Monitoreo y Optimización a sistemas SCADA convencionales con un enfoque TCP/IP

Adrian Pavesi[1,2], Diego Navarro[2], Antonio Castro Lechtaler[3],

Jorge S. García Guibout[2]

[1] SINOPEC Argentina, [2] Universidad de Mendoza,
[3] Universidad Tecnológica Nacional

{AdrianPavesi: Adrian_Pavesi@sinopecarg.com.ar, Diego Navarro diego.navarro@um.edu.ar, Antonio Castro Lechtaler: Antonio.castrolechtaler@gmail.com, Jorge S. García Guibout jgarcia@um.edu.ar}

Abstract. Históricamente los sistemas SCADA en las empresas productoras de petróleo han sido cuestionados debido a lo difícil que se hace justificarlos económicamente en las etapas primarias de la producción, pues sus ventajas operativas son variadas. Las razones, entre otras, es lo difícil de cuantificar sus beneficios para cada yacimiento. Esto se debe principalmente a que el sostenimiento de la producción se lleva a cabo con medidas que no dependen del procesamiento en línea. La implantación de este tipo de sistemas deriva de una decisión organizativa y política, más que de un claro estudio de los beneficios que serán atribuidos a los sistemas. Este trabajo describe las mejoras que es necesario realizar en los sistemas implementados para poder sostener la calidad del servicio, principalmente, en aspectos técnicos de networking y los problemas propios de su alcance debido a la complejidad y cantidad de puntos con los que cuenta la red de automatización. Éstas utilizan recursos simples, pensados estratégicamente para maximizar el uso de los escasos recursos humanos. Exigen por lo tanto, una mayor concentración del soporte técnico y de los activos instalados

Keyword: SCADA, TCP, IP, SNMP

1 Introducción

Durante el año 2006 la empresa norteamericana Occidental Petroleum, realizó la compra de los activos y áreas petroleras asociadas a la empresa VintageOil. El cambio implicó una renovación tecnológica que derivó en varias acciones organizativas para optimizar las tareas técnicas de campo y cambiar la metodología de trabajo de los yacimientos.

Durante el año 2007 se llevó a cabo la instalación de la infraestructura necesaria para conectar las oficinas de yacimientos a una red corporativa, realizando un anillo SDH de 100 MBS como troncal que además es redundante y los cableados estructurados necesarios para poder aplicar las herramientas de oficina que facilitaran

los reportes y la toma de decisiones. También se instalaron controladores y sistemas de Control de Supervisión y Adquisición de Datos - SCADA[1]en las principales plantas de tratamiento, baterías, como también en los controladores para los aproximadamente 2000 pozos de la empresa, repartidos en un total de 9 yacimientos en Santa Cruz, Chubut y Mendoza.

Los cortes de energía, muy habituales en los yacimientos, hace que se pierda el contacto con los dispositivos a controlar, lo que sumado a la gran cantidad de puntos de control y los pequeños tiempos de escaneo, hace que el sistema genere las consultas a esos dispositivos que al no ser completadas, lleva finalmente al bloqueo del servidor con la consiguiente caída de la totalidad del sistema. En la reanudación del mismo se bloquean manualmente aquellas zonas sin energía, debiendo reinstalarlas manualmente una vez subsanada la falla.

En la actualidad Occidental Petroleun vendió sus activos y áreas petroleras de Argentina a la empresa estatal China Sinopec International [1], quien ha continuado administrando y mejorando la totalidad de los sistemas instalados.

En la actualidad la empresa cuenta con los puntos de control y sistemas SCADA instalados que se detallan en la tabla 1.

Tabla1: Cantidad de dispositivos a controlar por yacimiento

ITEM	Santa Cruz	Mendoza	Total
Dispositivos Eléctricos	125	3	128
Baterías de Tanques	24	3	27
Plantas de Inyección de Agua	4	1	5
Puntos de medición de Gas	58	-	58
Unidades automáticas de medición	4	1	5
Plantas de Tratamiento	4	1	5
Calentadores	6	3	9
Compresores de Gas	8	-	8
Pozos	1550	100	1650
Servers & Clusters	10	6	16
Usuarios simultáneos de SCADA			150

[1]Supervisory Control And Data Acquisition.

2 Desarrollo

El modelo inicial se implementó definiendo un modelo operativo centralizado de los sistemas SCADA para áreas geográficamente contiguas.

De esta manera se instalaron en Argentina dos grandes centros de datos: uno en el departamento de Tupungato en la provincia de Mendoza y el otro en Cañadón Seco provincia de Santa Cruz.

La unidad de datos más compleja es la de Santa Cruz, ya que con el mismo Centro de Datos se le da servicio a un total de 8 áreas petroleras que son controladas en oficinas repartidas en una franja territorial de 80 por 160 kilómetros de largo.

La cantidad de puntos a controlar creció tanto que llegó a un punto que los fabricantes de los equipos no habían experimentado en el resto de las instalaciones en el mundo.

Esto derivo en la aparición de problemas complejos, muchos de los cuales nunca habían sido planteados, a tal punto que desbordaban aún al soporte oficial brindado por los desarrolladores de las tecnologías aplicadas, debiendo recurrir en estas ocasiones a la utilización de recursos de ingeniería local específicos a los problemas que fueron apareciendo.

Este trabajo trata de describir la actividad realizada para subsanar algunos de los problemas detectados específicamente en aplicaciones y comunicaciones de Automatización.

3 Descripción del escenario técnico

El escenario técnico esta descripto por un esquema de capas, las cuales sirvieron para estandarizar los equipos y llevar a cabo la implementación de ellos. Este esquema se detalla a continuación.

Nivel 0 (Dispositivos Finales de Medición).
Estos son los medidores, switches o instrumentos digitales que están en contacto directamente con el proceso, son los que originan los datos y valores de las variables de campo que son tomados por los dispositivos de control de procesos.
Por lo general son instrumentos digitales, de 4 a 20 mA, 0 a 5 Volts, medidores de pulsos o dispositivos con algún protocolo especial a la medida de las variables que se están midiendo.

Nivel 1 (Dispositivos de control de procesos).
Son los concentradores de la información de campo, estos generalmente poseen inteligencia para realizar cálculos con diferentes variables tomadas del nivel 0 y permiten no solo el control, sino el reporte de las mismas con algún protocolo de comunicación de datos estándar independiente del nivel anterior.

Los dispositivos de este nivel suelen ser Terminales Remotas (RTU), Controladores Lógicos Programables (PLC) o dispositivos específicos para la medición de procesos del petróleo, como por ejemplo medidores de fluido OMNI 6000 [5] para las unidades de entrega de petróleo o los controladores Lufkin SAM [4]

para regular la velocidad de funcionamiento de las bombas de los pozos con aparatos individuales de bombeo.

Nivel 2 (última milla de comunicaciones).

En este nivel tenemos como estándar las comunicaciones Ethernet, con Fibra óptica en plantas, cableado estructurado para los tableros o sistemas inalámbricos para los pozos y locaciones remotas. Estos diferentes modos de comunicación se integran al anillo de comunicaciones corporativo.

Nivel 3 (troncal de comunicaciones).

El troncal de comunicaciones está compuesto por más de 40 torres repetidoras, distribuidas geográficamente para poder llevar los datos de campo a los diferentes servidores de la compañía.

Este nivel está compuesto por dos anillos diferentes: un anillo para los datos de aplicaciones y usuarios y el otro anillo para los datos de campo. Son 2 redes separadas lógica y físicamente, que permiten un ágil acceso a los servidores e independizan los sistemas de control de las aplicaciones administrativas.

Nivel 4 (OPC Servers).

El OPC Server [2] (antiguamente definido como Ole for Process Control), es una aplicación que está desarrollada para la comunicación con dispositivos remotos como por ejemplo con PLC´s, módulos de I/O, etc., utilizando los protocolos propios de cada dispositivo, Posee la particularidad de dejar la información de los dispositivos remotos disponible en una jerarquía de árbol, que independiza a los sistemas de información de la comunicación con cada dispositivo en particular.

Nivel 5 (Human Machine Interface HMI)

El HMI (Interfase Hombre Máquina) [3] es el grupo de programas que se alimenta de la información disponible a nivel de OPC y permite la utilización de diagramas, alarmas y tendencias, para poder representar los diferentes procesos y el estado de las variables que lo componen. Es el nivel al cual acceden los usuarios para conocer en tiempo real el estado de los dispositivos de monitoreo y control de campo.

4 Mapa de red

La red de Santa Cruz está compuesta por un total de 40 repetidoras, en la figura 1 podemos observar en color rojo el nivel 3 correspondiente a la red de automatización y en color azul el nivel 3 correspondiente a las aplicaciones de oficina.

En ambos casos se utilizan VLAN´s para el direccionamiento y encaminamientos de datos para optimizar los anchos de banda. También en ambos casos se utilizan protocolos de redundancia como Rapid SpaningTree, para poder tener rutas alternativas para el tráfico de datos en caso de caída de los sitios repetidores.

En color celeste vemos las extensiones de última milla utilizados para puntos específicos que no tienen línea de vista con las repetidoras principales.

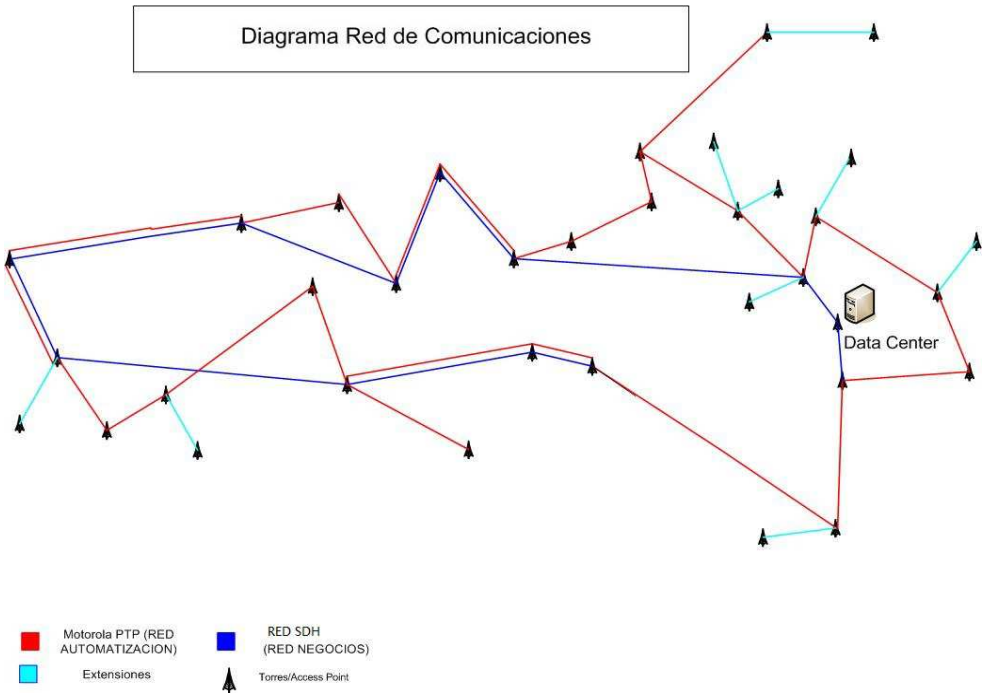

Figura 1: Red de comunicaciones del yacimiento en Sata Cruz

4.1 Situación problemática

Un problema emblemático se suscita cuando los remotos no responden a la capa OPC por problemas de comunicación.

Debido a que a la comunicación que genera el OPC para recolectar la información de los remotos es a través de los protocolos TCP/IP, el sistema operativo implementa hilos o threds independientes para cada uno de los dispositivos remotos.

Cuando se produce una falla importante durante la consulta, por ejemplo la pérdida de comunicación para un elevado número de remotos, gran parte de los recursos del server son utilizados para completar los tiempos de espera determinados por el protocolo. Esto hace que el OPC pierda el control de los paquetes y se generen grandes colas a la espera del establecimiento de la comunicación, lo que desencadena en errores del servicio OPC, dejando a las aplicaciones HMI sin obtener los datos esperados.

Estos errores obligan a acciones de control manual para reiniciar los servicios afectados en OPC y las aplicaciones HMI asociadas, proceso que lleva al menos un par de horas, dejando a los usuarios a ciegas hasta el restablecimiento del servicio.

4.2 Descripción general del desarrollo

El desarrollo debe ser simple y fácil de mantener, debido a la dinámica con la que se realizan altas, bajas y modificaciones en los nodos remotos, propio comportamiento de los yacimientos petrolíferos.

Una posibilidad y quizás la mejor opción es trabajar con el protocolo SMNP sobre las remotas, satisfaciendo uno de los requisitos impuestos que sea un protocolo estándar, que no agrega complejidad al desarrollo y permite ser flexibles a la hora de seleccionar la tecnología de conexión de los pozos.

Las necesidades puntuales requeridas para poder solucionar el problema son las siguientes:

- Asegurar la actualización del estado del canal de manera automática.
- El estado del canal debe concordar con el estado real del sistema remoto de pozos.
- El sistema debe reaccionar de manera rápida y ordenada, sin afectar de manera importante en los procesos que corren en los servidores.
- Debe permitir conocer el estado general en cualquier momento.
- Debe estar disponible un registro (log) de actividades de manera que permita observar el comportamiento en el tiempo de los canales.
- La herramienta debe ser flexible y fácil de implementar.
- Debe requerir el mínimo posible de mantenimiento.

La búsqueda de una solución estándar e integral a los dispositivos de la red y los diferentes sistemas, derivó en la posibilidad de utilizar el **Protocolo Simple de Administración de Red - SNMP**[2] como herramienta de control de comunicación del OPC Server.

Dependiendo del estado de la radio remota, se ejecuta una función que crea una escritura binaria sobre el campo “enabled” del servidor OPC, permitiendo bloquear el uso de los remotos que no contestan debido a fallas de comunicación o cortes de energía.

El hecho de consultar el estado de las remotas, no genera tráfico ni colas a nivel de OPC, logrando la estabilidad y el normal funcionamiento del servicio en el servidor, ya que durante el periodo de SCAN los remotos consultados son solo los activos.

Si la comunicación se restablece, el driver SNMP del remoto contesta con el nuevo estado, y esta condición es utilizada por la misma función para habilitar nuevamente el dispositivo en el servidor OPC.

5 Protocolo SNMP

Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento [7][8][9].

SNMP también puede trabajar con dispositivos no-SNMP utilizando agentes *proxy*. Un agente *proxy* es un conversor de protocolo que traduce las órdenes SNMP a las comprensibles por el protocolo de gestión propio del dispositivo. Actualmente SNMP está soportado en muchos sistemas como PC’s, switches, servidores, etc.

[2]Simple Network Management Protocol.

SNMP se basa en un sistema de **petición-respuesta**. La autoridad gestora no es la red como sistema sino una o varias estaciones NMS (por sus siglas en inglés de Sistema Administrador de Red).
La arquitectura SNMP consta de los siguientes componentes:

- **Gestores** (NMS's)
- **Agentes** (nodos administrados)
- **MIB** (base de datos con información)
- **SMI** (administración de la base de datos)
- **protocolos** (órdenes)

Una Base de Información de Administración (MIB) es una colección de información que está organizada jerárquicamente. Las MIB's son accedidas usando un protocolo de administración de red, como por ejemplo, SNMP.

Un objeto administrado (algunas veces llamado objeto MIB, objeto, o MIB) es uno de cualquier número de características específicas de un dispositivo administrado. Los objetos administrados están compuestos de una o más instancias de objeto, que son esencialmente variables.

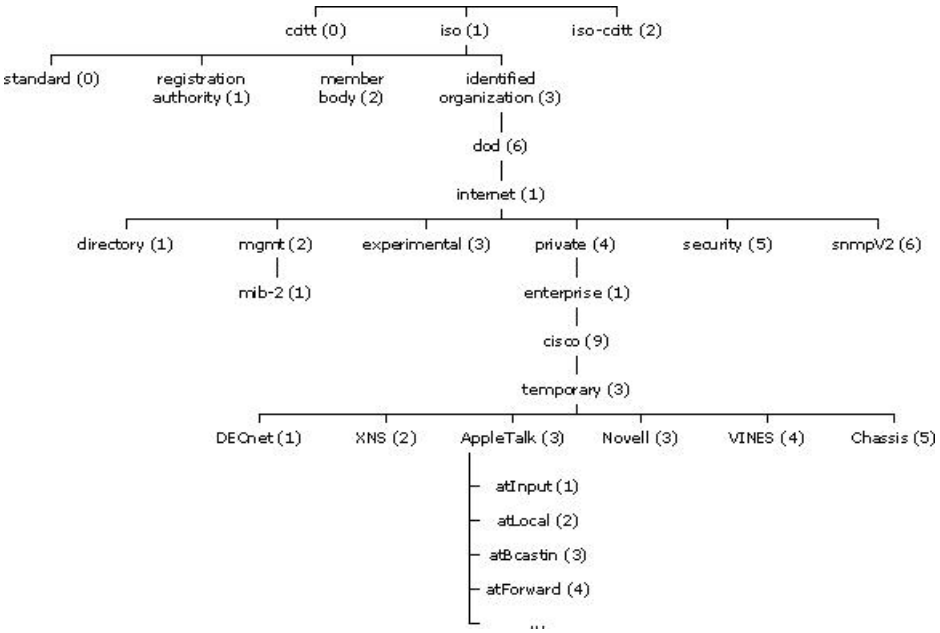

Figura 2: el árbol MIB ilustra las variadas jerarquías asignadas por las diferentes organizaciones

Existen dos tipos de objetos administrados: Escalares y tabulares. Los objetos escalares definen una simple instancia de objeto. Los objetos tabulares definen múltiples instancias de objeto relacionadas que están agrupadas conjuntamente en tablas MIB.

Un identificador de objeto (*object ID*) identifica únicamente a un objeto administrado en la jerarquía MIB. La jerarquía MIB puede ser representada como un

árbol con una raíz anónima y los niveles, que son asignados por diferentes organizaciones, como se muestra en la siguiente figura2.

Los identificadores de los objetos ubicados en la parte superior del árbol pertenecen a diferentes organizaciones estándares, mientras los identificadores de los objetos ubicados en la parte inferior del árbol son colocados por las organizaciones asociadas.

Los vendedores pueden definir ramas privadas que incluyen los objetos administrados para sus propios productos. Las MIB's que no han sido estandarizadas típicamente están localizadas en la rama de los árboles.

El objeto administrado atInput podría ser identificado por el nombre de objeto *iso.identified-organization.dod.internet.private.enterprise.cisco.temporary.AppleTalk.atInput* o por el descriptor de objeto equivalente *1.3.6.1.4.1.9.3.3.1*.

El corazón del árbol MIB se encuentra compuesto de varios grupos de objetos, los cuales en su conjunto son llamados mib-2.

Los grupos son los siguientes: System (1);Interfaces (2);AT (3);IP (4);ICMP (5);TCP (6);UDP (7);EGP (8);Transmission (10);SNMP (11).

Es importante destacar que la estructura de una MIB se describe mediante el estándar ASN.1 (Abstract Syntax Notation One).

SNMP utiliza el protocolo UDP, para evitar recarga de la red con protocolos orientados a la conexión, y los puertos utilizados son 161 y 162

6. Descripción lógica del sistema

La composición lógica es un modelo de definición con una entrada y dos posibles salidas, lo que permite realizar el código en cualquier herramienta que combine el servicio de SNMP con el de cliente de OPC.

Una vez obtenido el estado, se aplica la operación lógica en la herramienta OPC cliente, escribiendo sobre el TAGEnabled del dispositivo de árbol el estado que corresponda.

El funcionamiento de los 3 elementos, Figura 3, es directo y no se contemplan elementos de control entre la comunicación de las capas, el HMI se alimenta de la información recolectada por el OPC de las remotas de campo.

El desarrollo combina con estos tres niveles la lógica sencilla de verificación de comunicación con los dispositivos y optimiza el barrido de campo.

Esto se implementa agregando a estos 3 componentes el módulo SNMP para consultar si la comunicación con los dispositivos de campo se puede realizar, y un script que determina la escritura del canal OPC para habilitar y deshabilitar el dispositivo que corresponda. La propiedad enabled ya esta implementada en el driver OPC, por lo que se puede utilizar sin realizar ninguna modificación a el software.

En la figura 4 se ve el diagrama que describe la integración de los nuevos módulos.

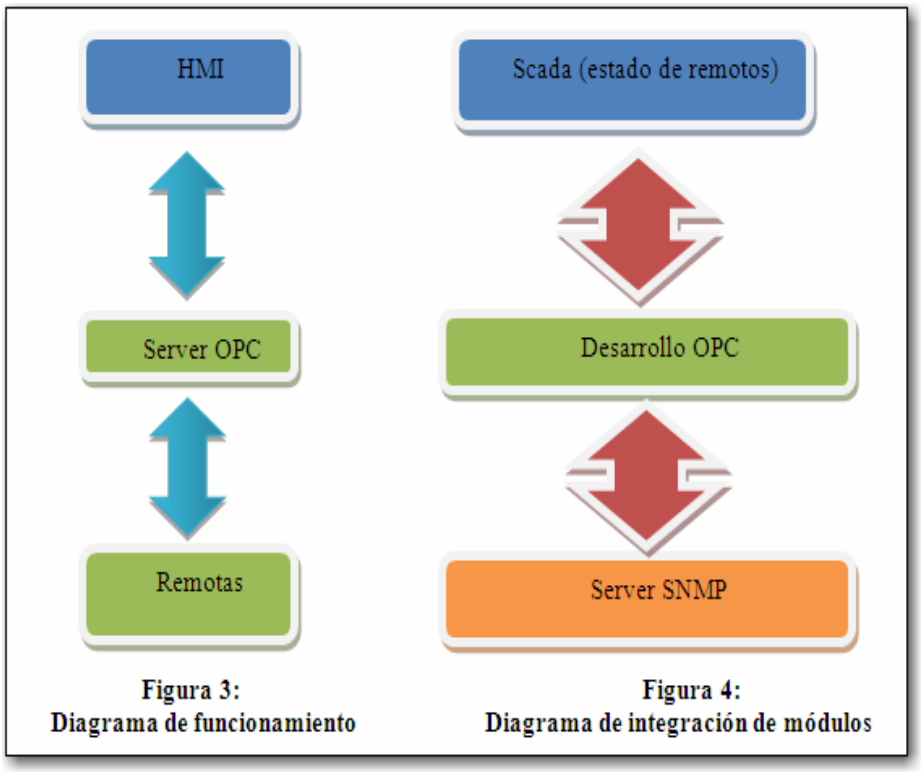

Figura 3:
Diagrama de funcionamiento

Figura 4:
Diagrama de integración de módulos

El comando a ejecutar para obtener el estado de los equipos de radio será en base a la MIB de los mismos:

Full OID 1.3.6.1.4.1.4130.2.1.1.2.3.2.0,

Esto comunica el estado de asociación de la remota en el AP wireless de la zona.

El comando para actualizar el estado en centro de control será:

"IF (Boolean Condition, Value IF true, Value if False) Condition"

Este comando llevado a las variables del sistema instalado será:

{{{{Matrikon.OPC.LufkinModbus.1\POZO_Nombre.Enabled}}= if({{snmp:Radio-Parameters ON\Ethernet Interfaces\Status("host")}},0,1)}}

La variable Matrikon es la aplicación en el servidor OPC que maneja el canal de comunicaciones del sistema remoto que se desea controlar.

7. Modelo final del sistema

El modelo final describe la interacción de los componentes.

Lo novedoso de este conjunto de acciones es que están interactuando diferentes herramientas estándares optimizadas para el mismo objetivo, que en definitiva es utilizar solo los recursos necesarios de servicios de servidor y también de comunicaciones, evitando las colas de espera y los potenciales errores en la capa de visualización de los procesos de usuario (HMI).

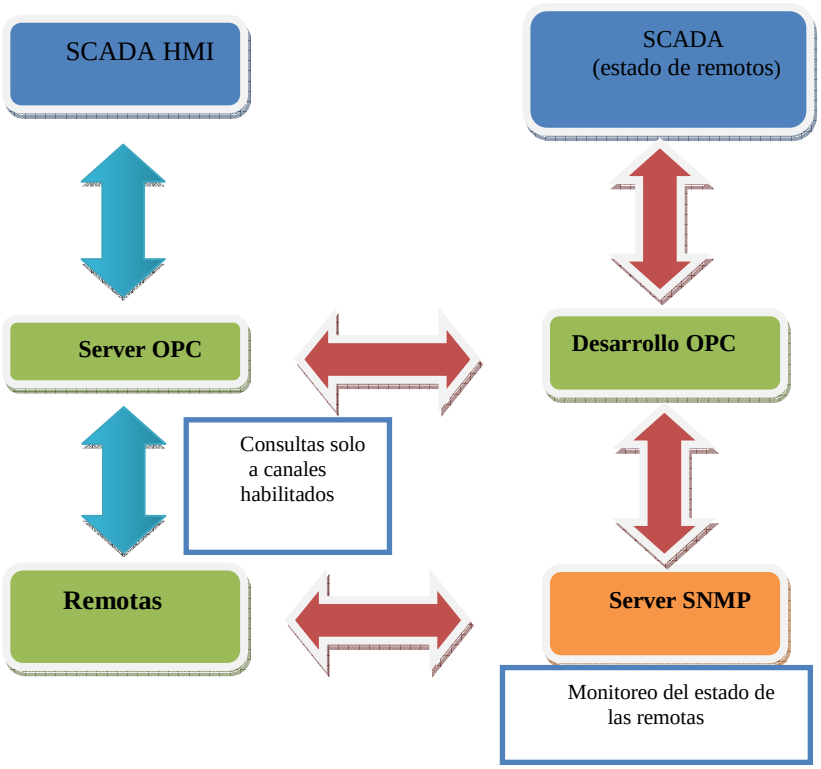

Figura 5: Diagrama final del sistema SCADA

8. Conclusiones

Muchos sistemas de supervisión y control crecen muy rápidamente sin dar oportunidad a decidir la creación de un nuevo centro de control para dichos sistemas.

Por lo tanto se siguen sumando puntos de monitoreo sin tener en cuenta que muchas veces se superan los límites para los que fueron diseñados o pensados estos sistemas.

Esto conlleva a que los mismos tengan tiempos de respuesta muy grandes, presenten fallas en la adquisición de los datos, fallas en el almacenaje, presentación y estadística de la información y otros problemas como los presentados en este trabajo.

El sistema en su conjunto deja de funcionar por falta de respuesta de los puntos remotos, lo que lleva a bloquear la totalidad de las aplicaciones debiendo inicializar los servers con las pérdidas que implica del control de la operación y el almacenamiento de los datos producidos en el tiempo que lleve recuperar los servicios.

Esto se ve agravado ante la falta de apoyo técnico oficial de los sistemas SCADA al superar todas las expectativas con que fueron creados.

Las ventajas de la solución planteada son diversas, ya que se hace uso de tecnología disponible en los equipos, pudiendo maximizar la utilización de módulos de software, unidades remotas y dispositivos de control instalados.

Esta solución permitirá tomar decisiones sobre la división en nuevos centros de control manteniendo la operativa de la totalidad del sistema con todas las ventajas técnicas y económicas que ello implica.

9. Bibliografía

1. Sinopec Argentina: http://www.sinopecgroup.com/english/Pages/index.html.
2. Matrikon- Honeywell: http://www.matrikom.com.
3. Iconics: http://www.iconics.com/home.aspx
4. Equipos de bombeos Lufkin: http://www.lufkin-arg.com/productos_ automatizacion.htm.
5. Medidor y control de flujo: www.omniflow.com
6. Protocolo Mudbus: http://www.modbus.org
7. Administración de MIB: RFC 1156 - Management Information Base for Network Management of TCP/IP-based internets.
8. SNMP: RFC 1157 - Simple Network Management Protocol (SNMP).
9. Tanenbaum, Andrews S. Sistemas de Computadoras. 4 Edición. Editorial Prentice Hall.