitectura básica

El Protocolo de Escritorio Remoto, RDP por sus siglas en Ingles de Remote Desktop Protocol, esta basado en la familia de protocolos T 120 y actúa como una extensión de éste.

RDP es un protocolo con capacidad de múltiples canales. Éste permite canales separados virtuales para dispositivos de comunicación que presentan los datos enviados desde el servidor, ya sea usando encriptación o no, y la respuesta de teclado y *mouse* *del equipo cliente-

RDP provee una base flexible para construir aplicaciones con más capacidades. Soporta hasta 64000 canales separados para la transmisión de datos así como también transmisión multipunto. Ejemplos de estas capacidades en RDP versión 5.0 son las características de redirección de impresión, mapeo de la aplicación Portapapeles (Clipboard) entre otras aplicaciones de canales virtuales.

RDP usa su propio controlador de video en el servidor para generar la imagen de salida construyendo la información de video en paquetes para ser enviados por la red al equipo cliente. Del lado del cliente se recibe la imagen generada y se interpretan los datos en la correspondiente llamada a la API (Application Program Interface) de WIN32 GDI.

Del lado de los dispositivos de entrada los mensajes de teclado y *mouse* del cliente son redirigidos desde el cliente hacia el servidor. En el servidor, RDP usa su propio controlador de teclado virtual y el controlador de *mouse* virtual para recibir estos eventos de teclado y *mouse.*.

Encriptación

Sin la encriptación sobre el protocolo de visualización es muy simple interceptar la señal sobre los cables para descubrir la contraseña de un usuario cuando éste accede al servidor. Permitir a un administrador acceder al servidor usando un protocolo no encriptado expone los recursos completos del dominio a la

vulnerabilidad de los ataques, especialmente si está conectado en una red pública sin usar una red privada virtual. Es importante notar que los protocolos que usan la técnica de «scrambling» (mezcla de caracteres) para proteger los datos son tan vulnerables a éste tipo de ataques como los protocolos que usan el texto textual para enviar datos.

RDP usa el cifrado RC4 de la seguridad de RSA. RC4 es un conjunto cifrado diseñado para encriptar eficientemente pequeñas cantidades de datos de tamaño variable. RC4 esta diseñado para comunicaciones seguras sobre redes. Es usado también en protocolos como SSL el cual encripta el tráfico desde y hasta los sitios Web seguros.

En Windows 2000 los administradores pueden elegir encriptar los datos usando claves de 56 o 128 bits. La encriptación es bidireccional, excepto cuando se elige la opción de baja seguridad, la cual sólo encripta los datos que viajan desde el cliente hacia el servidor. Indicado principalmente para proteger la información sensible como ser claves de acceso.

El valor por defecto de esta opción es medio. La cual utiliza una clave de 56 bits para encriptar los datos en forma bidireccional. Es posible emplear una encriptación con clave de 128 bits luego de instalar el adicional de encriptación alta de Windows 2000, Windows 2000 High Encription Pack.

Funcionalidad de reducción de ancho de banda

El protocolo RDP soporta varios mecanismos para reducir la cantidad de datos transmitidos sobre una conexión de red.

Además de la comprensión de datos, el cual es la recomendación por defecto para todas las sesiones de Servicios de Terminal, y el almacenamiento temporario de imágenes de mapas de bits y fragmentos en RAM, RDP versión 5.0 agrega la persistencia al almacenamiento temporario de imágenes de mapas de bits, el cual aumenta el almacenamiento temporario de RAM en 10 mega bites (MB) en el almacenamiento de imágenes de mapas de bits en disco.

Las imágenes de mapas de bits que son almacenadas temporáneamente en memoria pueden ser almacenadas también en el almacenamiento persistente para imágenes de mapas de bits, el cual también esta disponible para sesiones de Servicios de Terminal subsecuentes.

Este almacenamiento temporario puede mejorar substancialmente el desempeño sobre conexiones de bajo ancho de banda, especialmente al ejecutar aplicaciones que hagan un eso extensivo de grandes imágenes de mapas de bits.

Desconexiones

Los usuarios pueden interrumpir una sesión sin necesidad de desconectarse del servidor de aplicaciones permanentemente. Cuando el usuario recupera la conexión al sistema, ya sea por el mismo dispositivo cliente u otro distinto, el usuario es conectado automáticamente a su sesión anteriormente interrumpida.

Incluso si el usuario sé reconecta con una resolución de pantalla diferente, RDP automáticamente ajusta el tamaño de la sesión de Servicios de Terminal al tamaño correcto.

Portapapeles

Los usuarios pueden cortar, copiar y pegar textos y gráficos entre aplicaciones que estén corriendo en la máquina local y las que estén corriendo en una sesión de Servicios de Terminal, incluso entre sesiones.

Redirección de Impresión

Las aplicaciones que estén corriendo dentro de una sesión de Servicios de Terminal pueden automáticamente imprimir en una impresora local conectada al dispositivo cliente.

Canales virtuales

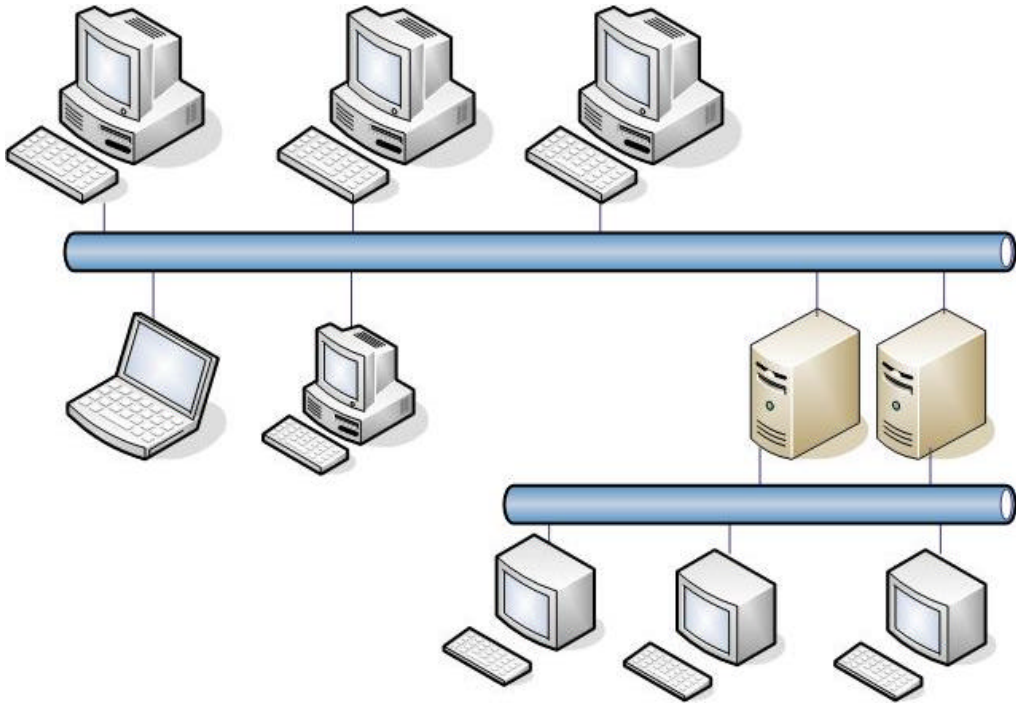
Gracias a la arquitectura de canales virtuales de RDP, las prestaciones de las aplicaciones existentes pueden ser aumentadas y nuevas aplicaciones pueden ser desarrolladas para agregar funcionalidades que requieran la comunicación entre el dispositivo cliente y una aplicación corriendo en una sesión de Servicios de Terminal en el servidor.

Control remoto

El control remoto facilita la asistencia a los usuarios de las aplicaciones. Las actividades del teclado, las imágenes enviadas y las del *mouse* son compartidas entre dos sesiones de Servicios de Terminal, permitiendo al personal de soporte de aplicaciones diagnosticar y resolver problemas de configuración como así también entrenar al usuario en forma remota.

Balance de carga de red

El protocolo RDP utiliza la ventaja de balance de cargas de red (NLB, Network Load Balancing) disponible en las versiones Advanced Server y Datacenter Server de Windows 2000, para permitir a los clientes de Servicios de Terminal conectarse a un grupo de servidores ejecutando los Servicios de Terminal, eliminando así un punto de falla único.



Esquema de conexión de terminales usando balance de cargas

Selección de aplicaciones

Selección de aplicaciones para Windows 2000 con Servicio de Terminal

Introducción

Los Servicios de Terminal son un servicio configurable incluido en el sistema operativo Windows 2000 Server que le proporciona la capacidad ejecutar aplicaciones basadas en Windows-32 en forma centralizada en un servidor. Esta tecnología fue incorporada en la versión Windows NT Server Teminal Edition, del antecesor Windows NT 4.0.

En el sistema operativo Windows 2000 Server, los Servicios de Terminal están completamente integrados con el corazón del sistema operativo. Los clientes emuladores de Servicios de Terminal están disponibles para varias plataformas de escritorio, como ser MS-DOS, Windows, Macintosh, Unix y otro, incluso existen agregados de terceras partes para equipos especiales de escritorio que no estén basados en Windows.

A diferencia de la arquitectura tradicional de cliente y servidor, en un entorno de Servicios de Terminal con Windows 2000 Server todo el procesamiento de la aplicación ocurre en el servidor. El cliente de Servicios de Terminal no realiza procesamiento local de la aplicación. La tecnología de Servicios de Terminal sólo muestra la salida de la aplicación, la interfaz gráfica con el usuario (GUI) en el cliente. Cada usuario conectado al servidor percibe sólo su sesión, la cual es administrada en forma transparente para el usuario por el sistema operativo del servidor y es independiente de otras sesiones de cliente que haya en el servidor simultáneamente.

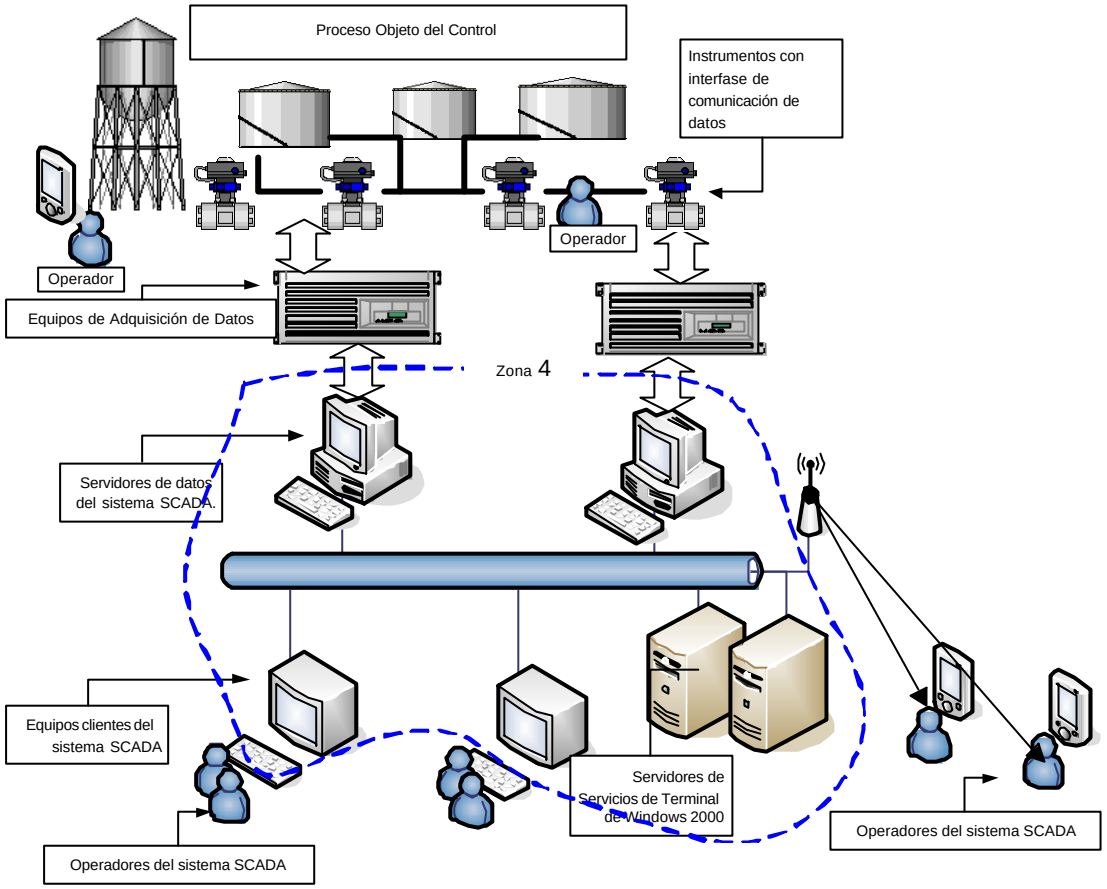
Desde el punto de vista del desarrollo de aplicaciones, una de las mayores ventajas de los Servicios de Terminal es que los desarrollos basados en Windows-32 y Windows-16 pueden correr sin mayores modificaciones.

Sin embargo esto no significa que todas las aplicaciones existentes correrán igualmente bien bajo un entorno de Servicios de Terminal. El desarrollo de aplicaciones que estén diseñadas y certificadas para

correr en un entorno de Servicios de Terminal podrán aprovechar las bondades de éste entorno de mejor manera que una aplicación que no haya sido desarrollada considerando el ambiente operativo.

De igual manera, una aplicación que acompañe la evolución de la tecnología de software podrá aprovechar las mejoras ofrecidas en sucesivas versiones.

La herramienta de desarrollo de aplicaciones SCADA seleccionada para la implementación fue desarrollada para correr en entornos de Servicios de Terminal y está certificada para tal propósito, dando así respaldo técnico a ésta en su conjunto mientras se mantiene un alto grado de cumplimiento de los requerimientos de certificación de Microsoft.



Los siguientes puntos exhiben la importancia de emplear una aplicación que haya sido desarrollada contemplando la existencia de los Servicios de Terminal, de manera de poder aprovechar los recursos disponibles.

Consideraciones para las aplicaciones

Las siguientes consideraciones deben ser observadas al momento de ejecutar una aplicación en un entorno de Servicios de Terminal. Si en el desarrollo de la aplicación no se observan los siguientes detalles de diseño, puede suceder que la aplicación en su conjunto termine en un fracaso.

La correcta selección de las aplicaciones y, si es posible, la configuración de sus parámetros para entorno de Terminal Server, resultan cruciales para el éxito de la implementación. Observar estas recomendaciones puede incluso servir de ayuda al momento de evaluar el desempeño de la aplicación.

Los Servicios de Terminal y las capacidades multiusuario

La tecnología de Servicios de Terminal va más lejos que la arquitectura tradicional de cliente y servidor. La arquitectura de los Servicios de Terminal permite a los usuarios y aplicaciones compartir recursos de hardware y software comúnmente encontrados sólo en servidores Windows 2000.

Estos recursos compartidos incluyen el uso de una CPU central, la memoria y sus medios de almacenamiento así como también los recursos del sistema operativo como la estructura de registro, las estructuras de datos y las aplicaciones instaladas en el servidor.

Estructuras centralizadas vs Servicios de Terminal de Windows 2000

En alguna forma los Servicios de Terminal son análogos a las antiguas estructuras centralizadas tipo Mainframes. En la arquitectura centralizada las terminales simples proveían un conducto orientado a caracteres entre el usuario y el servidor. Los usuarios acceden al servidor, ejecutan programas, leen y escriben en archivos compartidos, direccional las salidas a impresoras compartidas y acceden a bases de datos compartidas. Es más, cada terminal funciona independientemente de otras sesiones de terminal gracias a la arbitración entre los recursos compartidos que realiza el sistema operativo.

Los Servicios de Terminal difieren en ciertos aspectos con la estructura centralizada. La principal diferencia es la naturaleza gráfica del entorno del sistema operativo Windows 2000. Los entornos de servidores centrales fueron tradicionalmente orientados a caracteres, requiriendo sólo un tráfico muy pequeño en las líneas de comunicaciones entre el servidor y las terminales o los emuladores de terminales.

Con los Servicios de Terminal toda la salida gráfica de la pantalla y lo referido a entra y salida debe fluir entre el escritorio del cliente y el servidor de Windows 2000 ejecutando los Servicios de Terminal. Esto implica que grandes volúmenes de información deben viajar sobre la red hacia el dispositivo cliente.

Afortunadamente el protocolo gráfico que opera entre el cliente de Servicios de Terminal y el servidor optimiza esta transmisión y es completamente transparente al desarrollador de la aplicación.

Consideraciones en el diseño de la aplicación

Otro diferencia importante entre la arquitectura centralizada y los Servicios de Terminal es como las aplicaciones que corren en estos entornos deben ser diseñadas.

En un entorno de servidor centralizado las aplicaciones deben ser desarrolladas específicamente para correr en ese entorno particular. Con los Servicios de Terminal cualquier aplicación desarrollada para cualquier entorno Windows debería funcionar sin tener que ser específicamente desarrollada para el entorno de Servicios de Terminal. Las aplicaciones que corren en Windows 2000 Server y Windows NT 4.0 Server deberían correr sin modificaciones cuando se habilitan los Servicios de Terminal.

Esto es importante cuando se considere las implicaciones de múltiples usuarios compartiendo un sistema basado en Windows 2000 simultáneamente. En lugar de tener diferentes usuarios corriendo aplicaciones usando sus propios recursos de hardware y software, los usuarios de Servicios de Terminal comparten el hardware y el software disponible en el servidor. Por ejemplo, si dos usuarios corren las misma aplicación en un entorno de Sercitos de Terminal, dos copias de dicha aplicación son iniciadas en el mismo sistema pero cada una operando bajo contextos de usuario distintos. Todo esto es manejado en forma transparente por los Servicios de Terminal dentro del sistema operativo.

Múltiples usuarios accediendo el mismo grupo de aplicaciones en un sistema común pueden crear situaciones de competencia como las que se detallan a continuación:

Competencia por el tiempo de CPU

En un entorno de Servicios de Terminal cada usuario tiene su propio escritorio que puede ejecutar cualquier aplicación que disponible para ese escritorio. Sin embargo, todas las aplicaciones ejecutadas por todos los usuarios están compitiendo por los recursos de la CPU central disponible en el servidor. Si algún usuario ejecuta un aplicación diseñada pobremente que requiera un uso intensivo de la aplicación, los otros usuario en ese servidor experimentarán una baja en el desempeño del sistema.

Competencia por el acceso a disco

Este escenario es análogo a la forma de acceso a disco en entornos cliente y servidor usando conexiones de red. En el entorno de Servicios de Terminal la demanda de entrada y salida a disco sin más intensas ya que los usuarios no solo compiten por el acceso a las aplicaciones y sus archivos relacionados, sino también por el acceso a los archivos del sistema operativo. Por ejemplo, múltiples usuarios pueden estar haciendo diferentes llamadas a una librería dinámica (DLL) al mismo tiempo o intercambiando datos entre las áreas de memoria virtual y real. El recurso de disco único representa una estructura de único disco. Usar áreas comunes en lugar de carpetas específicas de usuario puede resultar en competencia o colisión.

Competencia por RAM

Cada usuario tiene una sesión independiente, la cual pueden llenar con las aplicaciones de acceso intensivo a memoria que necesiten. Algunos usuarios intentar abrir en sus escritorios tantas aplicaciones como les sea posible, mientras que otros toman una postura mas conservativa y ejecutan sólo las aplicaciones que necesitan. De todas formas, las necesidades de todos los usuarios son satisfechas desde el mismo recurso de memoria del servidor.

Competencia por el acceso a la red

En un entorno de procesamiento distribuido la red provee la tubería de comunicaciones entre los escritorios y los servidores. En un entorno de Servicios de Terminal la necesidad por acceso a la red es más crítica que en un entorno tradicional distribuido de cliente y servidor, ya que todo el tráfico de actividad del escritorio fluye sobre la red entre los clientes y el servidor. Sin una conexión de red al servidor un cliente de Servicios de Terminal ni puede operar. La conexión de red es usada para comunicar cada cliente mientras se sirve a las necesidades de red de las aplicaciones y servicios.

Competencia por acceso a recursos globales de Windows 2000

En el entorno de Servicios de Terminal, los usuario no ejecutan copias individuales de Windows 2000 Pro, algunos componentes clave del sistema operativo y componentes de aplicación son clonados, pero los restantes son compartidos entre los usuarios. Entonces los usuarios pueden estar compitiendo por el acceso al registro de Windows, el archivo de paginación, los servicios del sistema y otros recursos y objetos globales.Diseño de redes inalámbricas

Diseño de redes inalámbricas

Introducción

El diseño de redes inalámbricas involucra tanto la cuidadosa selección de los dispositivos móviles que formarán parte de ésta, como así también de la tecnología disponible en el momento de la selección.

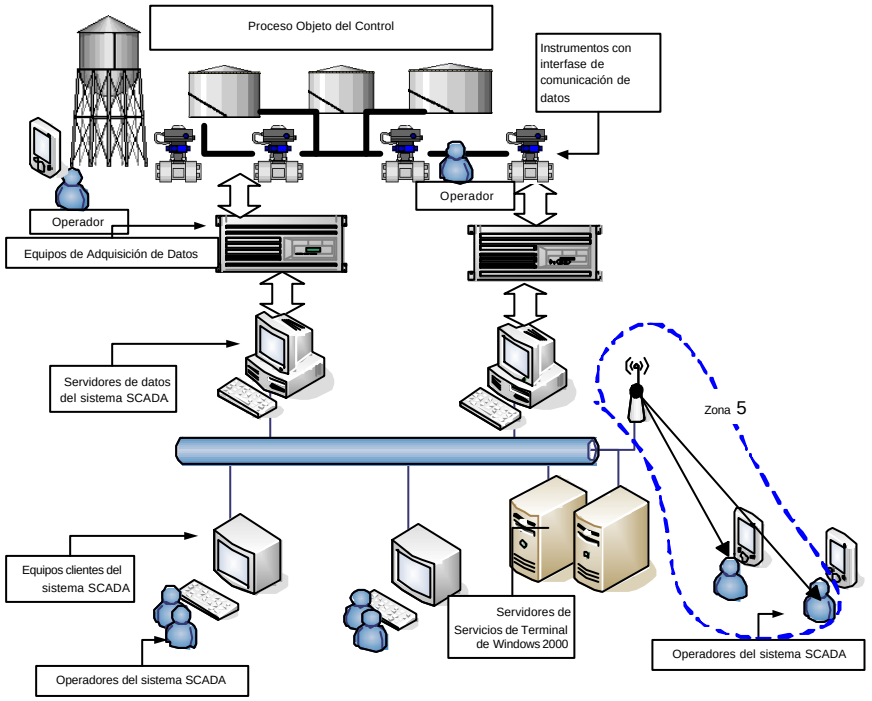
La variada oferta de equipos de mercado hace necesaria una preselección de opciones que cubran las necesidades básicas de la aplicación que se le dará a la red. Un estudio más detallado posterior descartara aquellos que no satisfacen las necesidades puntuales que cada puesto de trabajo exija.

Para el desarrollo de una aplicación SCADA que incluya dispositivos móviles, el camino es el mismo. Se debe seleccionar los componentes básicos que darán un marco de acción a la aplicación, junto con una tecnología de red inalámbrica que acompañe las necesidades planteadas. Sin por esto descartar la posibilidad de dejar abierta la alternativa de ampliación en un futuro cercano.

Así la selección de componentes básicos, junto a una preselección de tecnología, presentará un marco de acción convenientemente sólido que luego podrá ser usado como referencia en el estudio correspondiente a las necesidades puntuales.

Sin dejar de lado las opciones de seguridad referente a la encriptación que ofrece la tecnología de software de hoy, existen medidas de seguridad de aplicación inmediata que darán seguridad al marco de acción inicial al momento de diseñar la aplicación SCADA.

En la solución propuesta la red inalámbrica es la que permite el vinculo de los dispositivos móviles con la red del sistema SCADA.



Componentes básicos para el armado de una red inalámbrica

Una red inalámbrica está formada por componentes de hardware y software que interactúan para lograr la conectividad buscada entre los distintos equipos. Para esto, la selección de los componentes y la forma de interrelación de los mismo, no resulta un tema trivial.

Al igual que las redes cableadas, existen dispositivos adaptadores de red para cada tipo de equipos. Sólo que el concepto de movilidad de equipos, trae aparejados sus propios factores determinantes al momento de la selección.

Componentes de hardware

Los siguientes componentes de hardware pueden emplearse para armar una red inalámbrica básica:

Punto de Acceso:

El dispositivo denominado Punto de Acceso o AP, por sus siglas de Inglés de Access Point, permite que los equipos móviles equipados con tecnología inalámbrica se comuniquen con una red cableada existente a la cual éste está físicamente conectado.

También se los suele emplear para expandir el rango de cobertura de una red inalámbrica determinada, equipada con estos dispositivos.

Típicamente éste tipo de dispositivos cuentan con uno o más conectores Ethernet del tipo RJ-45, de manera de poder conectarlos a un red cableada Ethernet existente. Es posible también emplearlos como concentradores para varios equipos PC con placas Ethernet para armar así una pequeña red.

Desde el punto de vista de la conectividad inalámbrica el equipo cuenta con una antena omni direccional por la cual envía y transmite las ondas de radio correspondiente a la tecnología inalámbrica seleccionada.

Alternativamente los dispositivos contemplan la posibilidad de intercambiar estas antenas de manera tal de poder adaptarse a la geografía donde deban actuar o modificar al rango de cobertura del AP. Las alternativas suelen estar orientadas a colocar antenas externas o antenas de mayor ganancia.

Respecto a la alimentación necesaria, los AP diseñados para entornos de oficina o redes hogareñas suelen ser relativamente pequeños y necesitan de una fuente de alimentación externa provista por el fabricante. Los AP diseñados para redes más grandes suelen presentarse en formato industrial estándar de 19 unidades y su alimentación se toma directamente de la línea de 110 o 220 V correspondiente.

Punto de Acceso de Linksys

Adaptador inalámbrico para equipos PC portátiles

Este tipo de adaptadores está diseñado para permitir que un equipo PC portátil (Notebook) pueda unirse y participar de una red inalámbrica.

Si bien muchos equipos Notebooks incluyen hoy en día esta opción como una prestación incluida por el fabricante, los adaptadores inalámbricos para Notebooks están diseñados para conectarse a éste a través de la ranura de expansión del tipo PC CARD (PC-MCIA).

El adaptador se introduce dentro de la ranura de expansión del Notebook , de donde toma su alimentación, y pasa a formar parte de los periféricos del equipo PC. Lal tecnología Plug & Play de hoy día facilita la integración de estos nuevos dispositivos, haciendo que sea transparente para el usuaria la instalación de los controladores necesarios para el nuevo dispositivo.

En el extremo exterior del dispositivo adaptador se encuentra la antena de transmisión y recepción. La forma de éste varía según el adaptador y la tecnología inalámbrica seleccionada, pero generalmente se trata de antenas omni direccionales de dimensiones pequeñas.

Dependiendo del adaptador seleccionado, es posible que éstos contemplen también la posibilidad de remover o cambiar la antena provista, de manera de poder adaptarse a las exigencias móviles, tanto sea para el uso de una antena externa como para utilizar una antena de mayor ganancia.

Adaptador inalámbrico PC-Card para Notebooks de Linksys

Adaptador inalámbrico para equipos de mano

Los equipos de mano, del tipo Palm, iPaq o algunos más específicos, (conocidos como Palm PC o HandHelds), también incorporan un estándar de expansión para incluir nuevos periféricos al sistema.

A tales fines existen dispositivos adaptadores para redes inalámbricas que utilizan el estándar CF (Compact Flash) para conectarse a los dispositivos de mano. Así un equipo de mano que no tenga tecnología inalámbrica como una opción de fábrica, puede expandir su abanico de posibilidades y participar de una red inalámbrica.

Típicamente el adaptador se inserta en la ranura correspondiente del equipo de mano y, dependiendo del sistema operativo de este último, se instalarán o no los controladores correspondientes.

La alimentación se toma del propio dispositivo de mano, con lo cual se ve afectado el tiempo de duración de las baterías del mismo.

Alternativamente suelen ofrecer la posibilidad de intercambiar antenas de manera de poder ampliar el rango de cobertura a medida que se adapta a la portabilidad del mismo.

Adaptador inalámbrico CF para equipos de mano de Linksys

Adaptador inalámbrico para puertos USB

Para cubrir las alternativas de conectividad con periféricos que hoy en día ofrecen los quipos PC de escritorio y los equipos PC portátiles (Notebooks), existe la alternativa de conectar a un puerto USB disponible en el equipo PC un adaptador inalámbrico para puerto USB.

Éste tipo de adaptadores se instala generalmente en forma automática en el sistema operativo y permite que el equipo puede unirse a una red inalámbrica.

Típicamente presentan un conector USB para la conexión al puerto del equipo PC correspondiente, una entrada de alimentación externa, y una antena para transmisión y recepción de las ondas de radio correspondiente al estándar inalámbrico seleccionado.

Adaptador inalámbrico para puerto USB de Linksys

Dispositivos móviles

Los dispositivos móviles disponibles en el mercado de hoy satisfacen la mayoría de las necesidades de los usuarios actuales, tanto se trate de la necesidad de un dispositivo tipo PC portátil con conectividad inalámbrica, como de dispositivos altamente especializados.

La oferta abarca los dispositivos de mano mayormente aceptados por los usuarios de oficina, como aquellos que requieran el cumplimiento de algún estándar de normas industriales de seguridad.

Así podemos citar el caso de los equipos portátiles de la línea HP-Compaq, Sony o Palm, los cuales ampliamente satisfacen las necesidades de movilidad de usuarios de oficina. Estos equipos presentan distintas prestaciones basadas, mayormente, en el sistema operativo que incluyen como base.

Dispositivos de oficina mayormente usados

Para el caso de las aplicaciones industriales la oferta es considerablemente más amplia. Directamente relacionado con el tipo de aplicación para el cual serán empleados y el ambiente en el que deben desenvolverse, las alternativas van desde dispositivos sin teclados hasta teclados completos, pasando por teclas programables para funciones especiales definidas por la aplicación, hasta la inclusión de lectores ópticos de códigos de barras para el ingreso de datos.

El ambiente de trabajo influye notablemente en la selección del equipo móvil. La propuesta contempla la necesidad de equipos resistentes a determinadas vibraciones o golpes hasta amplios rangos de temperatura o presión, incluyendo condiciones de extrema humedad o ambientes corrosivos.

A tales fines podemos citar los equipos de la firma Symbol, la cual ofrece amplias soluciones para las necesidades planteadas anteriormente.

Dispositivos Symbol de mano para diversas aplicaciones

Componentes de software

El componente de software que interviene en el diseño de una red inalámbrica puede ser analizado desde dos puntos de vista. Uno de ellos relacionado con el software propio de cada adaptador o componente de la red, y el otro relacionado con el dispositivo que se desea conectar a la red inalámbrica.

Desde el punto de vista del dispositivo, solo basta un software que actúe como controlador del adaptador correspondiente, y contemple o maneje todas las opciones que éste puede presentar relacionadas con la tecnología inalámbrica seleccionada.

Prácticamente estas opciones están íntimamente relacionadas con el sistema operativo base del dispositivo en cuestión. Por tal motivo en la selección del dispositivo debe agregarse a la ecuación de elección, el software de base en relación con el adaptador para redes inalámbricas que el dispositivo pueda aceptar.

Desde el punto de vista de los adaptadores, es necesario seleccionar los estándares de comunicaciones que emplearan estos dispositivos para poder así asegurar la compatibilidad de éstos y su correcta integra-

ción a la red. Así mismo, existen factores de compatibilidad que deben ser tenidos en cuenta en el momento de agregar nuevos equipos a una red, o reemplazar alguno ya existente.

La selección del estándar adecuado permite entonces delinear el camino a seguir en el momento de la adquisición, reemplazo o expansión de componentes de la red.

Selección del estándar inalámbrico adecuado

Luego de tomada la decisión de armar una red inalámbrica para expandir la solución a los equipos móviles, el próximo paso es seleccionar el estándar de tecnología inalámbrica correcto, basado en el análisis de las necesidades y las opciones de mercado.

Básicamente, un estándar es un conjunto de especificaciones para un dispositivo determinado. Todos los dispositivos que siguen un determinado estándar comparten características operativas, como la frecuencia de radio empleada y la máxima velocidad de transferencia empleada, ente otros.

Para la construcción de redes inalámbricas existen tres estándares disponibles en productos de mercado para seleccionar. Estos son:

- IEEE 802.11 a.
- IEEE 802.11 b.
- IEEE 802.11 g.

Características sobresalientes de IEEE 802.11 b.

El estándar IEEE 802.11b es el que ha ganado más popularidad hasta el momento. Aunque el IEEE 802.11 g pareciera ser próximamente tanto o más popular que IEEE 802.11 b, el tiempo que lleva éste último en el mercado hace que ya sea empleado en varios equipos como una opción de fábrica.

La gran cantidad de productos que incorporan este estándar, junto a la importante oferta de dispositivos periféricos que permiten adaptar equipos PC y portátiles a IEEE 802.11b hace que el precio de estos dispositivos sea bajo. Por este motivo se denomina a éste estándar como el más económico.

De los tres estándares propuestos, éste es el de menor velocidad. Llega a 11 Mbps. Lo cual suena más que importante si tenemos en cuenta que los servicios de cable modem promedian típicamente entre los 4 y 5 Mbps.

La frecuencia central que utiliza se sitúa en 2.4 GHz con lo que debe compartir la frecuencia con algunos electrodomésticos de uso masivo, como teléfonos inalámbricos y hornos de micro ondas, con las consiguientes interferencias.

El rango de cobertura que ofrece depende directamente con la geografía del lugar de acción, como ser materiales de construcción, muros, mobiliarios y otros. Suele estar en un rango operativo entre 30 y 45 metros (100 a 150 ft).

La demanda por el acceso a Internet en lugares públicos genero la proliferación de sitios con puntos de acceso, como ser bares, centros de compras y aeropuertos, que eligieron a éste estándar como la opción más conveniente para adaptarse al creciente interés del público en general. Se espera que en el corto plazo se actualicen a un estándar más rápido.

Características sobresalientes de IEEE 802.11 a.

Éste estándar de nueva tecnología no goza de tanta popularidad como IEEE 802.11 b. Existen pocos dispositivos que incorporan a éste estándar como opción de fábrica, como así tampoco existen periféricos de uso masivo que permitan su implementación.

Principalmente por tal motivo los productos para implementar éste estándar son relativamente más caros comparados con los periféricos necesarios para implementar una red con IEEE 802.11 b.

Ofrece una velocidad de transferencia de datos cinco veces mayor que IEEE 802.11 b, llegando a los 54 Mbps. Pero tiene un rango de alcance mas limitado que IEEE 802.11 b. Típicamente responde al rango entre los 7.5 y 22 metros (25 a 75 ft) en ambientes interiores.

Trabajando en la frecuencia de los 5 GHz goza de los privilegios de una banda que, por el momento, no es empleada masivamente por dispositivos domésticos y de oficina, con lo cual puede coexistir con redes y dispositivos que trabajen en la banda de los 2.4 GHz sin interferencias.

Por el momento no existen lugares de acceso público que implementen éste estándar como servicio de red inalámbrica.

Características sobresalientes de IEEE 802.11 g.

Es un estándar de nueva tecnología que esta ganando mucha aceptación y proyecta un gran crecimiento en el corto plazo. Si bien hay pocos dispositivos que incorporan éste estándar como opción de fábrica, comparado con la oferta de equipos con IEEE 802.11 b, existen numerosos dispositivos externos y adaptadores que permiten vincular equipos a una red inalámbrica con éste estándar.

Los productos son relativamente baratos, comparados con las prestaciones. Pero se espera una mejora en los precios en el corto plazo.

Ofrece una velocidad de transferencia de datos cinco veces mayor que IEEE 802.11 b, llegando a los 54 Mbps, con un muy buen rango de cobertura. Típicamente se trabaja en el rango entre 30 y 45 metros (100 a 150 ft) en ambientes interiores, dependiendo de los mobiliarios y los materiales de construcción de muros.

Opera en la banda de los 2.4 Ghz, por lo que sufre de las posibles interferencias de los electrodomésticos que ocupen dicha banda. Como ser teléfonos inalámbricos, hornos de micro ondas, etc.

Existe una compatibilidad entre IEEE 802.11 g y IEEE 802.11 b, con lo que el acceso en lugares públicos es posible también con dispositivos que incluyen éste estándar.

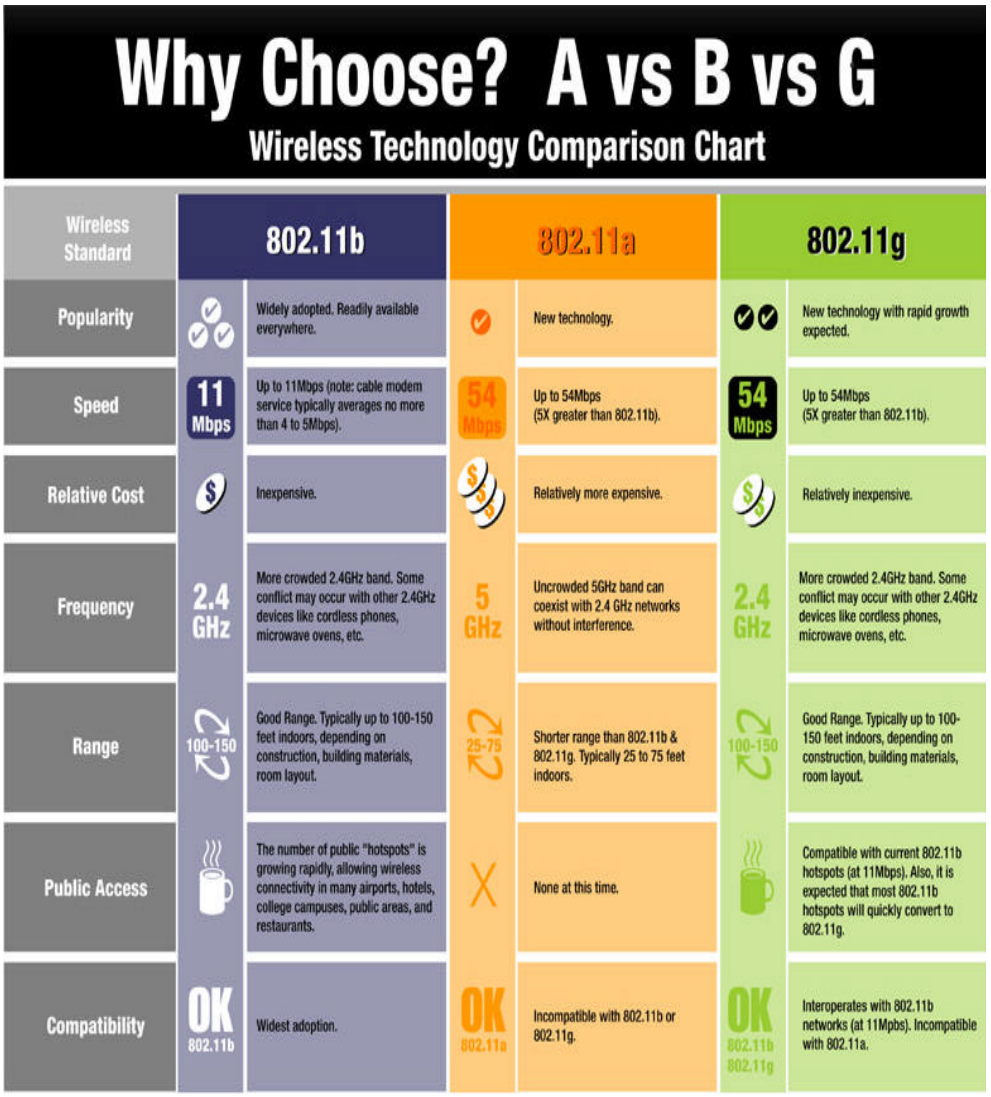
En realidad la compatibilidad se logra disminuyendo la velocidad de transferencia a 11 Mbps para que coincida con la de IEEE 802.11 b. Normalmente operando a 54 Mbps, lo que algunos fabricantes llaman «Modo Turbo», las tarjetas adaptadoras tiene opción manual o automática para cambiar de velocidad.

Sin embargo, desde el punto de vista de un ruteador o punto de acceso que administre una red inalámbrica con IEEE 802.11 g compatible con IEEE 802.11 b, puede suceder que la conexión de un equipo IEEE 802.11 b a 11 Mbps haga que toda la red pase de funcionar de los 54 Mbps de IEEE 802.11g a los 11 Mbps que requiere el estándar anterior, llevando en consecuencia al bajo rendimiento y desempeño de toda la red.

Por tal motivo es recomendable, siempre que sea posible, la re-configuración del ruteador o punto de acceso para que sólo acepte conexiones de equipos con IEEE 802.11 g.

Tabla de comparativa

El siguiente gráfico esquematiza las diferencias expuestas más arriba entre los estándares más difundidos para la implementación de redes inalámbricas.



Esquema comparativo entre IEEE 802.11 a/b/g.

Medidas de seguridad básicas en redes inalámbricas

Una red inalámbrica es, en muchos casos, una extensión de la red cableada existente en un área determinada. Por tal motivo, existen factores de seguridad que deben ser tenidos en cuenta.

La libertad que brinda la posibilidad de no depender de cables hace que armar una red inalámbrica sea fácil de implementar y conveniente de usar. Pero aún así, una red inalámbrica tiene un riesgo inherente, ya que ésta envía su información mediante ondas de radio. Al igual que las señales de un teléfono o equipo de radio, éstas también pueden ser interceptadas.

La tecnología de hoy en día provee una serie de opciones que pueden complementarse para mejorar la seguridad de las redes inalámbricas. Así mismo la industria de redes sin cables esta trabajando en el desarrollo de medidas de seguridad más fuertes, las cuales estarán disponibles en el futuro inmediato.

En términos generales las siguientes recomendaciones deberían ser aplicadas como medidas esenciales para restringir el acceso a una red inalámbrica:

- Cambiar el nombre por defecto de la red (SSID).
- Deshabilitar la opción de transmisión pública (broadcast) del SSID.
- Cambiar la clave de acceso por defecto de los dispositivos inalámbricos.
- Habilitar el filtro de direcciones MAC.

Con la tecnología actual de redes inalámbricas es necesario observar las opciones y seleccionar las mejores prácticas que apliquen a cada implementación. La combinación de simples medidas de seguridad con las opciones de encriptación disponibles para el acceso protegido a redes inalámbricas (WPA - Wi-Fi Protected Access) permiten armar una red que brinde seguridad, tanto desde el punto de vista del acceso y disponibilidad de ésta, como también de confiabilidad de la información que circula por la misma.

Cambio del nombre por defecto de la red (SSID)

Los dispositivos inalámbricos para armar redes tienen un SSID (Service Set Identifier) asignado por defecto por su fabricante. El SSID es, desde el punto de vista práctico, el nombre de la red inalámbrica que un determinado dispositivo administra, como por ejemplo un Punto de Acceso. Este nombre puede ser, prácticamente, cualquier cadena de caracteres que se desee.

Debido a que los nombres por defecto son ampliamente conocidos, éstos pueden ser empleados por personas maliciosas que intenten conectarse a una red determinada. Al cambiar el SSID a algo relativamente único y que no identifique la red o los productos que se utilizan para armarla, dificulta notablemente las posibilidad de conexión por personas extrañas a la red.

Como medida extra de precaución, se debería cambiar periódicamente el SSID de una red. De manera tal que si una persona no autorizada logró conectarse a la red en el pasado, deba buscar nuevamente el identificador de la red.

Deshabilitar la transmisión pública del SSID

Muchos dispositivos para el armado de redes inalámbricas vienen configurados de fábrica para publicar abiertamente (Broadcast) su identificador de servicio. Esto facilita que los dispositivos móviles pueden fácilmente conectarse a la red. Pero de igual manera pueden hacerlo personas con intenciones distintas al fin propio de la red.

Como regla general, si la red no esta destinada a ofrecer servicios de conectividad al público en general, no debería publicar su identificador de servicio.

Cambiar la clave de acceso a los dispositivos inalámbricos

Los dispositivos destinados a armar y administrar una red inalámbrica, como Puntos de Acceso (AP - Access Point) y ruteadores, solicitan una clave de acceso para acceder a modificar su configuración. Estos dispositivos traen una clave de acceso por defecto impuesta por el fabricante.

Estas claves de acceso por defecto son públicamente conocidas y pueden ser usadas por personas maliciosas para acceder al dispositivo y cambiar la configuración de red a su conveniencia.

Para evitar este tipo de ataques es recomendable cambiar la clave de acceso de forma tal que sea difícil de adivinar.

Habilitar el filtro de direcciones MAC

Dependiendo de las opciones que cada dispositivo de Punto de Acceso o ruteador ofrece, debería habilitarse el filtro de direcciones MAC (Media Access Control). La dirección MAC es una serie única de números y letras asignado a cada dispositivo de red.

Con la opción de filtro de direcciones MAC habilitada, el acceso a la red inalámbrica es permitido solamente a equipos con las direcciones MAC especificadas. Esto dificulta a los intrusos acceder a la red

empleando una dirección MAC cualquiera.

Uso de dispositivos móviles

Mejoras en los negocios tras la implementación de dispositivos móviles

Introducción

La proliferación de equipos portátiles, tanto para el usuario de oficina como para la industria, responde a la necesidad de acceso a la información independientemente del lugar geográfico en donde se encuentre el usuario.

Cada actividad humana relacionada a la industria y el comercio tiene características propias que determinan sus necesidades y fortalezas. Por otro lado, la observación de sus debilidades permite mejorar su funcionamiento y en consiguiente el resultado final.

A modo de ejemplo, los siguientes casos de uso explayan las oportunidades de mejora que pueden cubrirse mediante la implementación de dispositivos móviles al sistema actual de cada actividad.

Mejoras en el negocio de los servicios a clientes en campo

Los servicios en campo son de valor fundamental para las empresas de servicios que ofrecen a sus clientes asistencia técnica en sitio. Esta interacción presenta una excelente oportunidad de mantener y crear un relación duradera con los clientes.

Las herramientas inalámbricas para servicios de campos pueden transformar a los trabajadores de móviles de pasivos participantes del servicio a activos integrantes del negocio que interactúan con el sistema. Cuando los técnicos de campo tienen acceso a información crítica en el punto de actividad la organización y el cliente visualizan inmediatamente los beneficios. Estos beneficios incluyen: respuesta más rápida, tiempos de reparación más cortos, mejor manejo de inventarios, facturación rápida y precisa y otros beneficios que suman a mejorar la satisfacción del cliente.

Mejoras en el funcionamiento

Existen tres aspectos fundamentales en la implementación de un sistema de servicios de campo exitoso: los dispositivos móviles de computación, el software de aplicación y la infraestructura de comunicaciones. Los técnicos de campo utilizan aplicaciones específicas de la industria corriendo en resistentes dispositivos de computación de mano. La estructura central de comunicaciones es típicamente una combinación de redes inalámbricas amplias (WWAN) y redes inalámbricas locales (WLAN) que permiten la transmisión de datos entre el personal de servicio de campo y los sistemas en la oficina central. Estas tecnologías se combinan para reemplazar el manejo ineficiente de papel y los procesos de comunicación.

Históricamente los servicios de campo fueron procedimientos de manejo intensivo de papeles con sus considerables costos asociados, pérdidas de tiempo e ineficiencias. La tecnología móvil de hoy en día ofrece ayuda para rediseñar el proceso para acercarse a un flujo significativo de información digital, servicios y partes.

El primer paso en el proceso de servicios de campo es generalmente la transmisión de las ordenes de trabajo a los técnicos que se encuentran fuera de la oficina central. Las computadoras de mano con servicios inalámbricos permiten la transferencia automática en tiempo real de órdenes de trabajo o el reenvío al empleado más cercano al sitio necesario según el último trabajo conocido. El uso de computadoras móviles junto con programas de aplicación específica permite a los planificadores de trabajos de servicios de campo conocer, en cualquier momento, el paradero y el estado de cada técnico de campo.

Una de las ventajas claves de los sistemas de tiempo real es la habilidad de acotar los tiempos de llegada de la información facilitando la programación precisa de las tareas y un método certero para mejorar las estadísticas de satisfacción del cliente.

Mejoras en el servicio al cliente

Cuando los técnicos de campo tiene información crítica para el cliente «en la punta de los dedos» pueden responder inmediatamente a las necesidades del cliente y generar así oportunidades de venta, como extensiones de servicios de garantía en sitio o paquetes complementarios de servicios acorde a los registros del cliente, a la vez que acceden a la historia de trabajos previa del cliente para mejorar el proceso de localización de fallas, tienen la habilidad de ordenar partes directamente desde el lugar del cliente, imprimir recibos de trabajo y facturas de servicio, como también la transmisión inmediata del cierre de la orden de trabajo y sus facturas asociadas.

Eficiencia en el proceso

Cuando la información fluye ida y vuelta desde un trabajador de servicios remoto y la oficina central en tiempo real, la organización obtiene considerables beneficios como ser: menor cantidad de trabajo de papel, seguimiento de partes y materiales en tiempo real para mejora el manejo de los inventarios y obtener los resultados de vuelta del trabajo realizado momentos después de que éste fue terminado.

La precisión de la información permite a los supervisores analizar pedidos individuales de servicio, planificar en forma efectiva las operaciones del plantel de trabajo e identificar patrones repetitivos de fallas.

Mejora en los sistemas de control de inventarios en tiempo real

Los sistemas de Planeamiento de Recursos Empresariales (ERP, Enterprice Resource Planning) se han movido más allá de las líneas de ensamblado hacia cada rincón de la cadena de provisión. Obtener la información más reciente ayuda a los tomadores de decisiones a reaccionar tranquilamente cuando la demanda apremia, proporcionando esfuerzos en forma eficiente, controlando los costos, entregando la cantidad justa de bienes en el tiempo justo y estar un paso al frente de sus competidores.

Las soluciones de sistemas basadas en el «punto de actividad» capturan datos en tiempo real justo donde la actividad ocurre y los combinan la información de los ERP para administrar los inventarios unos minutos después.

Combinando los servicios de redes inalámbricas con dispositivos de captura de datos y el software adecuado se logran implementaciones que mejoran notablemente el planeamiento de los recursos empresariales.

Esta implementación permite capturar y transmitir datos en el instante en que cambian, eliminando los errores propios del manejo de códigos de producto, mejorando así la eficiencia en los controles.

La implementación de «puntos de actividad» involucra la combinación de dispositivos recolectores de datos mediante códigos de barras con redes inalámbricas alrededor de puntos de acceso usualmente utilizando el estándar IEEE 802.11b .

Mejora en las prestaciones relacionadas a la salud

El acceso a la información de más reciente de los pacientes facilita el trabajo de los especialistas. Obtener historias clínicas, tratamientos previos, medicaciones aplicadas, pruebas y resultados de los laboratorios, información de coberturas y demás permiten mejorar la toma de decisiones.

Con la implementación de soluciones móviles y redes inalámbricas los profesionales de la salud pueden disponer de toda la información al alcance de su mano.

Ya se trate de una atención en la cama de un paciente en un hospital o una visita domiciliaria, la información necesaria podría ser accedida en segundos. De igual manera los agregados del profesional serían incluidos instantáneamente a la historia clínica del paciente.

En lugar de recaer en escrituras en papel, las enfermeras actualizan la información del paciente, verifican la disponibilidad de drogas o las órdenes de tratamiento al lado de la cama del paciente con un dispositivo de mano sin necesidad de tener que volver a la guardia de enfermería para reportar las novedades.

La posibilidad de poder consultar los antecedentes del paciente junto con información de casos similares almacenados en bases de datos permitiría a los profesionales un mejor diagnóstico y mejor aplicación de los procedimientos.

Soluciones aplicables al negocio del transporte

Para permanecer competitivo es necesario relegar en la tecnología el manejo de las complejidades de la cadena de provisión. El uso efectivo de la tecnología mejora los márgenes de ganancias y ayuda a alcanzar o superar las expectativas de los clientes. Es posible alcanzar estos objetivos a través del manejo eficiente de las operaciones de transporte y sincronización con las operaciones interdependientes.

Las soluciones móviles para el transporte proveen una herramienta estratégica necesaria para alcanzar la mejora del desempeño y la reducción de costos. Con el uso de estos sistemas es posible colectar y diseminar información detallada acerca de una flota de reparto y sus actividades de entrega en tiempo real. Proporciona mayor control sobre la productividad de los recursos de transporte y mejora la visibilidad de los envíos, permitiendo así mejorar la administración de los inventarios y la confiabilidad del servicio.

Con el empleo de soluciones móviles en el transporte se reduce el mantenimiento de la flota, se bajan los tiempos de entrega, los costos e impuestos a los usuarios, trabajo en papel y su desperdicio. Mientras que se elimina los errores de carga de datos, errores en la entrega, esfuerzos duplicados, y pasos intermedios que no agreguen ningún valor. Al mismo tiempo se mejora la flexibilidad, la precisión, la calidad del servicio, la visibilidad de los inventarios, el seguimiento y la optimización de la carga de datos.

Antes de que la flota salga de la terminal los despachantes usan el planeamiento automático de rutas para identificar las rutas más eficientes, mientras que los sistemas a bordo del camión colectan información valiosa a medida que se viaja por esa ruta. De esta manera se mejoran los costos de envío haciendo más competitivo el negocio.

A su vez, ahorra tiempo en la forma de recibir pedidos de trabajo, ya que en el mismo momento que se realiza una entrega puede recogerse una nueva solicitud de entrega y el sistema se actualiza instantáneamente planificando las tareas de entregas para el día siguiente. Así mismo, nuevas solicitudes para el retiro de paquetes son enviadas al repartidor que se encuentre más cerca del punto de entrega del nuevo remitente.

Los dispositivos móviles pueden también imprimir generando así, recibos de confirmación para los clientes en el punto de entrega. Instantáneamente envía un mensaje de datos indicando la completitud del envió. Si se tratara de recoger una nueva solicitud de envío, la impresión serviría como un comprobante recibo de un nuevo paquete.

Selección del dispositivo adecuado

La gran variedad de oportunidades que brinda el negocio de los dispositivos operativos móviles se ve acompañada por una oferta igual de dispositivos de mano. La industria de las computadoras de mano acompaña el crecimiento constante de necesidades con una opción para cada tipo de uso.

A modo de ejemplo, los siguientes productos de la firma Symbol demuestran la diversidad de equipos existentes que satisfacen las más variadas exigencias.

Equipos para ingreso y captura de datos

Estos equipos están diseñados para capturar datos en puntos de operación. El dispositivo incluye un lector de códigos de barra y un teclado multifunción para completar las opciones de ingreso de datos más variados.

Equipos de operación y visualización

Estos equipos están diseñados para ser operados mayormente por la pantalla sensible al tacto incorporada, aunque es posible agregar funcionalidades extras mediante un teclado limitado con funciones programables.

Dispositivos resistentes al medio

Existen varios dispositivos que soportan agresiones del medios en el cual se espera que se desenvuelvan, como ser ambientes húmedos o mojados, distintos rangos de temperatura o incluso situaciones de impactos físicos.

Diseño del sistema en su conjunto

Diseño de la aplicación SCADA para entornos de Servicios de Terminal

Introducción

La implementación de una aplicación SCADA con equipos móviles utilizando los Servicios de Terminal de Microsoft Windows 2000, involucra tanto la configuración del servidor de terminal como la configuración de la aplicación SCADA en su entorno de trabajo.

Desde el punto de vista de los Servicios de Terminal, basta con habilitar los permisos de inicio de sesión a los usuarios correspondientes, junto con algunas políticas de seguridad y tratamiento de la sesión. Pero sin dejar de lado la aplicación de las y medidas de seguridad impuestas por las políticas de seguridad de la red a la que pertenece.

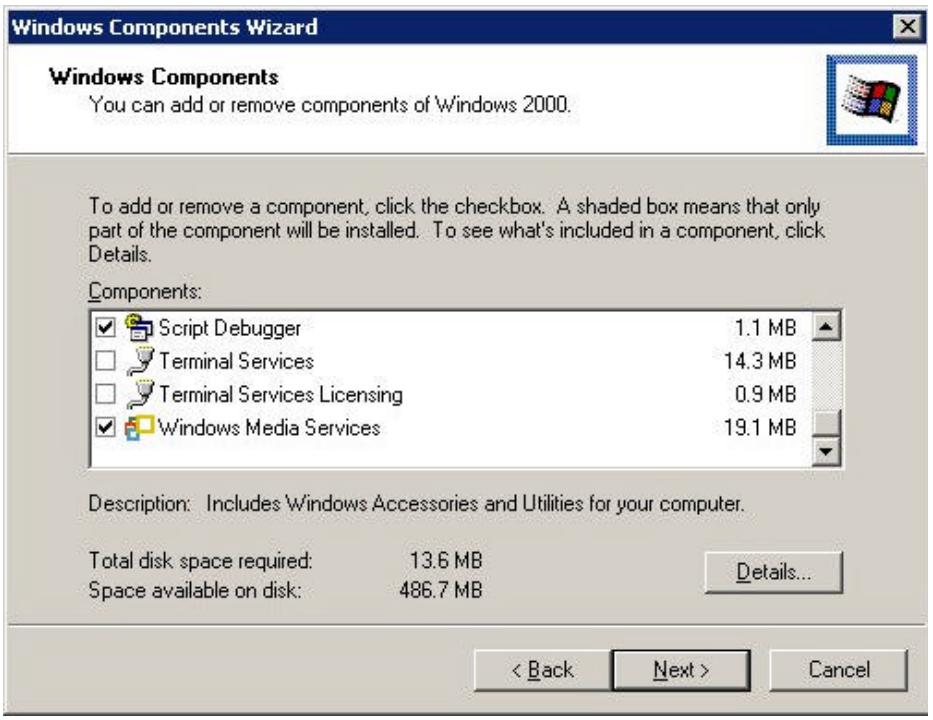
Por el lado de la aplicación SCADA, la configuración tiene un grado de complejidad mayor, dado por el propio entorno operativo de la aplicación. Esto implica determinar que información estará disponible para los usuarios que inician una sesión de Servicios de Terminal y deben acceder a visualizar la información del SCADA.

Los siguientes párrafos señalan los aspectos más relevantes para una implementación exitosa de una aplicación SCADA con dispositivos móviles apoyada en los Servicios de Terminal de Microsoft Windows 2000.

Configuración del servidor de Servicio de Terminal

Configuración del servicio

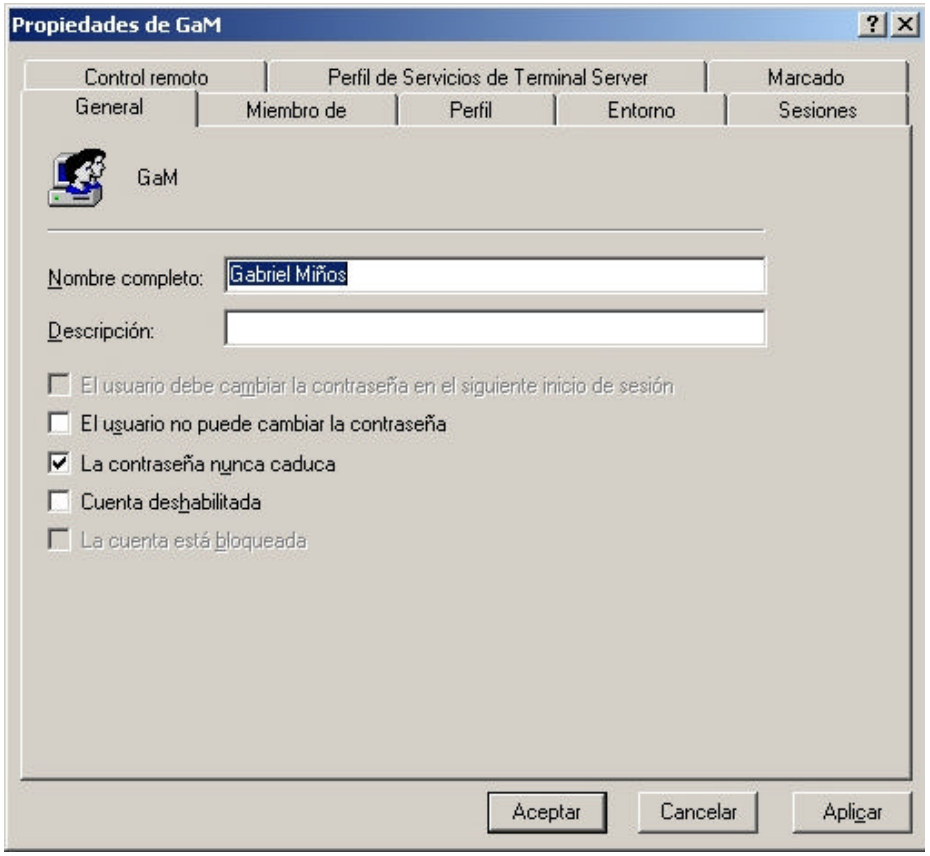
El Servicio de Terminal de Microsoft Windows 2000 es un componente incluido en el sistema operativo Microsoft Windows 2000 en las versiones para servidores. Como tal para su instalación sólo basta con incluirlo como componente del mismo.



Instalación del componente Servicios de Terminal.

Configuración de los permisos de usuario

Al incluir los Servicios de Terminal como componente del sistema operativo la herramienta de administración de usuarios sufre algunas modificaciones. Relacionadas mayormente con la configuración de los usuarios, se agregan a esta interfase las opciones necesarias para administrar la forma en la que los mismos podrán iniciar la sesión de Servicios de Terminal en el servidor.



Configuración de usuario tras la instalación de los Servicios de Terminal

Configuración del entorno de usuario y la sesión de terminal

Una vez que un usuario es autenticado en el servidor de Servicios de Terminal, éste puede presentarle dos opciones de interacción según se configure en el perfil del usuario.

Las opciones son:

- Presentar al usuario el escritorio de Windows relacionado con su perfil.
- Iniciar una aplicación determinada.

Conexión al escritorio de Windows

Si bien ésta no es la opción recomendada para los operadores de la aplicación SCADA, sí puede serla para un usuario con nivel de Administrador de la aplicación SCADA, de manera que él puede realizar tareas de ingeniería en la aplicación, como ser edición de pantallas y modificación de ciertos parámetros de configuración.

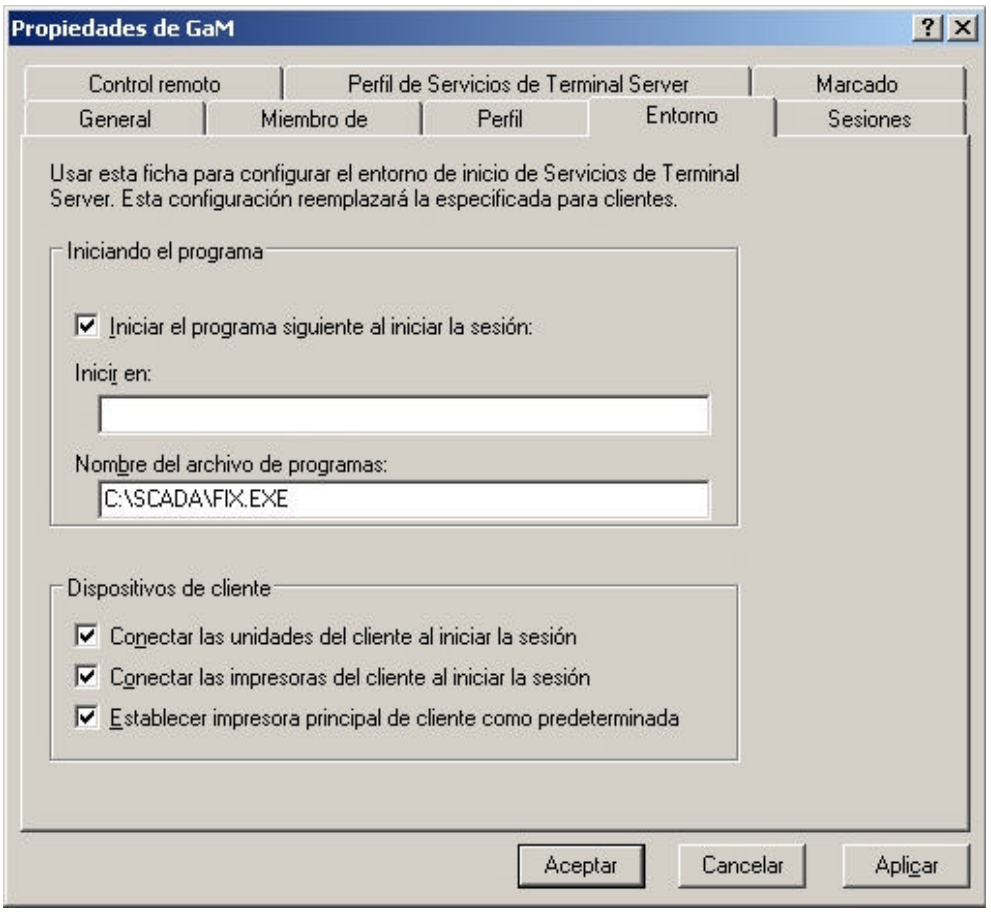
La conexión al escritorio de Windows presenta un vista familiar a la de una PC ejecutando el sistema operativo Microsoft Windows 2000. El usuario dispondrá de todas las opciones de navegación por las aplicaciones instaladas en el servidor, e incluso podrá hacer uso de los periféricos conectados a éste.

Inicio de una aplicación determinada

El administrador del servidor de Servicios de Terminal puede modificar el perfil del usuario de manera tal que cuando éste inicie una sesión en el servidor a través del Servicio de Terminal, se ejecute una sola aplicación que le es presentada al usuario.

Esta alternativa reduce las posibilidades de acceso inadecuado a otras aplicaciones, al mismo tiempo que agiliza la carga de la interfase propia del SCADA.

En particular la configuración de inicio de una aplicación determinada es la opción recomendada para la aplicación SCADA bajo Servicios de Terminal. De ésta manera, el usuario sólo podrá interactuar con la aplicación SCADA que se le presente y el mismo estará actuando en el servidor en un entorno reducido y controlado desde el punto de vista del consumo de recursos.



Especificación de la aplicación para la inicio de la sesión

Configuración de la aplicación SCADA

La configuración de la aplicación SCADA tiene determinados requerimientos fijados por la política de licenciamiento del producto mas una componente de optimización del uso de los recursos.

Así, se llega a un esquema de aplicaciones donde los servidores SCADA actúan en forma independiente del servidor de Servicios de Terminal, y éste se limita a actuar como cliente de todos los servidores SCADA que se encuentren en la red.

Esto aísla el funcionamiento del servidor de Servicios de Terminal y su carga de atención para sus clientes, de las tareas críticas que tenga que desempeñar cada nodo SCADA.

La configuración entonces, se separa en dos partes:

- Configuración de la aplicación SCADA en los servidores.
- Configuración de la aplicación SCADA en los servidores de Servicios de Terminal.

Configuración de la aplicación SCADA en los servidores

Es la configuración necesaria para el desarrollo de la aplicación de control que corre en los nodos SCADA servidores. Esta incluye la configuración de los controladores de comunicaciones, el diseño de la base de datos, configuración de los servicios de alarmas, el diseño de las pantallas gráficas y las restantes configuraciones particulares que demande el proceso objeto del control.

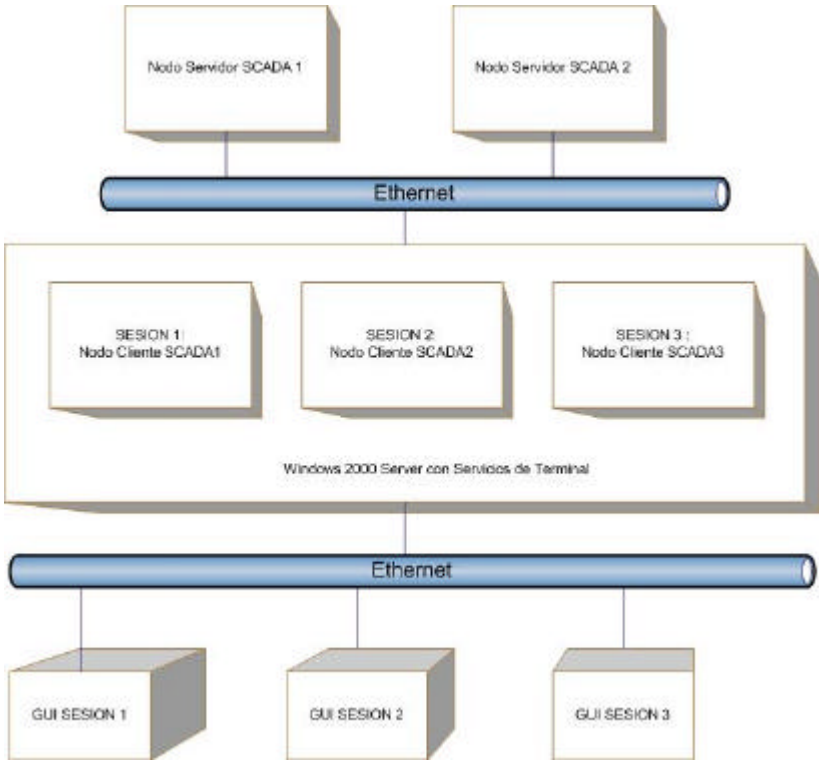
Configuración de la aplicación en el servidor de Servicios de Terminal

Esta configuración incluye las opciones que permiten la comunicación entre los nodos clientes que corren en cada sesión del servidor de Servicios de Terminal y los servidores SCADA. Incluye también la configuración del los perfiles y entornos de usuario para las cuentas habilitadas para establecer sesiones de Terminal.

Especificado por el diseño de la aplicación SCADA para entornos de Servicios de Terminal y la propia naturaleza del entorno multiusuario de estos, la configuración necesaria es similar a la que se necesita para armar un entorno de aplicaciones SCADA con uno o más servidores SCADA y numerosos clientes SCADA.

La diferencia fundamental radica en que el servidor de Servicios de Terminal es quien va a contener todos los nodos clientes que se requieran.

Esquemáticamente el modelo de funcionamiento es similar al siguiente:



Configuración de acceso a los nodos servidores SCADA

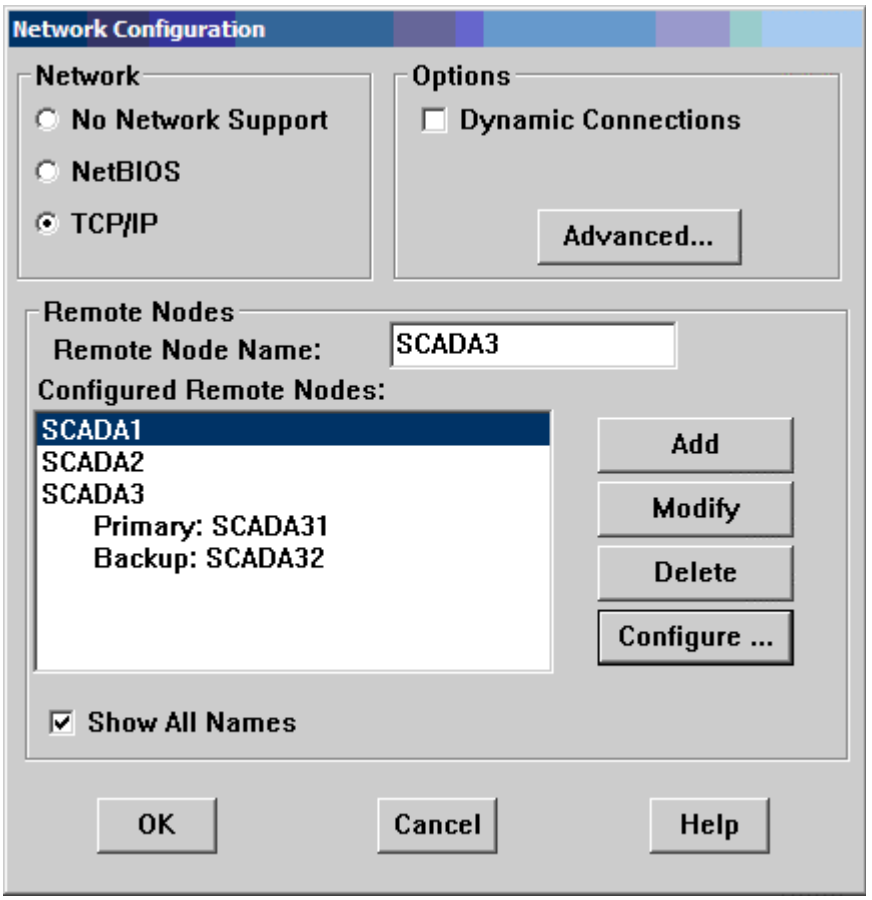
La configuración de red necesaria para que los nodos clientes SCADA de cada una de las sesiones puedan acceder a los servidores SCADA, se realiza utilizando la herramienta «Configuración del Sistema» provista por la aplicación SCADA. Ésta presenta una serie de opciones referidas a las habilidades de interconexión de los nodos clientes SCADA.

Las opciones necesarias para la comunicación entre nodos son: Protocolo de red y Nombres de nodos remotos.

El protocolo de red debe ser siempre TCP/IP. Si bien el sistema SCADA en forma independiente puede trabajar con NetBIOS* éste último no es soportado por la estructura de Servicios de Terminal presentada.

Los nombres de los nodos remotos son los nombres físico o lógicos de los nodos servidores SCADA que se encuentran dentro de la red del sistema SCADA y de los cuales se necesita obtener información.

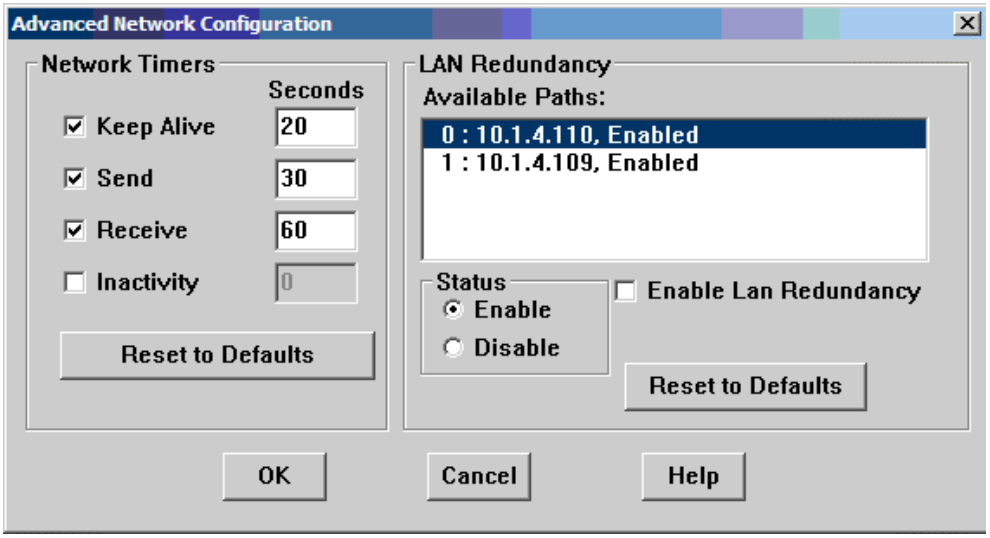
El siguiente gráfico muestra la configuración de red necesaria para conectar cada sesión de cliente de Servicios de Terminal con los servidores SCADA.



Configuración de red de nodos clientes SCADA

Por otro lado, cada sesión de cliente SCADA en el servidor de Servicios de Terminal debe utilizar una dirección IP distinta, de manera tal que cada servidor SCADA puede identifica a al nodo cliente que corresponde a cada sesión en el servidor.

Por tal motivo, es necesario configurar la dirección IP que utilizará cada nodo cliente SCADA. A tal fin la herramienta «Configuración del Sistema» provee un diálogo donde se especifica que dirección IP debe utilizar cada nodo cliente.



Configuración de la ruta de red para nodos clientes SCADA

Funcionamiento del sistema en su conjunto

El sistema en su conjunto exhibe la sinergia de la interacción de los componentes presentados. El valor agregado de reunir las características de los servicios seleccionados con la excelencia de determinados productos de mercado, mas la disponibilidad de tecnología que hasta hace unos años era privativa, permite crear una solución a un problema cotidiano que hasta el momento no contaba con una respuesta económicamente viable.

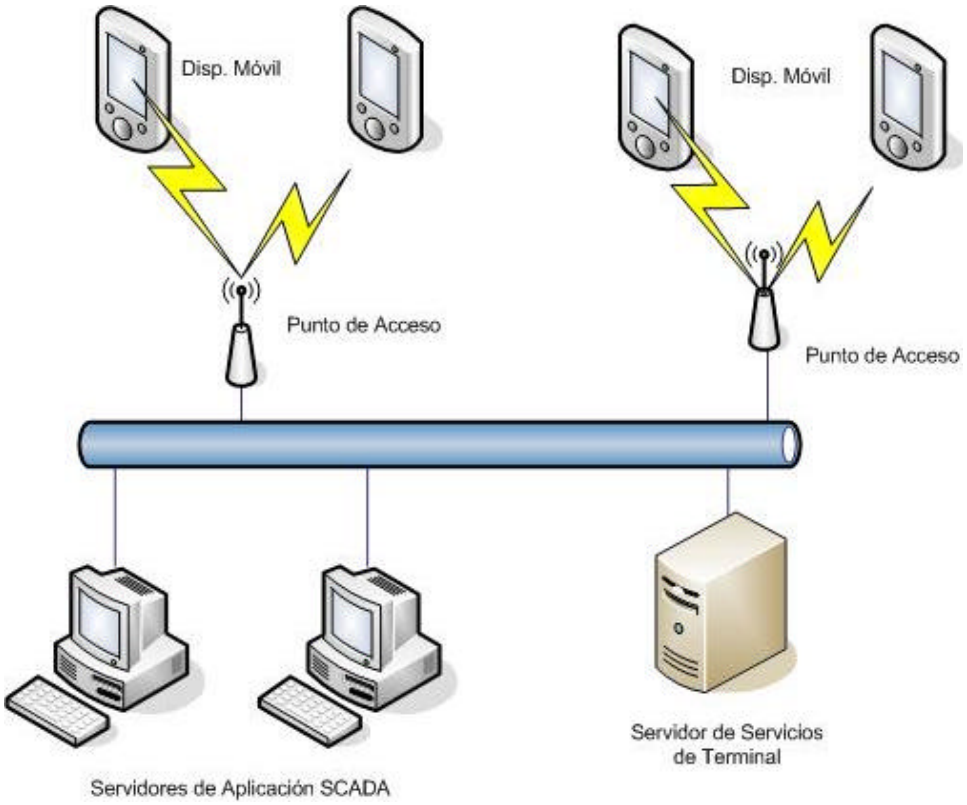
La solución integra entonces los siguientes componentes:

- Aplicación servidor de datos de SCADA.
- Aplicación HMI cliente de SCADA.
- Servicios de Terminal de Windows 2000.
- Tecnología de redes inalámbricas IEEE 802.11.
- Equipos móviles PocketPC de altas prestaciones.

Topología requerida por la aplicación

La topología de la aplicación presentada se ve reflejada en el siguiente esquema. En él se observan los siguientes componentes:

- Servidores de aplicación SCADA: En estos servidores se instala e implanta la aplicación de control para el proceso objeto que se desea controlar. La misma es desarrollada con el producto iFix de la compañía Intellution, la cual diseña producto de software para la industria del control de procesos basados en PC.
- Servidor de Servicios de Terminal: En éste servidor se instalar el sistema operativo Microsoft Windows 2000 en su versión servidor, junto a los servicios de Terminal incluidos en éste. También se instala el módulo cliente SCADA del producto iFix, configurado para que acceda a la información de los servidores SCADA presentes en la red.
- Red Ethernet: La red, y todas sus variantes de conectividad se basa en el estándar TCP/IP para poder lograr la interacción de todos los componentes.
- Puntos de Acceso: Son los dispositivos de tecnología inalámbrica IEEE 802.11 que permiten vincular una red de dispositivos inalámbricos con una red Ethernet TCP/IP existente. Estos se encargan de administrar el acceso a ésta de los dispositivos móviles a través de sus antenas estratégicamente instaladas.
- Dispositivos móviles: Son los equipos de mano de alta prestación, robustez y resistencia que emplearán los operadores de la aplicación SCADA en sus tareas diarias de operación y atención del proceso objeto del control. Estos dispositivos acompañan a los operarios, supervisores, personal de mantenimiento y de planificación, en su actividad diaria proveyendo información en tiempo real del estado y evolución del proceso.



Arquitectura de la aplicación propuesta

Conclusión final

Conclusión final acerca de la implementación
Conclusiones

El presente trabajo expone una forma alternativa a la utilización clásica de un producto de software para el control y supervisión de un proceso de naturaleza industrial. El enfoque práctico del mismo esta fundamentado en la necesidad de distribuir la información de manera de hacer más productivo el uso del sistema SCADA propuesto y colaborar activamente con la mejora del negocio.

Tras la cuidadosa selección de los productos disponibles en el mercado, complementado esto con un estudio de las fortalezas y debilidades de los mismos, se sugiere para la implementación un conjunto de herramientas que podrán cumplir con la expectativa de mejora esperada para un sistema como el aquí mencionado.

Los siguientes puntos señalan las fortalezas de la aplicación y el aporte de la propuesta a la industria de las aplicaciones SCADA.

Costo Total del Sistema

El Costo Total del Sistema (TCO – por sus siglas en Ingles de Total Cost of Ownership) se ve notablemente reducido al tomar la decisión de emplear para la implementación productos estándar del mercado. Al enfrentar la evaluación de los costos de un sistema desarrollado a medida de las necesidades de un determinado negocio, contra la implementación de determinados productos con reconocido prestigio, la valoración final se enfoca en las posibilidades de crecimiento del sistema.

Si se opta por una solución a medida, es muy probable que el sistema no logre evolucionar acompañando las necesidades del negocio. Y en caso de que si lo hiciera, éste costo suele ser más elevado comparado con la implementación de un producto de mercado, si se tiene en cuenta el costo que implica el tiempo de desarrollo e implementación.

Así mismo la libertad relacionada con la independencia de proveedores de soluciones específicas permitirá tomar las mejores decisiones respecto al empleo de fondos para proyectos de ampliación. Resulta trivial la observación que la dependencia de un proveedor impide la libre competencia de precios.

Mantenimiento

El mantenimiento del sistema está relacionado con las características del proceso y sus partes. Dentro de un sistema de control puede haber partes que no requieran mantenimiento a lo largo de su ciclo de vida, mientras que existen partes que sí necesitan de un mantenimiento periódico del tipo preventivo o del tipo correctivo.

En particular, los dispositivos que están relacionados con el uso intensivo por parte de personas están expuestos a grandes riesgos, ya sea por el desgaste como por los posibles malos tratos.

Estos factores se ven potenciados por la agresividad del medio donde deban desenvolverse. Evidentemente un ambiente extremadamente húmedo terminará oxidando partes metálicas de herramientas e instrumentos que no cuenten con la protección adecuada. De igual manera, los ambientes corrosivos terminan destruyendo las partes expuestas.

A los fines de disminuir estos impactos la industria propone ciertas normas de protección que deben seguir las partes de un proceso que trabajen bajo estas circunstancias. Así, es obligatorio que las herramientas en general que realizan trabajos de éste tipo cumplan con estas normas.

Para poder cumplir con estas exigencias es que se seleccionaron para esta implementación, equipos de mano que cumplen con los estándares de protección más estrictos comúnmente usados en la industria.

Esto permite que el reemplazo de los equipos frente a la eventualidad de su deterioro no afecte el cumplimiento de las normas necesarias. Así mismo, se cuenta con la libertad de elegir otros productos de mercado que ofrezcan similares características sin necesidad de modificar el sistema implementado.

Productividad

La implementación propone un sistema que complementa las acciones y trabajos cotidianos realizados con un sistema de supervisión tipo SCADA. El estudio de éstas acciones y la forma de llevarlas a cabo por el personal de trabajo manifiesta una posibilidad de mejora relacionada con el tiempo de respuesta.

Así, si el operador de un determinado equipo cuenta con la información necesaria para trabajar en él, en el preciso instante que está frente a él, evidentemente se hace más productivo su trabajo sobre éste.

La implementación se focaliza justamente en ese punto. En proveer a los operadores con una herramienta portátil que les permita interactuar con el sistema SCADA que supervisa un proceso determinado, al mismo tiempo que pueda proporcionar herramientas complementarias para optimizar el trabajo que se deba realizar.

Como propuesta para una aplicación de éste tipo podría utilizarse un dispositivo de mano que incluya un lector de códigos de barras de tecnología láser. El lector reconocería un código estampado sobre una unidad determinada y el sistema le proporcionaría información en tiempo real de la unidad que tiene frente a él.

De igual manera el sistema puede adaptarse a diversos y distintos perfiles de uso. Puede citar el caso de un supervisor de planta que, provisto con un dispositivo móvil conectado al sistema propuesto, contaría en todo momento con información en tiempo real del funcionamiento del proceso en cuestión. Podría tomar decisiones acerca del proceso e incluso adelantarse a los problemas que éste pueda tener.

Si, por ejemplo, se plantea el caso de un sistema de control para producción de determinado elemento en la modalidad «producción por lotes», el supervisor de producción podría conocer en todo momento el estado del ciclo de producción, conocer el tiempo restante para la finalización del mismo, o incluso ser notificado instantáneamente del problema. En éste último caso el dispositivo de mano lo proveerá de toda la información del proceso que él necesite para poder tomar una decisión rápida que permita disminuir el tiempo de parada del proceso y, en consecuencia, disminuir las pérdidas monetarias.

Confianza

Por los motivos antes expuestos, la implementación propuesta en el presente trabajo se fundamenta en el uso de productos y tecnologías que llevan un tácito sello de confianza por el renombre de compañías tecnológicas que acompañaron el desarrollo de la industria en los últimos años.

La forma seleccionada para la implementación y sus componentes están a la altura de la evolución tecnológica en sus respectivas áreas. En éste punto es importante considerar la tendencia del mercado hacia el uso de éstos dispositivos y las expectativas de las compañías para los próximos años. Estas auguran una notable expansión del uso de redes con tecnología inalámbrica y dispositivos móviles, a medida que la industria proporcione mejores técnicas de seguridad que acompañen la evolución de la ciencia en éste campo.

Crecimiento

Si se plantea el costo de implementar nuevas estaciones de trabajo para explotar la información del sistema, contemplando el tendido de cables, los requerimientos de una PC para correr un sistema SCADA,

el tiempo de instalación; contra la implementación inmediata que proporciona el sistema actual, la decisión es bastante simple.

Con la implementación propuesta, agregar una estación de consulta al sistema SCADA implica conectar una PC a la toma de corriente y proveerla de una placa de red con tecnología inalámbrica. El único requisito para el sistema operativo es que pueda correr un cliente de Servicios de Terminal, el cual se encuentra disponible para casi todas las versiones de Windows, Unix y Mac OS entre otros con muy bajos requerimientos de memoria.

Esto hace que acompañar el crecimiento del sistema tenga un impacto mínimo al momento de encarar la inversión de expansión.

Conclusión final

Es de esperar que tras la implementación de los dispositivos móviles con red inalámbrica al sistema completo de la aplicación SCADA, se vea una notable mejora en las siguientes áreas:

- La forma de trabajo diario.
- La forma de interactuar con el sistema de supervisión.
- Disminuya el tiempo para la toma de decisiones.
- Mejore el funcionamiento del sistema de control en relación con los interesados en la información del mismo y sus operarios.
- El sistema estará preparado para soportar mayores exigencias relacionadas con la demanda de información.

El constante avance tecnológico impulsado por la industria y alimentado por la creciente demanda de información en tiempo real, hará que las tecnologías que hoy se presentan como innovadoras, mañana pasen a estar en el recuerdo como los pilares que promovieron el cambio.

Los estándares actúan como el ADN para el mundo de la tecnología, es un código común que asegura la consistencia de los productos y el correcto funcionamiento de los mismos. Sin estos estándares los sistemas de computación serían un caos donde ninguno funcionaría con el otro, a no ser que se adquiera todo del mismo proveedor.

Si bien no puede tomarse esto como una regla universal y supeditar las inversiones a la «oferta del mes», es importante evaluar las necesidades actuales e intentar predecir las futuras. En ese arriesgado camino la tecnología seleccionada puede marcar la diferencia entre un largo camino de éxito y un fracaso a corto plazo.

Para el presente trabajo se tomaron los recaudos necesarios para proveer independencia a los sistemas de control existentes, mientras se genera un sistema con nuevas posibilidades de crecimiento. Es decir, que no requiere modificación alguna sobre la aplicación de control actual.

La implementación contribuye a la expansión de sistemas actuales cuyas oportunidades de mejora son evidentes. Pero sin embargo no propone un camino sin retorno que ponga en juego la integridad del proceso sobre el cual actúa el sistema de supervisión y control, preservando así las inversiones realizadas.

Cada negocio tiene sus propias necesidades de información y la tecnología informática provee las herramientas para satisfacerlas, al mismo tiempo que genera nuevas expectativas y abre las puertas para nuevos desarrollos innovadores.Glosario y Acrónimos.

Catálogo de términos y acrónimos usados en el escrito en su idioma original

802.11a - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz.

802.11b - An IEEE wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

802.11g - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.

Access Point - Device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

Adapter - This is a device that adds network functionality to your PC.

Ad-hoc - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

AES (Advanced Encryption Standard) - A method that uses up to 256-bit key encryption to secure data.

Backbone - The part of a network that connects most of the systems and networks together, and handles the most data.

Bandwidth - The transmission capacity of a given device or network.

Beacon Interval - The frequency interval of the beacon, which is a packet broadcast by a router to synchronize a wireless network.

Bit - A binary digit.

Boot - To start a device and cause it to start executing instructions.

Bridge - A device that connects two different kinds of local networks, such as a wireless network to a wired Ethernet network.

Broadband - An always-on, fast Internet connection.

Browser - A browser is an application program that provides a way to look at and interact with all the information on the World Wide Web.

Buffer - A block of memory that temporarily holds data to be worked on later when a device is currently too busy to accept the data.

Cable Modem - A device that connects a computer to the cable television network, which in turn connects to the Internet.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) - A method of data transfer that is used to prevent data loss in a network.

CTS (Clear To Send) - A signal sent by a device to indicate that it is ready to receive data.

Daisy Chain - A method used to connect devices in a series, one after the other.

Database - A collection of data that is organized so that its contents can easily be accessed, managed, and updated.

DDNS (Dynamic Domain Name System) - The capability of having a website, FTP, or e-mail server-with a dynamic IP address-use a fixed domain name.

Default Gateway - A device that forwards Internet traffic from your local area network.

DHCP (Dynamic Host Configuration Protocol) - A protocol that lets one device on a local network, known as a DHCP server, assign temporary IP addresses to the other network devices, typically computers.

DMZ (Demilitarized Zone) - Removes the Router's firewall protection from one PC, allowing it to be «seen» from the Internet.

DNS (Domain Name Server) - The IP address of your ISP's server, which translates the names of websites into IP addresses.

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

DSL (Digital Subscriber Line) - An always-on broadband connection over traditional phone lines.

DSSS (Direct-Sequence Spread-Spectrum) - A type of radio transmission technology that includes a redundant bit pattern to lessen the probability of data lost during transmission. Used in 802.11b networking.

DTIM (Delivery Traffic Indication Message) - A message included in data packets that can increase wireless efficiency.

Dynamic IP Address - A temporary IP address assigned by a DHCP server.

EAP (Extensible Authentication Protocol) - A general authentication protocol used to control network access. Many specific authentication methods work within this framework.

EAP-PEAP (Extensible Authentication Protocol-Protected Extensible Authentication Protocol) - A mutual authentication method that uses a combination of digital certificates and another system, such as passwords.

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) - A mutual authentication method that uses digital certificates.

Encryption - Encoding data to prevent it from being read by unauthorized people.

Ethernet - An IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

Finger - A program that tells you the name associated with an e-mail address.

Firewall - Security measures that protect the resources of a local network from intruders.

Firmware - 1. In network devices, the programming that runs the device. 2. Programming loaded into read-only memory (ROM) or programmable read-only memory (PROM) that cannot be altered by end-users.

Fragmentation - Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

FTP (File Transfer Protocol) - A standard protocol for sending files between computers over a TCP/IP network and the Internet.

Full Duplex - The ability of a networking device to receive and transmit data simultaneously.

Gateway - A system that interconnects networks.

Half Duplex - Data transmission that can occur in two directions over a single line, but only one direction

at a time.

Hardware - The physical aspect of computers, telecommunications, and other information technology devices.

HTTP (HyperText Transport Protocol) - The communications protocol used to connect to servers on the World Wide Web.

IEEE (The Institute of Electrical and Electronics Engineers) - An independent institute that develops networking standards.

Infrastructure - Currently installed computing and networking equipment.

Infrastructure Mode - Configuration in which a wireless network is bridged to a wired network via an access point.

IP (Internet Protocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

IPCONFIG - A Windows 2000 and XP utility that displays the IP address for a particular networking device.

IPSec (Internet Protocol Security) - A VPN protocol used to implement secure exchange of packets at the IP layer.

ISM band - Radio band used in wireless networking transmissions.

ISP (Internet Service Provider) - A company that provides access to the Internet.

LAN (Local Area Network) - The computers and networking products that make up the network in your home or office.

LEAP (Lightweight Extensible Authentication Protocol) - A mutual authentication method that uses a username and password system.

MAC (Media Access Control) Address - The unique address that a manufacturer assigns to each networking device.

Mbps (Megabits Per Second) - One million bits per second; a unit of measurement for data transmission.

mIRC - An Internet Relay Chat program that runs under Windows.

Multicasting - Sending data to a group of destinations at once.

NAT (Network Address Translation) - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

Network - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

NNTP (Network News Transfer Protocol) - The protocol used to connect to Usenet groups on the Internet.

Node - A network junction or connection point, typically a computer or work station.

OFDM (Orthogonal Frequency Division Multiplexing) - A type of modulation technology that separates the data stream into a number of lower-speed data streams, which are then transmitted in parallel. Used in 802.11a, 802.11g, and powerline networking.

Packet - A unit of data sent over a network.

Passphrase - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.

Ping (Packet INternet Groper) - An Internet utility used to determine whether a particular IP address is online.

POP3 (Post Office Protocol 3) - A standard protocol used to retrieve e-mail stored on a mail server.

Port - 1. The connection point on a computer or networking device used for plugging in a cable or an adapter. 2. The virtual connection point through which a computer uses a specific application on a server.

Power over Ethernet (PoE) - A technology enabling an Ethernet network cable to deliver both data and power.

PPPoE (Point to Point Protocol over Ethernet) - A type of broadband connection that provides authentication (username and password) in addition to data transport.

PPTP (Point-to-Point Tunneling Protocol) - A VPN protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. This protocol is also used as a type of broadband connection in Europe.

Preamble - Part of the wireless signal that synchronizes network traffic.

RADIUS (Remote Authentication Dial-In User Service) - A protocol that uses an authentication server to control network access.

RJ-45 (Registered Jack-45) - An Ethernet connector that holds up to eight wires.

Roaming - The ability to take a wireless device from one access point's range to another without losing the connection.

Router - A networking device that connects multiple networks together, such as a local network and the

Internet.

RTS (Request To Send) - A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SMTP (Simple Mail Transfer Protocol) - The standard e-mail protocol on the Internet.

SNMP (Simple Network Management Protocol) - A widely used network monitoring and control protocol.

Software - Instructions for the computer. A series of instructions that performs a particular task is called a «program».

SPI (Stateful Packet Inspection) - Type of firewall that inspects incoming data packets to make sure that they correspond to an outgoing request. Unsolicited (and possibly harmful) packets are rejected.

Spread Spectrum - Wideband radio frequency technique used for more reliable and secure data transmission.

SSID (Service Set IDentifier) - Your wireless network's name.

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

Static Routing - Forwarding data in a network via a fixed path.

Subnet Mask - An address code that determines the size of the network.

Switch - 1. Device that is the central point of connection for computers and other devices in a network, so data can be shared at full transmission speeds. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP/IP (Transmission Control Protocol/Internet Protocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

Telnet - A user command and TCP/IP protocol used for accessing remote PCs.

TKIP (Temporal Key Integrity Protocol) - A wireless encryption protocol that periodically changes the encryption key, making it harder to decode.

TFTP (Trivial File Transfer Protocol) - A version of the TCP/IP FTP protocol that uses UDP and has no directory or password capability.

Throughput - The amount of data moved successfully from one node to another in a given time period.

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

UDP (User Datagram Protocol) - A network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent.

Upgrade - To replace existing software or firmware with a newer version.

Upload - To transmit a file over a network.

URL (Uniform Resource Locator) - The address of a file located on the Internet.

VPN (Virtual Private Network) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN (Wide Area Network) - The Internet.

WEP (Wired Equivalent Privacy) - A method of encrypting data transmitted on a wireless network for greater security.

WINIPCFG - A Windows 98 and Millennium utility that displays the IP address for a particular networking device.

WLAN (Wireless Local Area Network) - A group of computers and associated devices that communicate with each other wirelessly.

WPA (Wi-Fi Protected Access™) - A security method that encrypts the data transmitted on a wireless network so that only users who know the passphrase or shared key can access the network or understand the transmitted data.

WPA-Personal - A version of WPA that uses long and constantly changing encryption keys to make them difficult to decode.

WPA-Enterprise - A version of WPA that uses the same dynamic keys as WPA-Personal and also requires each wireless device to be authorized according to a master list held in a special authentication server.

Acrónimos

AES - Advanced Encryption Standard
CSMA/CA - Carrier Sense Multiple Access/Collision Avoidance
CTS - Clear To Send
DDNS - Dynamic Domain Name System
DHCP - Dynamic Host Configuration Protocol
DMZ - Demilitarized Zone
DNS - Domain Name Server
DSL - Digital Subscriber Line
DSSS - Direct-Sequence Spread-Spectrum
DTIM - Delivery Traffic Indication Message
EAP - Extensible Authentication Protocol
EAP-PEAP - Extensible Authentication Protocol-Protected Extensible Authentication Protocol
EAP-TLS - Extensible Authentication Protocol-Transport Layer Security
FTP - File Transfer Protocol
HTTP - HyperText Transport Protocol
IEEE - The Institute of Electrical and Electronics Engineers
IP - Internet Protocol
IPSec - Internet Protocol Security
ISP - Internet Service Provider
LAN - Local Area Network
LEAP - Lightweight Extensible Authentication Protocol
MAC Address - Media Access Control Address
Mbps - Megabits Per Second
NAT - Network Address Translation
NNTP - Network News Transfer Protocol
OFDM - Orthogonal Frequency Division Multiplexing
PDB – Process Data Base
Ping - Packet INternet Groper
PoE - Power over Ethernet
POP3 - Post Office Protocol 3
PPPoE - Point to Point Protocol over Ethernet
PPTP - Point-to-Point Tunneling Protocol
RADIUS - Remote Authentication Dial-In User Service
RJ-45 - Registered Jack-45
RTS - Request To Send
SAC – Scan and Alarm Control
SCADA – Supervisory Controls And Data Acquisition
SMTP - Simple Mail Transfer Protocol
SNMP - Simple Network Management Protocol
SPI - Stateful Packet Inspection
SSID - Service Set IDentifier
TCP/IP - Transmission Control Protocol/Internet Protocol
TFTP - Trivial File Transfer Protocol
TKIP - Temporal Key Integrity Protocol
UDP - User Datagram Protocol
URL - Uniform Resource Locator
VPN - Virtual Private Network
WAN - Wide Area Network
WEP - Wired Equivalent Privacy
WLAN - Wireless Local Area Network
WPA - Wi-Fi Protected Access™

Bibliografía

Referencia de las fuentes de información empleadas en el análisis

Intellution
Manual oficial de capacitación – iFix Fundamentals versión 3.0.01.03 – GE FANUC Intellution.
Sitio de referencia: www.intellution.com

Microsoft
Guía de implementación de aplicaciones para Servicios de Terminal en Windows 2000– Windows 2000 Terminal Server White Pappers – Microsoft Corporation.
Introducción a RDP 5.0 - Windows 2000 Terminal Server White Pappers - Microsoft Corporation.
Guía de Optimización de Aplicaciones para Servicios de Terminal - Windows 2000 Terminal Server White Pappers - Microsoft Corporation.
Sitio de referencia: www.microsoft.com/windows2000/technologies/terminal/

Symbol
Dispositivos móviles de altas prestaciones – Symbol.
Sitio de referencia: www.symbol.com

LinkSys
Guía para la implementación de redes inalámbricas – Linksys.
Sitio de referencia: www.linksys.com/edu/