UNIVERSIDAD CATÓLICA ANDRÉS BELLO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

UNIDAD DE TELEMETRÍA PARA SUPERVISIÓN Y CONTROL DE SEÑALES ANALÓGICAS Y DIGITALES USANDO PROTOCOLO DE INTERNET Y BASADO EN PÁGINAS WEB Y WAP

TRABAJO ESPECIAL DE GRADO

presentado ante la

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

como parte de los requisitos para optar al título de

INGENIERO EN TELECOMUNICACIONES

REALIZADO POR Juan Andrés Goncalves Pita

PROFESOR GUIA José Gregorio Cotúa

FECHA Caracas, 24 de Septiembre de 2007

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

UNIDAD DE TELEMETRÍA PARA SUPERVISIÓN Y CONTROL DE SEÑALES ANALÓGICAS Y DIGITALES USANDO PROTOCOLO DE INTERNET Y BASADO EN PÁGINAS WEB Y WAP

TRABAJO ESPECIAL DE GRADO

presentado ante la

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

como parte de los requisitos para optar al título de

INGENIERO EN TELECOMUNICACIONES

REALIZADO POR Juan Andrés Goncalves Pita

PROFESOR GUIA José Gregorio Cotúa

FECHA Caracas, 24 de Septiembre de 2007

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA DE TELECOMUNICACIONE

UNIDAD DE TELEMETRÍA PARA SUPERVISIÓN Y CONTROL DE SEÑALES ANALÓGICAS Y DIGITALES USANDO PROTOCOLO DE INTERNET Y BASADO EN PÁGINAS WEB Y WAP

Este Jurado; una vez realizado el examen del presente trabajo ha evaluado su contenido con el resultado: .....

J U R A D O E X A M I N A D O R

Firma: Nombre: José Cotúa Firma: Nombre: INAKI MENDIJABAL Firma: Nombre: BIAGIO CAMTE

REALIZADO POR	Juan Andrés Goncalves Pita
PROFESOR GUIA	José Gregorio Cotúa
FECHA	Caracas, 24 de Septiembre de 2007

UNIDAD DE TELEMETRÍA PARA SUPERVISIÓN Y CONTROL DE SEÑALES ANALÓGICAS Y DIGITALES USANDO PROTOCOLO DE INTERNET Y BASADO EN PÁGINAS WEB Y WAP

Goncalves, Juan Andrés
juangoncalves@gmail.com

Ante la necesidad de realizar la gestión de procesos a distancia, se plantea una alternativa de sistema de monitoreo y control remoto manejado a través de equipos terminales de uso común para la población, como son: la *PC* y los equipos móviles celulares. De esta manera, se puede adquirir los datos de un proceso físico remoto y actuar sobre él para obtener una respuesta deseada a través de una página web o wap, dependiendo del equipo terminal. Utilizando un micro controlador PIC18F4620, con la capacidad de comunicarse por medio del controlador Ethernet ENC28J60 y utilizando el *stack* MODBUS/TCP, se crea la unidad remota de telecontrol capaz de transmitir los valores de las señales en sus interfaces a la base de datos de la Unidad Central de Control. Esta última, además de establecer la comunicación con la RTU, se encarga de publicar los valores contenidos en su base de datos a través de las páginas web y wap. Además, esta misma UCC a través de las aplicaciones web/wap también permite el control de las señales en los pines del micro controlador ubicado a distancia usando los formularios de las páginas. De esta manera, aprovechando el gran desarrollo en las redes basadas en TCP/IP, se puede conectar la RTU en cualquier lugar con acceso a Internet y acceder a la misma desde con una PC conectada a Internet o con un teléfono celular dentro de una red que permita navegar a través de páginas wap.

Palabras Claves: Telemetría, control, SCADA, RTU, Modbus/TCP

AGRADECIMIENTOS

Quiero agradecer a todos las personas que me apoyaron y depositaron toda su confianza en mí, sin dudarlo en ningún momento, durante la realización de este Trabajo Especial de Grado:

A mis padres, por haber sacrificado tanto para que yo pudiera lograr mis sueños, indudablemente soy lo que soy gracias a su esfuerzo y apoyo en todo momento.

A mi tutor y gran amigo, el Profesor José Gregorio Cotúa por guiarme a lo largo del TEG, apoyándome siempre con sus consejos e importantes sugerencias en todo momento.

Al Profesor, amigo y padrino de promoción, Iñaki Mendizábal, por prestarme su ayuda incondicional durante el proyecto, y a lo largo de la carrera universitaria con su apoyo y sincera amistad.

Al Profesor Uribe por compartir conmigo su sabiduría, tanto en el desarrollo de este TEG, como durante la carrera.

A los grandes compañeros, que fueron un respaldo en todo momento, haciendo que esto definitivamente valiera la pena.

A todos mis profesores, con quienes tuve el privilegio de ver clases y que con su experiencia y conocimiento me formaron como Ingeniero.

Y finalmente a Dios por iluminarme en los momentos más difíciles y por permitirme conocer a tanta gente tan especial, que sin duda alguna han formado mi ser durante todo este tiempo en la Universidad.

Juan A.

ÍNDICE GENERAL

RESUMEN ii
AGRADECIMIENTOS iii
ÍNDICE GENERAL iv
INTRODUCCIÓN vii
CAPITULO I PLANTEAMIENTO DEL PROYECTO 1
I.1 Planteamiento del problema 1
I.2 Objetivos 3
I.3 Alcances y Limitaciones 4
CAPITULO II MARCO TEÓRICO 6
II.1 *Supervisory Control And Data Adquisition* (SCADA) 6
II.1.2 Arquitectura de un Sistema SCADA 8
II.2 *Remote Terminal Unit* (RTU) 9
II.2.1 Microcontroladores 11
II.3 Unidad Central de Control (UCC) 13
II.3.1 Capa de comunicaciones con las unidades remotas 13
II.3.2 Capa de base de datos 14
II.3.3 Capa de servidor web/wap 16
II.4 Sistema de Telecomunicaciones 21
II.4.1 Protocolos del *Stack* TCP/IP 21
II.4.2 Protocolos de comunicaciones de la RTU (Modbus) 23
CAPITULO III METODOLOGÍA 26
III.1 Fase de Investigación 26
III.2 Fase de desarrollo (Servidor Web/Wap) 27
III.3 Fase de desarrollo (Base de datos) 28
III.4 Fase de desarrollo (RTU) 29
III.5 Fase de Interconexión 30

III.6 Fase de Pruebas 30
III.7 Fase de resultados, análisis y conclusiones 31
CAPITULO IV DESARROLLO 32
IV.1 Fase de Investigación 32
IV.2 Fase de desarrollo (Servidor Web/Wap) 33
IV.3 Fase de desarrollo (Base de datos) 35
IV.4 Fase de desarrollo (RTU) 36
IV.5 Fase de Interconexión y pruebas 41
CAPITULO V RESULTADOS 43
V.1 Investigaciones Teóricas 43
V.2 Desarrollo de la RTU 44
V.3 Desarrollo de la UCC 47
V.3.1 Demonio para comunicación UCC-RTU 47
V.3.2 Base de Datos en MySQL 47
V.3.3 Páginas web/wap 49
V.4 Interconexión 50
CAPITULO VI CONCLUSIONES Y RECOMENDACIONES 52
VI.1 Posibilidades de Extensión Futura 54
VI.2 Alcances del Sistema 55
BIBLIOGRAFÍA 56
ANEXO A EL MICROCONTROLADOR PIC18F4620 Y CONTROLADOR ETHERNET ENC28J60 60
1 La arquitectura PIC18F de Microchip 61
1.1 El Procesador 61
1.2 Organización de la Memoria 63
1.3 Líneas de entrada y salida. 64
1.4 Módulos auxiliares 65
2 Módulos Auxiliares externos (ENC28J60) 66
3 El PIC18F4620 67

ANEXO B DESARROLLO DE LA RTU 69
ANEXO C DESARROLLO DE LAS PAGINAS WEB/WAP 73
ANEXO D DIAGRAMAS DE BLOQUES 78
ANEXO E INTERCONEXIÓN Y PRUEBAS 82
1. Ambientes de Interconexión 83
2. Capacidad de Respuesta del Sistema 84
3. Anchos de Banda 87
4. Funcionamiento del Protocolo Modbus/TCP 88
ANEXO F REFERENCIAS TÉCNICAS 89
1. RTU 90
2. Páginas de Control 93
3. Conexión 93
ACRÓNIMOS 94

INTRODUCCIÓN

Con la revolución industrial y el avance de nuevas técnicas para el desarrollo de productos y servicios, las industrias se han visto en la necesidad de invertir en personal y dispositivos para una continua supervisión del desarrollo de los distintos procesos industriales involucrados. Inclusive, dependiendo del caso, estos procesos suelen desarrollarse en lugares remotos o incluso inaccesibles para el ser humano.

Con motivo de reducción de costos de personal y la tendencia vanguardista por parte de las industrias a adquirir tecnologías para convertir sus procesos de producción más eficientes; ha traído consigo la necesidad del desarrollo de sistemas capaces de: a) adquirir los datos del proceso físico, y b) actuar sobre el proceso para obtener una respuesta deseada a distancia. Actualmente se han desarrollado sistemas para el procesamiento, envío y recepción de señales analógicas y/o digitales de campo al personal interesado; los cuales suelen ser equipos complejos y manejados por personal especializado en el área.

Dado todos los beneficios que trae la telemetría a las empresas; se ha encontrado la gran utilidad que tiene la supervisión y control a distancia en aplicaciones como: sistemas contra incendio, sistemas de seguridad, sistemas de riego, hogares y edificios inteligentes, etc.

Sin embargo, dada la complejidad en el uso de estos equipos, es necesario rediseñar estas herramientas para que sean sencillas para el uso del público en general, actualizadas tecnológicamente y de fácil integración a plataformas ya existentes. Son estos elementos los que motivan este Trabajo Especial de Grado con el objetivo de: desarrollar una unidad de telecontrol y medición de señales que sea manejado a través de equipos terminales de uso común para la población, como lo son la *PC* y los equipos móviles celulares.

Este documento está estructurado en capítulos. En el Capítulo I se describe el planteamiento del proyecto; su justificación; los objetivos generales y específicos delimitados dentro de los alcances y limitaciones. Para el desarrollo de este trabajo se requirió de una investigación teórica relativa a los sistemas de supervisión y control de señales analógicas y digitales, así como los protocolos de comunicación necesarios para su implementación, descritos brevemente en el Capítulo II del Marco Teórico, el cual busca situar al lector dentro del contexto teórico necesario.

A partir de la investigación teórica, se desarrolló la unidad de telemetría para la supervisión y control, capaz de comunicarse vía protocolo de Internet con la unidad central de control y supervisión del dispositivo remoto. El *software* de la unidad central de control también es desarrollado dentro del marco de este trabajo y entre sus funciones están: la publicación en una página web / wap de los resultados de esta supervisión y que a la vez permita controlar las señales de salida de la unidad remota.

Una vez planteados el problema y los objetivos a cumplir en el desarrollo de este Trabajo Especial de Grado (TEG), se trabajó bajo una metodología para el desarrollo de los objetivos descrita en el Capítulo III del Marco Metodológico que, según Bavaresco (1992, p.26), es una investigación aplicada debido a que: "pretende dar solución a un problema concreto en un periodo de tiempo corto" a través del desarrollo de las actividades comprendidas en las 7 fases descritas en el Capítulo IV de Desarrollo y cuyos resultados se pueden apreciar en el Capítulo V, respondiendo al cumplimiento de los objetivos planteados.

Ya en el Capítulo VI se presentan las conclusiones y recomendaciones que se desprenden de los resultados obtenidos a lo largo de un año de investigación aplicada en la elaboración de este TEG, dando a conocer las posibles aplicaciones del producto resultante y sus posibles mejoras para quienes deseen desarrollar soluciones alternativas a las propuestas en este documento.

Para quienes deseen indagar más sobre el tema, en el Capítulo VII se da a conocer la bibliografía consultada para la elaboración de este trabajo. Además, en el Capítulo VIII se presentan un conjunto de anexos que amplían los puntos tratados a lo largo de este TEG en cuanto al: microcontrolador utilizado y sus módulos externos; los esquemas de los algoritmos programados en la unidad remota y en la central, junto con su respectivo esquema de comunicación, y al final se presentan los resultados de las pruebas de interconexión del sistema en distintos ambientes de prueba.

Queda presentado la estructura y el propósito de este TEG, que busca masificar la implementación de la telemetría y el control a distancia a través de equipos terminales comunes (PC y teléfonos celulares) con la creación de un sistema que cuenta con una arquitectura que permite una gran flexibilidad para adaptarse a las necesidades de cualquier ambiente de propósito general.

CAPITULO I

PLANTEAMIENTO DEL PROYECTO

I.1 Planteamiento del problema

En la actualidad existe una clara tendencia, por parte de las industrias, a optar por procesos de automatización y reemplazo de la mano de obra por equipos mecánicos, eléctricos, electrónicos y sistemas automatizados para la óptima utilización de los recursos existentes en los procesos de fabricación de productos y prestación de servicios. Así pues, con los avances de la tecnología se ha logrado desarrollar estos equipos, sin embargo, esta automatización debe venir acompañada de una continua observación del desenvolvimiento de todos los elementos involucrados durante la producción o préstamo del servicio por la industria.

La adquisición de datos para supervisión y el control a distancia se han convertido en parte integral de cualquier actividad industrial. La necesidad de una continua supervisión requiere de una inversión en personal y dispositivos necesarios para medir, registrar y guardar el desarrollo de los distintos procesos en la industria. En algunos casos estos procesos suelen implementarse en lugares remotos, lo que implica la necesidad de un sistema capaz de (a) adquirir en tiempo real los valores de las principales variables o condiciones de los procesos físicos a distancia y (b) actuar sobre el proceso para obtener una respuesta deseada.

Incluso, esta tendencia de supervisión y control ha pasado de ser, no solo una necesidad en industrias; sino que además es utilizada en otros ambientes como sistemas contra intrusión y hurto; sistemas contra incendio; hogares y edificios inteligentes; entre otros.

Teniendo en cuenta los antecedentes anteriormente descritos y sumando el hecho de que cada vez más el usuario común -aquella persona que carece de conocimientos técnicos en el campo de la telemetría y control a distancia- requiere de herramientas sencillas, actualizadas tecnológicamente, de fácil integración a plataformas ya existentes, y que sean capaces de controlar y supervisar eventos a distancia; han sido todos estos citados elementos los que motivaron a la elaboración de este Trabajo Especial de Grado. Trabajo que tuvo como propósito fundamental el desarrollo de una unidad remota de telecontrol y adquisición de datos, manejado por medio del protocolo de Internet mediante PC y equipos móviles celulares.

La idea estuvo inspirada en una tendencia de la población mundial al acceso a equipos móviles celulares y a la Internet cada vez más creciente. Asimismo, es común hoy en día que las empresas, e incluso los hogares, cuenten con redes LAN con acceso a Internet.

La labor del ingeniero en telecomunicaciones para el desarrollo de este producto fue fundamental, ya que este proyecto estuvo envuelto en una integración de diferentes estándares y protocolos en prácticamente todas las capas del modelo de referencia OSI. Este Trabajo Especial de Grado involucró: partir desde el estudio de los sistemas de telemetría y control existentes en la actualidad, y así poder adquirir el conocimiento necesario para llegar hasta la elaboración de un equipo; el cual permita el fácil y económico acceso a la población en general de un producto de alta tecnología y con la flexibilidad de adaptarse a las necesidades del consumidor.

El desarrollo de este producto se fundamentó en un esquema de investigación científico, a fin de poder cumplir con los objetivos que se describen a continuación.

I.2 Objetivos

I.2.1 Objetivo General

Desarrollo de una unidad de telemetría para supervisión y control de señales analógicas y digitales, usando protocolo de Internet y basado en páginas web y wap.

I.2.2 Objetivos Específicos

- Realizar una investigación teórica relativa a los sistemas de supervisión y control de señales analógicas y digitales usando unidades de telemetría.

- Hacer una investigación teórica relativa a los protocolos de comunicación necesarios para la implementación de un sistema de supervisión y control vía protocolo de Internet y basado en páginas web y wap.

- Desarrollar el *hardware* y el *software* de la unidad de telemetría para la supervisión y control de señales tanto analógicas como digitales. Incluyendo un módulo de comunicación vía protocolo de Internet.

- Programar una aplicación que funciona como unidad central de control y supervisión del dispositivo de telemetría para la publicación en páginas web/wap de los resultados de esta supervisión y que a la vez permite controlar las señales de salida de la unidad de telemetría.

I.3 Alcances y Limitaciones

Este trabajo especial de grado está confinado bajo los siguientes alcances y delimitaciones:

I.3.1 Alcances del Trabajo

Este TEG se fundamentó en el estudio, desarrollo y puesta en funcionamiento de una unidad de telemetría, la cual es manejada a través de cualquier PC que esté conectado a Internet y soporte las más recientes versiones de navegadores Web tales como: *Internet Explorer* (desde la versión 6), *Mozilla Firefox* (desde la versión 2), *Opera* (desde la versión 9).

También contempla la posibilidad de poder controlar y monitorear las señales conectadas a las interfaces de una unidad de telemetría por medio de cualquier teléfono móvil en cualquier parte del mundo, siempre y cuando este teléfono soporte la tecnología WAP y la red celular brinde el servicio.

En este TEG se incluyó la elaboración de una unidad remota capaz de manejar: 8 señales digitales: 4 de entrada y 4 de salida, junto con la posibilidad de trabajar con: 4 señales analógicas de entrada y una señal analógica de salida. Vale la pena destacar que esta unidad remota puede estar conectada en cualquier parte del mundo, siempre y cuando se cuente con acceso a Internet y su respectiva alimentación eléctrica (120V AC ó 5V DC).

Así como la RTU (*Remote Terminal Unit*) contempla la posibilidad de ser conectada en cualquier lugar; la unidad central de control también posee esta propiedad, dado que se referencia la dirección IP de esta central a un nombre a través de la resolución de DNS, permitiendo que la RTU ubique a la central por su nombre.

I.3.2 Limitaciones del Trabajo

Este Trabajo Especial de Grado no incluyó el desarrollo de un programa especial para que el teléfono móvil pudiera controlar y supervisar la unidad remota. Los teléfonos con los cuales se hicieron las pruebas soportan WAP y se realizaron en la ciudad de Caracas, donde todas las operadoras dan soporte de este servicio.

La unidad de telemetría posee la capacidad de manejar solo los protocolos TCP, UDP, IP, ARP, DHCP, ICMP, DNS, todos estos como cliente y Modbus/TCP/IP como servidor. Los citados protocolos son suficientes y necesarios para las especificaciones de este trabajo. Además, la unidad de telemetría solo cuenta con una dirección MAC definida y la capacidad de adquirir una dirección IPv4 vía DHCP. La interfaz física Ethernet es a través de un conector RJ-45.

Es importante destacar que la PC establecida como Unidad Central de Control debe tener los requerimientos mínimos de memoria, procesador, interfaces, etc. para operar bajo el sistema operativo *Windows XP*. A su vez, este SO debe incluir el paquete de protocolos de red básico necesarios para el funcionamiento del servidor de páginas web/wap descritos en el Capítulo de Desarrollo. Además, la Unidad Central de Control (UCC) debe poseer al menos una interfaz física Ethernet con su dirección MAC definida y única, junto con su respectiva dirección IPv4 pública. Esta última restricción es necesaria a fin de asociar la IP del UCC a un nombre DNS valido para toda la red de Internet.

En el caso de la RTU, esta solo posee la mencionada interfaz Ethernet y un puerto RS-232, este último se utiliza solo para el terminal de configuración del RTU. Para efectos de este TEG, todas las pruebas de interconexión y funcionamiento de los distintos elementos que conforman este sistema se realizaron en una LAN controlada con acceso a Internet y en la ciudad de Caracas; a fin de asegurar el servicio de Wap.

CAPITULO II

MARCO TEÓRICO

A continuación, este marco teórico pretende situar al lector en el contexto del desarrollo de este TEG; partiendo desde la investigación de las características y funcionamiento de los sistemas de telemetría comunes, haciendo énfasis en el sistema SCADA. Y de allí dar a conocer las características, funcionamiento y componentes que conforman todo el sistema de supervisión y control a distancia desarrollado en este TEG, el cual está dividido en tres subsistemas: la unidad remota de telecontrol, la unidad central de control y el sistema de telecomunicaciones que los interconecta.

Existe una clara tendencia, por parte de las industrias, hacia la automatización de procesos capaces de hacer con mayor eficacia ciertas tareas; Consecuentemente con este proceso de automatización, ha crecido también la necesidad de una constante supervisión de sus labores. Es a partir de esta necesidad que nacen las estaciones remotas de control y adquisición de datos como una medida económica y eficaz, integrando sistemas capaces de adquirir datos del proceso físico bajo control y que a la vez pueda actuar sobre proceso para obtener una respuesta deseada.

II.1 *Supervisory Control And Data Adquisition* (SCADA)

De esta manera, nacen los Sistemas de Adquisición de Datos, Supervisión y Control de procesos a distancia denominados por las siglas en inglés SCADA, los cuales deben garantizar tres operaciones básicas:

Adquisición de datos: Para leer, transmitir y almacenar la información de las variables de interés (señales de campo).

Supervisión: Para analizar la evolución de estas variables.

Control: Para modificar la evolución del proceso, cambiando los valores de alguna de estas variables a distancia.

Generalmente los SCADA están diseñados para funcionar sobre computadores en los procesos de producción o cualquier otra actividad que requiera control (sistemas de seguridad, edificios inteligentes, sistemas contra incendio o de emergencia); proporcionando comunicación a los dispositivos de campo (controladores autónomos, autómatas programables, microcontroladores, etc.). De esta manera, el sistema permite el control de las actividades remotas desde la pantalla del computador u otro equipo que ofrezca una interfaz al usuario final.

Según Uribe (2004) es importante destacar que "a diferencia de otros sistemas de control, un SCADA funciona primordialmente a "lazo abierto", siendo indispensable la actividad de un operador humano para emitir las ordenes que se ejecutan". Sin embargo, Uribe añade que también ciertas operaciones se pueden realizar a "lazo cerrado", bien sea localmente -en donde los dispositivos remotos automáticamente establecen las acciones- o por medio de una estación maestra.

Los Sistemas SCADA según Álvarez, Vázquez, Sierra, Fernández, y Machiran (2003) se pueden dividir según su propósito en:

Propósito Específico: permiten una alta especialización en la aplicación a la cual están dedicados, sin embargo, dado que están diseñados para solo un propósito en específico; son menos flexibles y realizan un número limitado de funciones.

Propósito General: en contaste al anterior, ofrecen gran flexibilidad y se adaptan a un gran número de aplicaciones, pero por lo general exigen más recursos de los que realmente utilizan.

II.1.2 Arquitectura de un Sistema SCADA

Según Daneels y Salter (2000) la arquitectura de un sistema SCADA la podemos dividir en varios elementos, entre los que destacan:

Arquitectura de hardware

Se distinguen dos capas básicas en el hardware un sistema SCADA: la "capa del cliente": que se encarga de la interacción entre la máquina y el usuario y la "capa del servidor de datos" que maneja la mayor parte de las actividades del proceso en el control de datos. Estas capas se observan con mayor detalle en la siguiente figura.

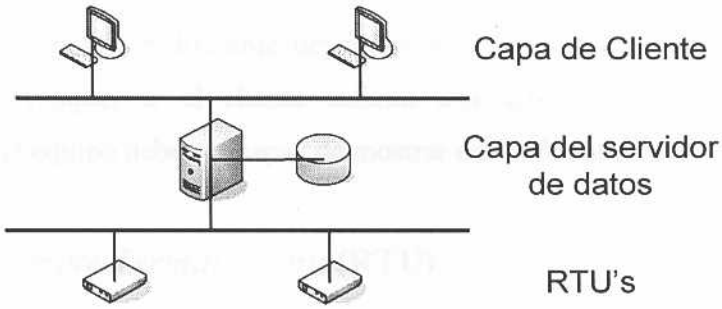


Figura 1. Arquitectura típica de hardware

Arquitectura del software

El software se soporta en un sistema multiproceso y sobre una base de datos en tiempo real (RTDB) situada en uno o más servidores. Los servidores son responsables de la adquisición de datos y control (ejemplo: los reguladores de las interrogaciones, alarmas, cálculos, registros y archivos). Por lo general la arquitectura del software esta soportada bajo una serie de protocolos interconectados necesarios para la comunicación entre los distintos elementos que conforman el sistema y también para la presentación y control de las variables a través de las interfaces de usuario.

Arquitectura de comunicaciones

Se puede destacar los siguientes tipos de comunicaciones:

- **Comunicación interna:** la comunicación del Servidor-cliente y del servidor-servidor es, en general, un sistema basado en un publicador y un manejador de eventos comunicados mediante buses especiales o redes LAN (Autómatas Industriales, 2006). De esta manera, cuando un parámetro del equipo al cual se está monitoreando cambia; inmediatamente se le informa al cliente cuando lo solicita.

- **Acceso a dispositivos:** Las estaciones centrales interrogan a los dispositivos en un periodo de tiempo definido por el usuario. Este periodo de interrogación puede ser diferente dependiendo de la naturaleza del dispositivo a monitorear. Aunque, si el cliente solicita una actualización inmediata de un dispositivo, el equipo debe ser capaz de mostrar esta información a tiempo.

II.2 *Remote Terminal Unit* (RTU)

Una RTU (Unidad Remota de Telecontrol) es un dispositivo instalado en un lugar remoto, el cual recoge señales de campo y los transforma en un formato que sea transmisible a una estación central. Estas unidades también recogen la información del dispositivo principal (peticiones de control) y pone los procesos en ejecución que son dirigidos desde el cliente.

Las RTU se equipan de interfaces de entrada para detectar o medir y de interfaces de salida para el control. Todas estas deben tener la capacidad de manejar señales tanto analógicas como digitales. Es necesario que las RTU cuenten también con puertos de comunicaciones para conectarse con la estación central en modo *full duplex*. Analizando en detalle cada una de las interfaces de adquisición de datos (monitoreo) y control, tenemos según Gordon y Deon (2004, cap. 2, p. 22) los diferentes tipos de interfaces:

Entradas Digitales. Estas interfaces se encargan de monitorear las señales digitales binarias de campo y de procesarlas para ser interpretadas y empaquetadas por la RTU para su posterior transmisión. Por lo general, este tipo de señales se asocian a: estados de interruptores, válvulas, motores; alarmas; entre otras señales de naturaleza binaria.

Salidas Digitales. Las señales binarias de salida en estas interfaces son resultado del procesamiento de los comandos hacia los controladores de campo. Estas interfaces pueden contar con relés de estado sólido que transmiten un pulso a otro equipo terminal con la finalidad de ejecutar o cambiar el estado del equipo o elemento conectado. Generalmente estas señales son asociadas a: comandos de apertura y cierre de interruptores; encendido/parada de motores; válvulas; etc.

Entradas Analógicas. Estas interfaces cuentan con convertidores analógicos/digitales, con la finalidad de digitalizar las señales fluctuantes de campo y poder ser procesadas por la RTU para su transmisión. Ejemplo de la naturaleza de estas señales son: temperatura; intensidad de corriente o de voltaje; presión; peso; entre otras señales fluctuantes de baja frecuencia que, a través de transductores, son transformadas las magnitudes de los fenómenos físicos y químicos en señales equivalentes eléctricas analógicas.

Salidas Analógicas. Generalmente utilizadas en el envío de señales para regular elementos como: presión; temperatura; luminosidad; velocidad de motores; ente otros equipos que admiten valores fluctuantes. Estos dispositivos se basan en el mismo procedimiento de las entradas analógicas, pero envían un valor escalable al equipo terminal conectado.

Para los efectos de este TEG, se utilizó un microcontrolador PIC18F4620 de la compañía Microchip como RTU, debido a que son económicos; robustos; con la suficiente capacidad de procesamiento, memoria y velocidad para operar como

estación remota; contemplan distintas interfaces de comunicación y además, poseen un módulo para conexión vía Ethernet. A continuación se detalla más sobre estos microcontroladores, con el fin de apreciar su capacidad de operar como una RTU, tal y como se ha descrito anteriormente.

II.2.1 Microcontroladores

Un microcontrolador es, según Usategui y Martínez (2003, cap.1, p.1), un circuito integrado programable o chip que integra las tres unidades funcionales básicas de un computador: CPU, memoria y unidades de E/S, tratándose entonces de un computador completo en un solo circuito integrado pero con prestaciones limitadas, debido a que desde un principio han sido concebidos para el control de máquinas (teléfonos, autos, A/A, juguetes, sistemas de encendido, electrodomésticos, líneas de ensamblaje, etc.) o incluso otros controladores. Sin embargo, debido a su gran versatilidad, hoy en día son usados para otras aplicaciones de mayores exigencias, como es el caso de este TEG.

Dadas sus características, los MCU[1] son una de las opciones más comunes a la hora de implementar sistemas embebidos. Entendiéndose por sistemas embebidos como: los dispositivos utilizados para controlar las operaciones de diversos equipos, en donde todos o la mayoría de sus componentes están integrados en una sola tarjeta. Estos sistemas son fabricados de forma robusta y con un alto grado de integración, contando con la mayoría de las ventajas de un computador convencional; pero incorporando solo los recursos estrictamente necesarios para su labor.

Existen muchas compañías fabricantes de microcontroladores, pero en el desarrollo de este TEG se optó por los MCU de la familia PIC18F de la compañía

[1] MCU o microcontrolador

Microchip (www.microchip.com). El cual es uno de los fabricantes de microcontroladores más populares de 8-bit y tienen cientos de diferentes modelos.

Estos MCU tienen la capacidad de trabajar hasta a 40Mhz y ejecutar instrucciones cada 4 ciclos de reloj, es decir, a 10Mips. Un PIC18F típico posee en su interior un generador de *clock* integrado; una pequeña cantidad de memoria RAM, flash y EEPROM. Para hacerlos funcionar solo se necesita: un programa que se carga en el PIC para que ejecute el algoritmo especificado; alimentación (típicamente 3.3V ó 5V) y un cristal de sincronización (opcional).

Los PIC18F disponen también de: una gran variedad de dispositivos de entrada/salida; convertidores de analógico a digital; temporizadores; varios UART y buses de interfaz serie especializados como: I^2C y CAN. Además, Microchip ofrece módulos externos al PIC para aplicaciones específicas como controladores Ethernet, para dotar de conectividad a los microcontroladores.

Para más información sobre la arquitectura de estos versátiles MCU y sobre todas las especificaciones del modelo 18F4620 y del controlador Ethernet ENC28J60, utilizados para la construcción de la RTU, véase el Anexo A donde se profundiza en el tema.

II.3 Unidad Central de Control (UCC)

Para este TEG se ha diseñando una unidad central de control (UCC), como la que se puede ver en la Figura 2, la cual comprende 3 capas fundamentales con funciones específicas.

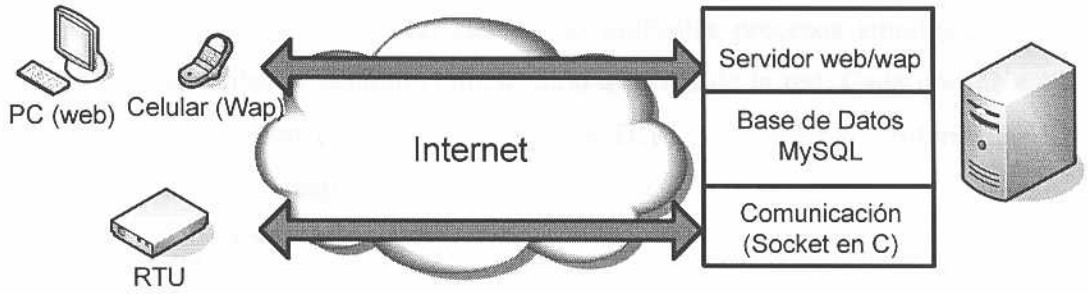


Figura 2. Esquema de comunicaciones y de la unidad central de control

Con el fin de cumplir con los objetivos de la unidad central de control, fue necesaria la implementación práctica de todo un conjunto de protocolos, programas y gestores de bases de datos que serán comentados a continuación según las especificaciones de cada capa de la UCC:

II.3.1 Capa de comunicaciones con las unidades remotas

Como el nombre indica, esta capa tiene como función establecer la comunicación entre la UCC y la unidad remota, usando protocolo de Internet, para poder monitorear y controlar los equipos conectados a las interfaces de la RTU.

Sockets en C

Para el establecimiento de la conexión a nivel de software con la remota, se implementó la programación de *sockets* en lenguaje C. Los *sockets* constituyen una interfaz de entrada-salida que permite la comunicación entre varios procesos que pueden estar ejecutándose en diferentes máquinas (*Departamento de Tecnoloxías da*

Información e as Comunicacións de la Universidade da Coruña, 1997, ap.). Específicamente los *sockets* para TCP/IP permiten la comunicación de dos procesos que estén conectados a través de una red TCP/IP.

En una red de este tipo, cada máquina está identificada por medio de su dirección IP aunque, por comodidad se les asignan nombres a cada una de las máquinas. En cada *host* se están ejecutando múltiples procesos simultáneamente, algunos de los cuales se estarán comunicando a través de la red. Cada uno de estos procesos se asocia con un número de puerto TCP, para poder así diferenciar los distintos paquetes que reciba la máquina.

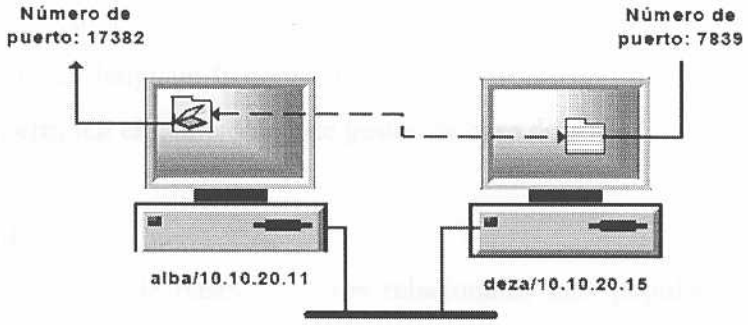


Figura 3. Establecimiento de conexión identificando dirección IP y puerto (TCP/IP).
Tomado de: (*Departamento de Tecnoloxías da Información e as Comunicacións de la Universidade da Coruña*, 1997, p. 3)

Entonces, un *socket* se identifica particularmente por: dirección IP + número de puerto, en consecuencia, una comunicación entre sockets se identifica unívocamente mediante: identificador de socket origen + identificador de socket destino.

II.3.2 Capa de base de datos

Esta capa comprende dos funciones muy importantes: la primera de ellas es almacenar el estado de la unidad remota, llevando a la vez el registro de todo el historial de las interfaces conectadas a la remota. La segunda función de esta capa es

ofrecer un puente de intercomunicación entre la capa de comunicación con la unidad remota y la capa del servidor web/wap. Este puente trabaja de la siguiente manera:

El programa en C (demonio) recoge los datos adquiridos por la remota y guarda estos valores en la base de datos; estos mismos registros son utilizados por la página web/wap dinámica para su respectiva publicación. De igual manera, las órdenes de control provenientes desde la página web/wap son guardadas en la misma base de datos que utiliza el demonio, para de esta manera, enviar las órdenes de control a la estación remota.

Para esta labor se utiliza el gestor de base de datos MySql ya que tanto, el demonio escrito en lenguaje C como, las páginas web/wap escritas en PHP poseen librerías que permiten el manejo de este gestor de base de datos.

MySql

Es el servidor de bases de datos relacionales más popular, desarrollado y proporcionado por MySQLAB. Empresa cuyo negocio consiste en proporcionar servicios en torno al servidor de bases de datos MySQL. Una de las razones para el rápido crecimiento de popularidad de MySQL es que se trata de un producto *Open Source*, y por lo tanto, va de la mano con este movimiento (Gutiérrez, 2006).

Una base de datos no es más que una colección estructurada de datos. El gestor de bases de datos MySQL consiste en: un sistema cliente/servidor que se compone de un servidor SQL multihilo; varios programas clientes y bibliotecas; herramientas administrativas y de una gran variedad de interfaces de programación (API). Se puede obtener también una biblioteca multihilo que se enlaza con otras aplicaciones para obtener un producto más pequeño; más rápido y más fácil de manejar. Para obtener información técnica más detallada, consulté la guía de referencia de MySQL (MySql LAB, 2006).

II.3.3 Capa de servidor web/wap

Esta capa tiene como función: la publicación de los estados de las señales conectadas a los puertos de la unidad remota. Además, de servir como interfaz al usuario para el control de las señales en los terminales de la RTU.

Este servidor tiene la capacidad, por medio del uso de PHP, de publicar páginas web para los terminales PC y, a la vez, mostrar esta misma información a cualquier equipo móvil celular que cuente con la tecnología wap. A continuación se presentan los distintos protocolos, intérpretes y funciones con las que cuenta esta capa:

WEB

Viene del *"World Wide Web"* y se podría traducir como la telaraña mundial refiriéndose al conjunto de todas las páginas que pueden consultarse en Internet. La Web o WWW es un sistema de hipertexto que funciona sobre Internet. Para ver la información se utiliza una aplicación llamada navegador web, que se encarga de extraer elementos de información (llamados documentos o páginas web) de los servidores web (o sitios) y mostrarlos en la pantalla del usuario.

El usuario puede entonces seguir hiperenlaces que hay en la página a otros documentos o, incluso, enviar información al servidor para interactuar con él. A la acción de seguir hiperenlaces se le suele llamar "navegar" por la Web. No se debe confundir la Web con Internet, donde la última es la red física mundial sobre la que circula la información.

Del mismo modo que se puede distinguir entre una intranet (una inter-red) y la Internet; uno puede referirse a "una web" como una página, sitio o conjunto de sitios que proveen información por los medios descritos, y "la Web" que es la enorme e interconectada web disponible prácticamente en todos los sitios de Internet.

La arquitectura del *World-Wide Web.* Según el W3C *Working Draft* (Booth, Champion, Ferris, Hasa, McCabe, Newcomer, y Orchard, 2003) el diseño del WWW sigue el modelo cliente-servidor: un paradigma de división del trabajo informático en el que las tareas se reparten entre un número de clientes que efectúan peticiones de servicios de acuerdo con un protocolo, y un número de servidores que las atienden. En la Web, las estaciones de trabajo son clientes que demandan hipertextos a los servidores. Para poner en marcha un sistema como éste es necesario un conjunto de protocolos y lenguajes, los cuales se indican a continuación:

HTTP (*HyperText Transfer Protocol*). Es el protocolo de alto nivel del WWW que rige el intercambio de mensajes entre clientes y servidores del Web, esto es: desde un nodo de origen a uno de destino, que podría ser un texto o parte de un texto; una imagen; un sonido; una animación; fragmento de vídeo o cualquier tipo de información en formato electrónico.

HTML (*HyperText Markup Language*). Es un lenguaje que permite representar hipertextos, donde se incluye la información sobre la estructura y el formato de representación y especialmente para indicar origen y destino de saltos hipertextuales. Contiene la especificación de estructuras del texto, por ejemplo: títulos; encabezados; límites de los párrafos; listas de elementos. HTML también comprende otros elementos importantes como: Objetos multimedia (imágenes o sonido) y conexiones hipertextuales a otros objetos de la red (enlaces a otras páginas). Todo este valor añadido al texto se codifica como etiquetas llamadas *tag* que se insertan en el propio texto.

URL: (*Uniform Resource Locutor*). Representa de un modo compacto la localización y el método de acceso a cualquier recurso de la red. Los URL son de gran importancia debido a que no sólo hay más de dos millones de ordenadores conectados a las miles de redes que forman la Internet; sino que también existen múltiples protocolos o diferentes formas de acceder a la información (FTP, gopher,

http, etc..). De esta manera, los URL aportan esos dos datos esenciales: dónde se encuentra un recurso y cómo se puede acceder a él. En la actualidad existen esquemas definidos para todos los servicios, por solo citar los más comunes:

FTP (*File Transfer Protocol*)	ftp://usuario:contraseña@host:puerto/ruta;tipo=<*typecode*>
http (*HyperText Transfer Protocol*)	http://<host>:<puerto>/<ruta>?<*searchpart*>
mailto (correo electrónico)	mailto:<rfc822-addr-spec>

Para el caso de las páginas wap, se emplea también una URL que lo identifica como pagina wap, a continuación se profundiza este protocolo y los distintos elementos que lo conforma.

WAP *Wireless Application Protocol*

Traducido como protocolo de aplicaciones inalámbricas, es un estándar abierto internacional para desarrollos que utilizan las comunicaciones inalámbricas, por ejemplo acceso a servicios de Internet desde un teléfono móvil. Según *Open Mobile Alliance* (OMA, 2006), WAP se define como un entorno de aplicación y una pila de protocolos para aplicaciones y servicios accesibles a través de terminales móviles. Todas estas especificaciones son definidas por la *Open Mobile Alliance / WAP Forum*, permitiendo que los desarrolladores diseñen aplicaciones de interconexión para terminales móviles, típicamente teléfonos.

Tecnología. En la versión 1 de WAP, definida en 1999, el lenguaje de presentación de contenidos es el WML (*Wireless Markup Language*). La pila de protocolos de WAP 1 no es compatible directamente con la de Internet: WSP (*Wireless Session Protocol*), WTP (*Wireless Transaction Protocol*), WTLS (*Wireless Transport Layer Security*), y WDP (*Wireless Datagram Protocol*) son la pila de protocolos necesarios para la integración con el Internet.

La incompatibilidad de la pila de protocolos WAP1 con la Internet exige la presencia de un nodo pasarela para hacer de intermediario en la comunicación entre

un terminal WAP y un servidor de contenidos WAP residente en Internet. El siguiente esquema da muestra del proceso para el establecimiento de la conexión en la petición por parte de un equipo móvil de una página wap, donde se evidencia la importancia de la pasarela en la adquisición de contenidos vía wap.

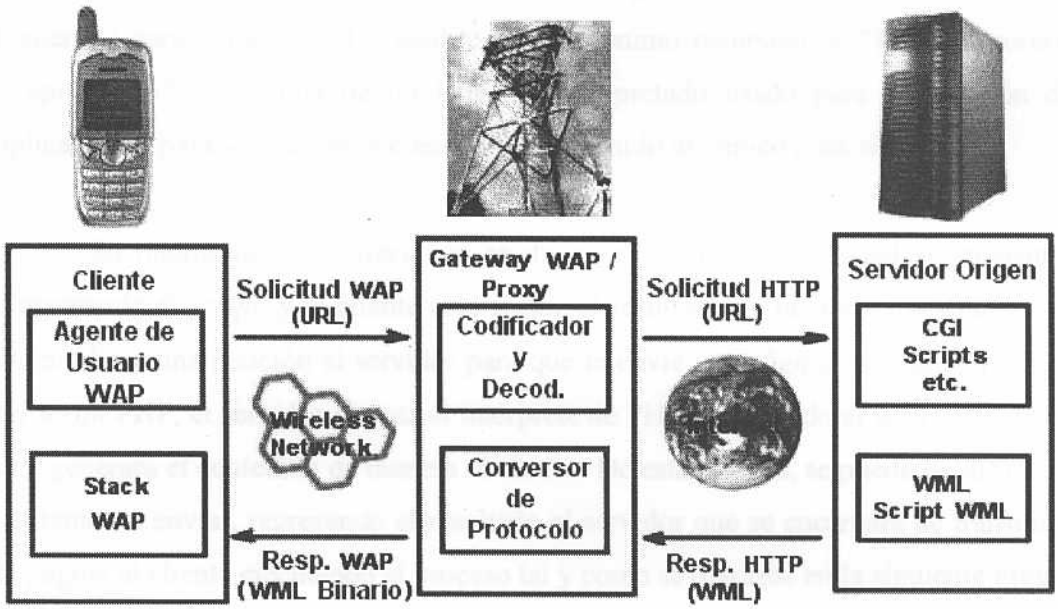


Figura 4. Esquema de petición de páginas wap. Traducido de: MobileFish (2007)

WML. Es un lenguaje de marcas similar al HTML, el cual es compatible con XML 1.0. Una página WML es como una página HTML en la que hay una serie de cartas (páginas), al conjunto de estas cartas se les suele llamar baraja. Los navegadores WAP solo pueden mostrar una carta al mismo tiempo. Entre las características principales de WML se pueden citar:

- Soporte para imágenes y texto, con posibilidad de texto con formato.
- Tarjetas agrupadas en barajas.
- Posibilidad de navegar entre cartas y barajas de la misma forma que se navega entre páginas web.
- Manejo de variables y formularios para el intercambio de información entre el teléfono celular y el servidor.

Sin embargo, para la creación de las páginas dinámicas, bien sean wap o web, es necesario la programación a través del lenguaje PHP.

PHP

Es un lenguaje de programación usado generalmente para la creación de contenido para sitios web. El nombre es el acrónimo recursivo de "PHP: *Hypertext Preprocessor*" y se trata de un lenguaje interpretado usado para la creación de aplicaciones para servidores, o creación de contenido dinámico para sitios web.

Su interpretación y ejecución se da en el servidor, en el cual se encuentra almacenado el *script*, y el cliente sólo recibe el resultado de la ejecución. Cuando el cliente hace una petición al servidor para que le envíe una página web, generada por un *script* PHP, el servidor ejecuta el intérprete de PHP procesando el *script* solicitado que generará el contenido de manera dinámica. De esta manera, se puede modificar el contenido a enviar, regresando el resultado al servidor que se encargará de transmitir la página al cliente ejecutando el proceso tal y como se describe en la siguiente Figura 5. (webestilo, 2006).

Figura 5. Procedimiento de generación de páginas dinámicas con PHP.

Nota. Tomado de webestilo (2006)

II.4 Sistema de Telecomunicaciones

En este apartado se profundiza sobre los distintos protocolos y estándares involucrados en la comunicación entre los elementos que conforman el sistema SCADA.

Como se ha comentado a lo largo de este documento, se conecta la unidad remota con la UCC a través de la interfaz física y de enlace Ethernet. Para dotar de conectividad a nivel de red se utiliza el protocolo de Internet (IP) a fin de establecer una conexión TCP para la transferencia segura de datos entre los citados elementos. Además, la UCC está encargada de aceptar las conexiones de los usuarios finales, para el control y monitoreo de la unidad remota por medio de las páginas web/wap, empleando también los protocolos anteriormente citados.

Cabe destacar que los paquetes que envía y recibe la RTU se corresponden al protocolo Modbus encapsulados en tramas TCP (Modbus/TCP) y direccionados por IP. A continuación se explica con más detalle la arquitectura de todos estos protocolos:

II.4.1 Protocolos del *Stack* TCP/IP

IP, *Internet Protocol.*

La RFC791 (Postel, 1981a) da las especificaciones que se tuvieron en cuenta en el desarrollo del protocolo de Internet. IP fue diseñado para implementarse en sistemas interconectados de computadoras basado en el intercambio de paquetes. Este protocolo permite enviar bloques de datos, llamados datagramas, desde una máquina (*host*) a otra. Estos *hosts* son identificados por una dirección de longitud fija. IP también provee capacidades de fragmentación y reensamblado de paquetes, si es necesaria la transmisión por redes cuyo tamaño de paquete máximo sea muy pequeño.

IP no incluye ningún método para garantizar la transferencia de los datos de un extremo a otro de la red, ni dispone de control de flujo o algún otro servicio comúnmente encontrado en protocolos *host-to-host*. Para ello IP necesita de las bondades de TCP para contar con una conexión segura.

TCP, *Transport Control Protocol.*

En la RFC793 (Postel, 1981b) se explican las características de TCP. Allí se describe que TCP es pensado para sistemas interconectados de redes de computadoras basados en conmutación de paquetes. Es un protocolo orientado a la conexión que garantiza el enlace y entrega de datos de un extremo a otro.

TCP fue diseñado para encajar dentro de un modelo basado en capas, justo por arriba del Protocolo de Internet (IP), el cual provee a TCP un medio para enviar y recibir segmentos de datos de longitud variable. TCP fue desarrollado principalmente para ofrecer un protocolo que permita establecer circuitos lógicos virtuales; garantizando la conexión; controlando el flujo de los datos y estableciendo seguridad. TCP parte de la base de que la capa inferior no ofrece estas características. A grandes rasgos, TCP brinda:

Confiabilidad. TCP es capaz manipular paquetes con datos perdidos, modificados, duplicados o enviados fuera de orden.

Control de Flujo. TCP permite que el receptor informe al transmisor la cantidad de datos que es capaz de recibir.

Multiplexación. Para permitir que muchos procesos de un mismo *host* puedan usar comunicaciones basadas en TCP simultáneamente (puertos).

Conexión. La confiabilidad y el control del flujo de datos necesitan que TCP inicialice y mantenga información sobre el estado de cada flujo de datos.

II.4.2 Protocolos de comunicaciones de la RTU (Modbus)

Modbus

Este protocolo de capa de aplicación define una estructura del mensaje que los controladores reconocen y usan, con independencia del tipo de redes sobre la que se comuniquen. Según Gordon y Deon (2004), Modbus describe el proceso que usa un controlador para pedir acceso a otro dispositivo; cómo responderá a las peticiones desde otros dispositivos y cómo se detectarán y notificarán los errores. Además, establece un formato común para la disposición y contenido de los campos del mensaje.

Transacciones sobre Redes Modbus

Los controladores se comunican usando una técnica "maestro – esclavo", en la cual sólo un dispositivo (el maestro) puede iniciar transacciones (llamadas peticiones). Los otros dispositivos (los esclavos) responden suministrando al maestro el dato solicitado o realizando la acción solicitada en la petición, tal y como se aprecia en la siguiente figura que es un esquema sencillo que representa el ciclo de petición – respuesta de maestro – esclavo.

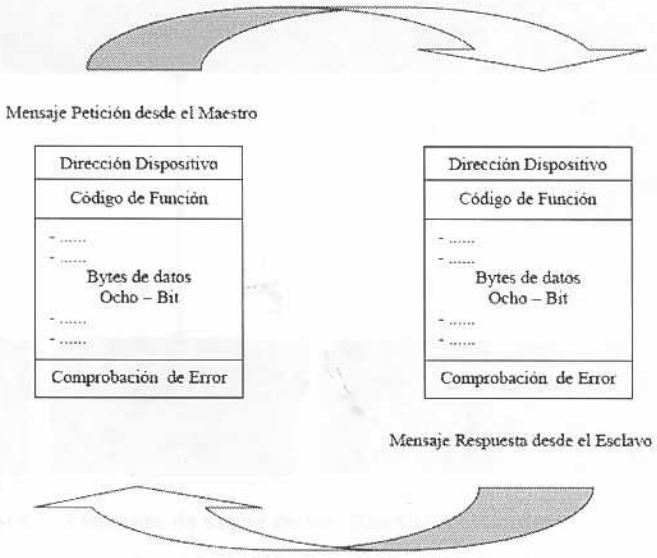


Figura 6. Ciclo de petición – respuesta de maestro - esclavo

Entre los dispositivos maestros típicos se incluyen: los procesadores centrales y los paneles de programación; para el caso de este TEG será el UCC. Los Esclavos típicos son: los PLC o también, como es el caso de este trabajo, se usan microcontroladores.

Modbus / TCP

El Modbus/TCP significa que el protocolo de Modbus está siendo utilizado sobre TCP/IP. El Modbus/TCP es una red de Ethernet abierta que ha sido especificada por la organización Modbus-IDA en cooperación con el destacamento de fuerzas de Ingeniería del Internet (IETF) como estándar del Internet del RFC.

El funcionamiento de una red Modbus/TCP es altamente dependiente del tipo y diseño de la red Ethernet que se utiliza y del funcionamiento de los procesadores en las interfaces de comunicaciones de los respectivos dispositivos. Como se puede ver en la Figura 7, Modbus/TCP está soportado bajo una mayor cantidad de capas con relación a su versión original, lo que le proporciona mayor seguridad y confiabilidad; pero también mayor retardo debido a la cantidad de procesos involucrados.

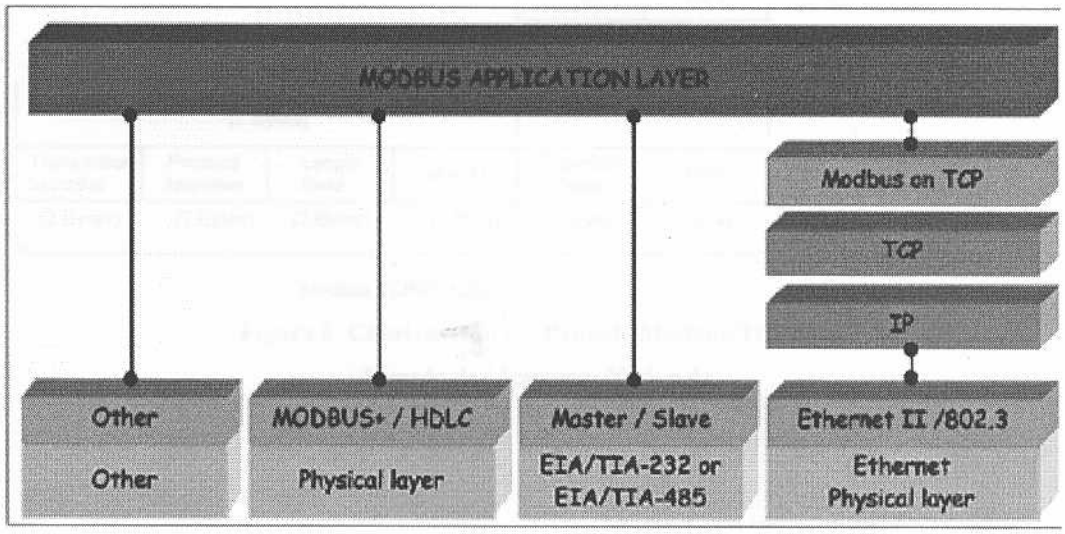


Figura 7. Esquema de capas de los diferentes estándares de Modbus.

Tomado de (Modbus-IDA, 2004, P. 15)

Modbus/TCP es un acercamiento pragmático para utilizar Ethernet como medio de transmisión de datos para los usos de monitoreo y control. Los costes adicionales de la infraestructura de la red se pueden justificar por las ventajas de Ethernet tales como: el gran número de estaciones en una red y por las ventajas sustanciales debido a la transferencia adicional del Internet, correo electrónico y de archivos que puede utilizar el mismo medio que ofrece control y señalización.

Prácticamente, Modbus/TCP es colocar el paquete Modbus tradicional dentro de una trama TCP, con la excepción que no es necesaria la dirección y el *cheksum* del propio paquete Modbus, dado que estos elementos de seguridad y direccionamiento ya los proporciona la dupla TCP/IP, tal y como se puede observar en la siguiente figura. Para aplicaciones Modbus el puerto TCP 502 está reservado para tal fin (Modbus-IDA, 2004, P. 5).

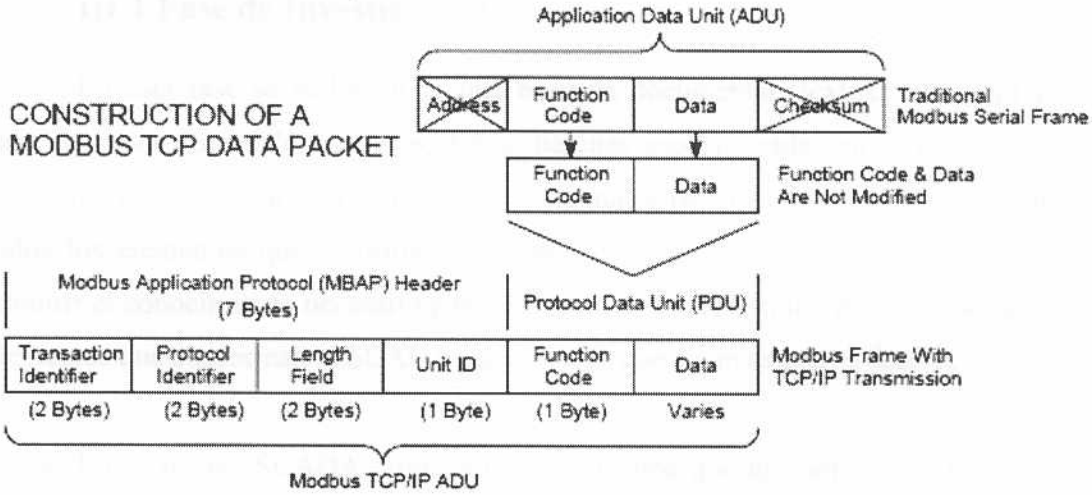


Figura 8. Construcción del Paquete Modbus/TCP/IP.

Tomado de (Acromag, 2005, p.4)

CAPITULO III

METODOLOGÍA

Tipo de Investigación

Una vez planteados el problema y los objetivos a cumplir en el desarrollo de este TEG, se trabajó bajo una metodología para el desarrollo de los objetivos. Según Bavaresco (1992, p.26), el propósito de la investigación es aplicada: ya que "pretende dar solución a un problema concreto en un periodo de tiempo corto". En este caso es: la creación de una unidad de telemetría y control de señales tanto analógicas como digitales, manejado vía IP mediante PC y equipos móviles celulares. Las actividades se dividieron en 7 fases:

III.1 Fase de Investigación

En esta fase se realizó toda una revisión documental (textos, bibliografías, tesis de grado, manuales, revistas, foros, páginas especializadas en Internet, entre otros) junto con consultas a profesores y personal especializado en el campo sobre todos los elementos que conforman el sistema SCADA. Todo esto con el fin de adquirir el conocimiento necesario para, en las fases de desarrollo, poder elaborar los elementos que conforman el SCADA. Los tópicos que se investigaron fueron:

- Los sistemas SCADA: arquitectura, elementos que lo conforma, estándares, protocolos, ingeniería, desarrollos previos, etc.
- Las unidades remotas de telecontrol (RTU): arquitectura, protocolos de comunicaciones, rangos de voltaje, corrientes y características de las señales de campo, interfaces de comunicación; de control y supervisión.
- Microcontroladores, específicamente los PIC fabricados por la compañía Microchip. Se centró la investigación en: su arquitectura, procesadores, velocidades,

capacidad de memoria, interfaces y módulos de comunicaciones, puertos, módulos para tratamiento de señales, rangos de voltaje, corriente, etc. Toda esta investigación tuvo como fin: poder determinar si estos microcontroladores son capaces de realizar las funciones de una RTU tal y como se investigo en el punto anterior.

- Desarrollo web: arquitectura, programas, lenguajes y protocolos necesarios para el desarrollo de páginas web estáticas y dinámicas.
- Desarrollo wap: tecnología wap; elementos necesarios para el desarrollo de páginas wap; dispositivos con los que debe contar un equipo móvil para la presentación de páginas wap; protocolos WML, WMLScript, WTAI, entre otros.
- Bases de datos: funcionamiento; gestores de bases de datos; formatos de bases de datos aplicados a los sistemas SCADA.

III.2 Fase de desarrollo (Servidor Web/Wap)

Esta fase contempló toda la metodología necesaria para poner en funcionamiento el servidor de páginas web/wap. También tuvo lugar en esta fase la creación de las páginas web y wap que se alojan en este servidor. En el desarrollo de esta fase se realizaron las siguientes actividades:

- Comparación entre los distintos programas, investigados en la fase anterior, para servidores web y wap existentes en el mercado; para adquirir los más adecuados.
- Instalación y configuración del servidor web/wap; alojando adecuadamente las páginas wap y web estáticas y dinámicas. En el caso de las páginas web, son accesibles desde cualquier computadora conectada a Internet que cuente con las últimas versiones de los exploradores *Internet Explorer, Mozilla Firefox* u *Opera* (desde las versiones 6, 2 y 9 respectivamente). Para las páginas wap, el servidor se configuró para ser accesible desde cualquier teléfono que cuente con la última versión del conjunto de protocolos Wap v1 bajo una red móvil celular que lo soporte.

- Comparación entre los distintos programas para el desarrollo de páginas, tanto web, como wap existentes en el mercado; junto con la adquisición de los programas más adecuados para este trabajo.
- Estudio de los lenguajes de programación necesarios para el desarrollo de las páginas web y wap, utilizando los programas adquiridos y poniendo estos conocimientos en práctica en la creación de las páginas.

III.3 Fase de desarrollo (Base de datos)

En esta etapa se realizaron todas las actividades necesarias para poner en funcionamiento una base de datos. En esta BD se almacenan todos los valores de las señales presentes en las interfaces de la unidad de telemetría y a la vez es accesible desde el servidor web/wap; para la publicación de estos valores registrados mediante las páginas web y wap. En el desarrollo de esta fase se contempló las actividades que se describen:

- Comparación entre los distintos gestores de bases de datos existentes en el mercado, con el fin de adquirir el más adecuado para este trabajo.
- Instalación y configuración del gestor adquirido, de tal manera que la BD es accesible desde: el programa que se comunica con la remota (demonio en c), el cual almacena los valores de las señales presentes en las interfaces de la unidad de telemetría. También esta base de datos se configuró para que pueda comunicarse con el servidor web/wap y así poder publicar los valores almacenados mediante las páginas alojadas.
- Adquisición, estudio e implementación de las API[2] del gestor de base de datos adquirido para la elaboración de los programas en C y PHP, necesarias para: el demonio que se comunica con la remota y para las páginas web y wap dinámicas respectivamente.

[2] API: *Application Programming Interface*, es un conjunto de especificaciones de comunicación entre componentes software.

III.4 Fase de desarrollo (RTU)

En esta fase se desarrolló y puso en funcionamiento la unidad de telemetría para la supervisión y control remoto, utilizando un microcontrolador que cumple con las especificaciones necesarias para funcionar como una RTU investigada en la primera fase. El desarrollo de esta fase contempló las siguientes actividades:

- Comparación entre los distintos PIC existentes en el mercado, para el encargo desde Estados Unidos del MCU más adecuado para la realización de las labores de una RTU de propósito general.
- Encargo desde Estados Unidos del controlador Ethernet que dota de conectividad al MCU utilizando Ethernet (IEEE 802.3).
- Diseño de todo el esquema circuital necesario para el funcionamiento del PIC. Este esquema contempló también la interconexión del PIC con el controlador Ethernet y la adaptación de las interfaces de medición de señales y control del PIC.
- Aplicación del estudio del lenguaje de programación del MCU, C18 de Microchip, en el desarrollo del algoritmo en el PIC para el control y supervisión de las señales conectadas en las interfaces; junto con el respectivo procesamiento y almacenamiento de estas señales en el PIC.
- Programación de todo el *stack* TCP/IP en el microcontrolador, junto con el algoritmo para su comunicación con el controlador Ethernet, asegurando la efectiva conexión entre el PIC y la UCC.
- Programación del *stack* Modbus para la comunicación entre la unidad Central de Control (UCC) y la RTU bajo este protocolo de petición y respuesta.

III.5 Fase de Interconexión

Tal y como el nombre lo indica, esta fase contempló toda una serie de actividades necesarias para la interconexión entre los distintos elementos que conforman el sistema SCADA. Las actividades que se realizaron en esta fase fueron:

- Programación del demonio en C, utilizando *socket,* para la comunicación entre la unidad remota y la UCC. Este programa, además de manejar un *Stack* TCP/IP necesario para el *socket*, también es capaz de operar bajo el protocolo Modbus para su correcto funcionamiento como unidad maestra. Este mismo programa a través de una API puede comunicarse con el gestor de base de datos y así poder almacenar allí los valores que se encuentran en las interfaces de la unidad remota.
- Interconexión y asignación de direcciones IP a la RTU; a la UCC y al Terminal final de usuario (PC) dentro de una red LAN controlada con acceso a Internet para sus respectivas pruebas.
- Verificación de la conexión por separado de los sistemas RTU - UCC y UCC – Terminal (PC) tanto, a nivel de hardware como de software (ICMP). Junto con la verificación de la conexión de todos los sistemas juntos, incluyendo la conexión UCC-Terminal (Celular) solo en cuanto a la presentación de las páginas wap.
- Verificación, mediante analizadores de protocolos, del correcto funcionamiento de los protocolos involucrados en la comunicación RTU-UCC (Modbus, TCP, IP, ICMP, ARP). Este mismo procedimiento se efectuó en el tramo UCC-Terminal.

III.6 Fase de Pruebas

En esta etapa se llevaron a cabo las distintas pruebas a los elementos, por separado y en conjunto, que conforman el sistema SCADA. Estas pruebas también fueron desarrolladas en distintos ambientes para determinar las limitaciones que tiene el sistema. Para todo esto, se realizaron las siguientes actividades:

- Verificación de la capacidad del RTU, UCC y Terminal de usuario (PC) para adquirir direcciones IP, DNS, *gateway* y máscara por medio del servidor DHCP.
- Pruebas de la respuesta adecuada por parte del RTU (esclavo) a las diferentes peticiones del UCC (maestro).
- Pruebas sobre la frecuencia de muestreo de las señales en las interfaces de la unidad remota, analizando cuales son las frecuencias adecuadas para los distintos tipos de señales que se supervisan y controlan en estos sistemas. Teniendo en cuenta las limitaciones de procesamiento del PIC y de la calidad de servicio de la red.
- Pruebas de estrés a la unidad remota y al UCC, haciendo bombardeos de paquetes durante tiempos determinados para evaluar las capacidades de procesamiento de estos sistemas y adecuar sus límites recomendados.
- Evaluación del comportamiento, en distintos ambientes de interconexión, de los elementos del sistema SCADA: distintas topologías de interconexión; conexiones a nivel de LAN y WAN, etc.
- Verificación del correcto refrescamiento de las páginas web y wap según el periodo establecido por el usuario.
- Confirmación de la correcta publicación en las páginas de los valores de las señales presentes en las interfaces de la RTU.
- Verificación de la presencia, en los puertos de la RTU, de los valores dispuestos como control por parte del usuario desde las páginas web y wap.

III.7 Fase de resultados, análisis y conclusiones.

A partir de los valores obtenidos de las pruebas realizadas en la fase anterior, se extrajeron los resultados de los experimentos y con estos valores se realizaron los análisis y conclusiones sobre el funcionamiento del sistema. A partir de todos estos resultados, análisis y conclusiones se elaboraron las debidas recomendaciones para el correcto uso y funcionamiento de todo el sistema SCADA. Tales recomendaciones están contenidas en este documento en el Capítulo de Conclusiones y Recomendaciones.

CAPITULO IV

DESARROLLO

En este capítulo se detallan las actividades realizadas para la implementación práctica de los elementos que conforman el SCADA descrito a lo largo de todo este documento, destacando los procesos involucrados y las dificultades que se tuvieron que sortear en cada una de las siguientes fases:

IV.1 Fase de Investigación

Dado que en este TEG lo que se quiere es rediseñar los tradicionales sistemas de supervisión y control a distancia, fue necesario tener conocimiento sobre los sistemas de telemetría y control tradicionales: protocolos, características de las RTU y la arquitectura del sistema en conjunto. A partir de toda esta información, se pensó en distintas soluciones para el desarrollo de un sistema de monitoreo y control más accesible al público y que cumpliera con las características de los sistemas tradicionales.

Tras varias consultas con profesores y a partir de los conocimientos adquiridos durante la carrera, se optó por la implementación de un microcontrolador como corazón de un sistema embebido que hace todas las funciones de una RTU, tal y como se ha descrito en capítulos anteriores. Para el caso de los terminales de usuario se eligió el PC y teléfonos móviles a través de páginas web y wap respectivamente, debido al gran porcentaje de población mundial que está familiarizado con estas interfaces de presentación. Todos estos elementos anteriormente citados también formaron parte de la investigación teórica, a fin de conocer la mejor manera de integrarlos y formar un sistema SCADA tal y como el estudiado anteriormente, contando con el respaldo de base de datos para el almacenamiento de históricos.

IV.2 Fase de desarrollo (Servidor Web/Wap)

Tras conocer las especificaciones para la creación y publicación de las páginas web y wap, se procedió a realizar una comparación entre los distintos programas para servidores tanto web como wap existentes en el mercado, entre los cuales se encuentran:

	Velocidad	Memoria	Costo	Servicios
Apache	Veloz	Considerable	Gratuito	Jsp, threads, Unix, API, soporte IPv6, pág. de error personalizadas
IIS	Veloz	Considerable	Gratuito	FTP, SMTP, NNTP, HTTP, HTTPS, API, IPv6, pág. de error personalizas
Cherokee	Rápido	Muy ligero	Gratuito	HTTPS, pág. de error personalizadas
Lighttpd	Sumamente Rápido	Mínimo uso	Gratuito	CGI, SCGI Y fastCGI
Thttpd	Rápido	Ligero	Gratuito	JPEG, pág. de error personalizadas

	Lenguaje del Servidor	Software	SO	Protocolo
Apache	PHP, PERL, Python, Ruby, ASP	*Open Source* (libre)	MacOS, Linux, BSD, Solaris, Unix, Windows	HTTP
IIS	ASP, ASP.NET, PHP, PERL	No libre	Windows	HTTP
Cherokee	PHP, PERL, Python, Ruby	*Open Source* (libre)	MacOS, Linux, BSD, Solaris, Windows	HTTP
Lighttpd	PHP, PERL, Python, Ruby on Rails	*Open Source* (libre)	MacOS, Linux, BSD, Solaris, Unix, Windows	HTTP Y URL
Thttpd	PHP, ASP	*Open Source* (libre)	FreeBSD, SunOS4, Solaris2, BSD/OS, Linux, OSF	HTTP, no HTTPS

Tabla 1. Comparación entre los servidores web/wap más conocidos.

Datos tomados de (Baca, 2006)

Tras analizar todas las características presentadas en la tabla, se optó por emplear el servidor HTTP *Apache*, el cual: funciona adecuadamente bajo los protocolos investigados en la fase anterior; permite alojar páginas dinámicas tanto web como wap diseñadas en php; muy popular por ser software libre y con las prestaciones necesarias para este TEG. Es importante destacar el hecho de que cualquier servidor web puede adaptarse para publicar páginas WML: tan sólo es necesario configurar el servidor para que asocie las extensiones WML y WMLS a los correspondientes tipos MIME[3].

Adquirido el software anteriormente mencionado, se instaló bajo el SO Windows y se pudo configurar adecuadamente, luego de haber indagado en manuales de instalación (Apache Software Foundation, 2006), foros y páginas en Internet (Gracia, 2006).

Otro aspecto muy importante dentro de esta fase es el contenido almacenado en este servidor. Para ello, primero se realizó una comparación entre los distintos programas para el desarrollo de páginas tanto web como wap existentes en el mercado, entre los cuales destacan: *Macromedia Dreamwaver, Microsoft Frontpage, Adobe Golive, Nokia WML Studio* y *Raptor*. De esta manera, y luego de un estudio comparativo se escogió el programa *Microsoft Front Page*: el cual posee un ambiente de desarrollo que permite diseñar páginas de manera similar a un editor de texto como *Microsoft Word*; mientras automáticamente va creando el respectivo código HTML. Además, permite editar este código HTML a fin de agregar *scripts* PHP necesarios para la presentación dinámica de páginas.

[3] MIME: Multipurpose Internet Mail Extensions. Protocolo de envío de información no codificada en código ASCII

Aunque *Macromedia Dreamwaver* también es un excelente programa, la creación de páginas en *Frontpage* es más intuitiva, rápida y fácil para quien se inicia en el diseño web, obteniendo un resultado profesional. Así pues, se configuró este programa para poder trabajar con paginas PHP permitiendo de esta manera, pero bajo ciertas restricciones, la creación de las paginas wap también.

En esta fase fue necesario estudiar, entre otros lenguajes, el PHP: con el fin de lograr contenidos dinámicos y también para poder hacer la conexión con el gestor de base de datos. También se estudiaron los lenguajes HTML y WML con el fin de diseñar los contenidos estáticos de las páginas, web y wap respectivamente, bajo ciertos requerimientos especiales y además para saber dónde ubicar adecuadamente los *scripts* PHP.

IV.3 Fase de desarrollo (Base de datos)

Entre los gestores de bases de datos considerados para el desarrollo de este TEG figuran: dBase, Fox Pro, Window Base. Sin embargo, los más destacados son los que se presentan en la siguiente tabla comparativa:

Gestor	MySQL	Oracle
Nombre de la empresa	Mysql AB	Oracle Corporation
1° Lanzamiento público	1996	1977
Ultima Versión Estable	5.0	10g release2
Tipo de Licenciamiento	GPL o Propietario	Propietario
SO Soportados	Windows, Linux, MacOS, Solaris, otros	Windows, Linux, MacOS, Solaris, otros
Interfaces	C, C++, Delphi, PERL, Python, Java, PHP, ASP	C, Delphi, PERL, Java, PHP, ASP
Conectores	.Net, Obdc, Jdbc	.Net, Obdc, Jdbc
Otras características	Ofrece niveles de seguridad para datos, copia de seguridad, importación y exportación de datos, bloqueo de registros, procesamiento distribuido de transacciones, índices, vistas.	

Tabla 2. Comparación entre los gestores MySQL y Oracle

Datos tomados de (Burbano, 2006)

Se eligió MySQL, el cual aparte de ser GPL[4], es un sistema de gestión de base de datos, multihilo y multiusuario sumamente conocido y muy utilizado en páginas web hechas en PHP y almacenadas en servidores Apache.

Este sistema de gestión que desarrolla MySQLAB como software libre, tiene la gran ventaja de contar con varias API que permiten, a aplicaciones escritas en diversos lenguajes de programación, acceder a las bases de datos MySQL.

Tras la decisión por MySQL, se instaló y configuró adecuadamente el gestor de base de datos logrando escribir código compatible tanto para, el programa que se comunica con la remota (demonio en c), como para las páginas web/wap utilizando PHP. Sin embargo, no bastó con configurar adecuadamente el gestor; también se consiguieron las API para PHP y C. En el caso de este último lenguaje de programación fue bastante difícil conseguir la API, dado que no es muy común hacer llamados a este gestor en programas hecho en C. A pesar de esto, se logró crear la API tras conseguir información en páginas especializadas en la Web (Pozo, 2005).

IV.4 Fase de desarrollo (RTU)

En esta fase de desarrollo de la RTU, como se ha comentado anteriormente, se utilizó un PIC18F. Sin embargo, no todos los microcontroladores de esta familia eran aptos para cumplir con las exigencias que implica una RTU. A fin de escoger el más apropiado, se partió de la siguiente tabla comparativa; donde se presentan las características de los MCU PIC18F de mayor desempeño.

Tras estudiar los diferentes modelos se decidió por el PIC18F4620. Dadas las características que se describen en el anexo A, este MCU cuenta con la velocidad; capacidad de memoria; interfaces; módulos de comunicación; puertos; módulos para tratamiento de señales y demás características necesarias para operar como una RTU

[4] GPL: *General Public License*

tal y como se conoce. Sobre todo el factor de capacidad de memoria es uno de los elementos más críticos, dado que el algoritmo necesario para que el MCU trabaje como una RTU consume prácticamente un 95% de su capacidad.

Modelo	Costo al mayor	Tipo de Mem. de programa	Kb	KWords	Data EEPROM	RAM	I/O	Canales ADC
PIC18F4620	$5.44	Flash	64	32	1024	3968	36	13
PIC18F4525	$5.01	Flash	48	24	1024	3968	36	13
PIC18F4680	$6.08	Flash	64	32	1024	3328	36	11

Modelo	Muestreo ADC (kmps)	Interfaces	Max. Velocidad MHz	Vdd Min.	Vdd Max.	Cant. Pines	Encapsulados
PIC18F4620	100	EUSART MI²C Compatible/SPI	40	2	5.5	44	40/PDIP 44/QFN 44/TQFP
PIC18F4525	100	EUSART MI²C Compatible/SPI	40	2	5.5	44	40/PDIP 44/QFN 44/TQFP
PIC18F4680	100	EUSART MI²C Compatible/SPI	40	2	5.5	44	40/PDIP 44/QFN 44/TQFP

Tabla 3. Comparación entre los MCU PIC18F de mayor desempeño

Datos tomados de (microchip, 2007a)

Definido el microcontrolador a utilizar, se encargó desde Estados Unidos el PIC y el controlador Ethernet ENC28J60 para poder dotar de conectividad al MCU. Vale la pena destacar que Microchip cuenta con varios MCU que ya tienen integrado un controlador Ethernet 10BaseT (Tabla 4) sin embargo, debido a su encapsulado para montaje superficial, no era práctico para la realización de prototipos sobre *protoboard* necesario para este TEG.

Integrado	Memoria	KBytes	I/O	Canales ADC	Vel. Muestreo ADC (kmps)	*Buffer* RAM Eth (Kb)	Pines	Empaques
PIC18F67J60	Flash	128	39	11	100	3808	64	64/TQFP
PIC18F87J60	Flash	128	55	15	100	3808	80	80/TQFP
PIC18F97J60	Flash	128	70	16	100	3808	100	100/TQFP

Tabla 4. MCU PIC18F con controlador Ethernet integrado

Datos tomados de (microchip, 2007a)

Otras compañías como *Freescale* ofrecen MCU, controladores Ethernet y ambos integrados en un mismo hardware (Tabla 5) con iguales o mayores prestaciones que los ofrecidos por *Microchip*. Sin embargo, dado el conocimiento adquirido en la carrera en la implementación de soluciones con estos MCU y su abundante información en la web, fueron los factores que impulsaron a adoptar al PIC18F4620 como el corazón del sistema embebido que conforma el RTU.

Integrado	Paquete	A/D	Características Adicionales	Max F (MHz)	Flash (Mb)	RAM (Kb)	Interfaces
MC908GP32CPE	PDIP 40	8	Watchdog OSC/Timer,Real-Generador de *Clock* interno	32	32	512	IRSCI, SPI, I2C
MC9S12NE64CPVE	Montaje Sup.	8	MAC (FEC) 10/100 Ethernet	-	64	8000	I2C, SCI, SPI
MCF5270AB100	Montaje Sup.	-	MAC (FEC) 10/100 Ethernet, 16Kb cache	50	-	64000	I2C, SCI, SPI, USB

Tabla 5. Comparación de MCU Freescale

Datos tomados de (freescale, 2007)

En la tabla se puede ver que el MC908GP32CPE es un MCU de 8 bits con prestaciones parecidas a la de un PIC18F, sin embargo, no cuenta con un controlador Ethernet integrado como los otros dos MCU de la tabla. Para tal caso se puede utilizar el integrado de la familia MPC860T como controlador Ethernet 10BaseT. Vale la pena destacar que el microcontrolador MCF5270AB100 es de 32 bits *ColdFire®*. Para más información visite www.freescale.com.

Además del microcontrolador, la RTU está compuesta por:

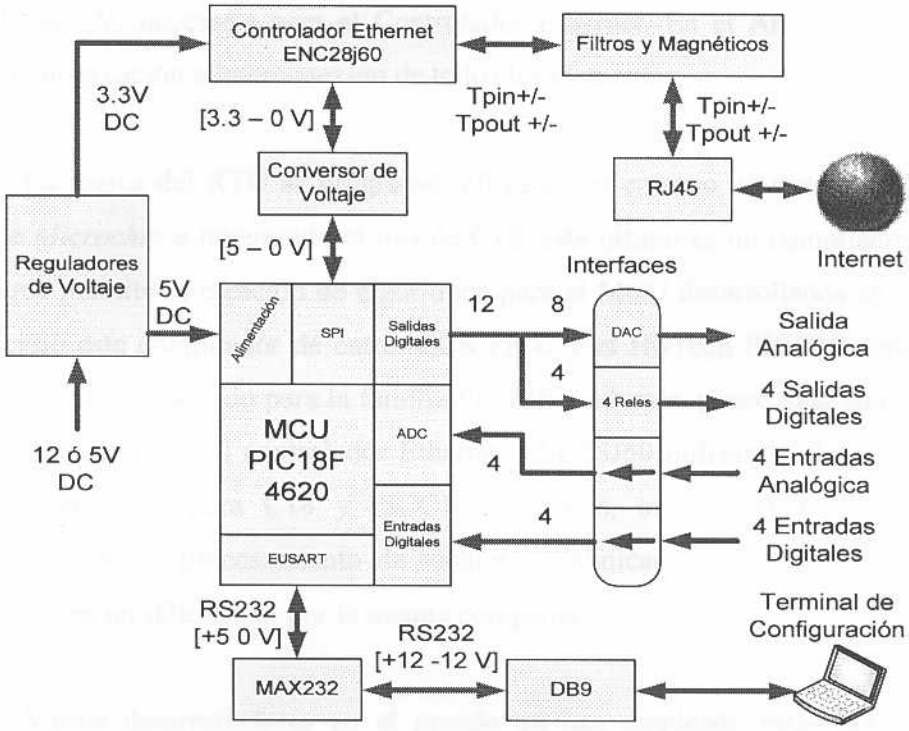


Figura 9. Esquema de bloques del RTU

Como se aprecia en la figura, el sistema cuenta con un DAC0832 de *National Semiconductor* que permite la salida de señales analógicas de entre 0 a 5V; 4 relés que permiten el control digital; un conversor de voltaje (MAX232) para poder establecer comunicaciones seriales según el estándar RS-232 por medio de un conector DB9; conversor de voltaje entre el PIC y el controlador Ethernet ENC28J60 (compuerta AND 78HCT08) para dotar de comunicación al MCU vía terminal RJ-45 y utilizando filtros y magnéticos dispuestos para adaptar las señales que entran y salen del MCU aislando el circuito de los elementos externos conectados.

En cuanto a la alimentación del circuito se emplearon los reguladores: LM7805 a fin de garantizar los 5V al: PIC; Max232; arreglo Darlington para la operación de los relés; DAC; Opam LM318 (salida del DAC) y a la compuerta AND que se emplea como conversor de voltaje entre el Controlador Ethernet y el PIC. Además, se empleó el regulador LM3940-3.3 que garantiza 3.3V a partir de una

entrada de 5V, necesario para el Controlador Ethernet. En el Anexo B se aprecia mejor la disposición e interconexión de todos los elementos.

La lógica del RTU se programó utilizando el entorno de desarrollo *MPLAB IDE* de *Microchip* e integrando el uso de C18, este último es un compilador de alto nivel que permite la creación de algoritmos para el MCU desarrollados en ANSI-C. Se decidió este compilador de entre: CCS PICC y el Hi-Tech PICC18 dado que el escogido es especializado para la familia PIC18F y además, posee toda una API para la comunicación con el controlador Ethernet ENC28J60 utilizando el *Stack* TCP/IP 3.75 (desarrollado para C18 y PICC18). Además, ofrece funciones para otras aplicaciones en el procesamiento de señales, comunicaciones seriales y otras más integradas en un IDE hecho por la misma compañía Microchip.

Varios desarrolladores en el mundo ya han empleado estos controladores Ethernet para sus soluciones, y a partir de sus investigaciones se pudo extraer valiosa información de sus sitios web, como es el caso de (Amodio, 2006), pudiendo aprovechar el contenido de su página como punto de partida en esta etapa del trabajo. Realizando ciertas modificaciones al esquema circuital que Jorge Amodio presenta en su página, se ha logrado dotar de comunicación al microcontrolador y desarrollar la base del algoritmo para la comunicación vía TCP/IP. Añadiendo los respectivos algoritmos para codificación y empaquetamiento Modbus/TCP y junto con los algoritmos de control y monitoreo, se cargó en el PIC el respectivo algoritmo cuyo funcionamiento se describe en el diagrama de flujo del Anexo D (Figura D. 3). Cabe destacar, que fue necesaria una extensa revisión bibliográfica a fin de conocer en detalle el protocolo Modbus/TCP a programar en el PIC, aparte que la actividad de programación fue bastante ardua a fin de elaborar un código robusto, eficiente y sobre todo que se pudiera almacenar en la memoria del MCU.

IV.5 Fase de Interconexión y pruebas

En esta fase se realizaron todas las actividades necesarias para la conexión y prueba de los elementos involucrados en el SCADA desarrollado. Entre las actividades estuvo el desarrollo del eslabón fundamental en la interconexión: el demonio escrito en C. Este programa, tal y como se ha comentado a lo largo de todo el documento, consta de dos elementos sirviendo de puente entre el terminal de usuario y la RTU: un *socket* a través del puerto 502 TCP (puerto destinado para Modbus/TCP) hacia la IP de la RTU, para la comunicación UCC-RTU a fin de realizar las peticiones de monitoreo y control de las interfaces de la remota; por otra parte, se encuentra la gestión con la base de datos, a través del API en C, en donde se depositan los resultados obtenidos a partir de las interrogaciones a la RTU y a la vez sirve para tomar las peticiones de control provenientes de las páginas web/wap. El funcionamiento de este programa se detalla mejor a través de la Figura D. 2 del Anexo D que consiste en un diagrama de flujo del algoritmo elaborado. En esta fase también se realizó la interconexión de los distintos elementos involucrados en el SCADA en los siguientes ambientes:

- Una red LAN controlada con acceso a Internet.
- El UCC ubicado remotamente del RTU y el Terminal, los dos últimos ubicados detrás de una red privada (caso de pruebas en la UCAB).
- Todos los elementos ubicados remotamente.

En todos los ambientes presentados (cuyo esquema esta en el Anexo E) se verificó su conexión, en la medida de lo posible, a nivel de hardware (cables de red RJ-45, *switches*, *routers*) y a la vez a nivel de software utilizando comando de *echo request* y *echo reply* (ICMP – *ping y traceroute*). Estas verificaciones se hicieron primero entre pares directamente involucrados (Terminal - UCC, UCC- RTU) y tras confirmar su adecuada comunicación se procedió a la interconexión del sistema completo en conjunto.

Además, utilizando el monitor de protocolos *Ethereal* [5], se hicieron ajustes y monitoreo sobre el contenido de los paquetes y el tráfico generado por todos los protocolos involucrados en la intercomunicación del sistema (Modbus, TCP, IP, ICMP, ARP, UDP, DHCP); prestando especial énfasis en los paquetes Modbus/TCP en cuanto a la adecuada respuesta por parte del RTU a las interrogaciones del UCC que fueron programados desde cero. A través de la Figura D. 1 del Anexo D se puede apreciar a groso modo los flujos de paquetes involucrados en el sistema, permitiendo tener una mejor idea del esquema de comunicación del conjunto.

Existe una frecuencia de consulta del UCC al RTU la cual es variable y comprende una primera fase para la interrogación de las interfaces analógicas y, luego de un tiempo establecido, para las digitales respectivamente. En el caso de las peticiones de control, estas pueden interrumpir a la RTU en cualquier momento de su operación, siempre y cuando no sea durante el proceso de medición. Para ello el demonio en el UCC mantiene un control del orden en el cual se debe hacer las peticiones de monitoreo y control para procurar el mejor desempeño del sistema.

Todos los elementos estuvieron bajo pruebas de estrés: altas frecuencias de peticiones a la RTU; acceso desde múltiples sesiones a las páginas web/wap; alta carga de tráfico en el UCC representado por altas frecuencias de refrescamiento de las paginas; y demás pruebas que permitieron establecer los límites tolerables del sistema, que se describen en el Capítulo de resultado. Junto con estas pruebas, se verificó que la RTU ejecutara adecuadamente las mediciones y control, y que además, el contenido de las páginas reflejara con la mayor brevedad posible el real estado de los elementos bajo supervisión y control remotos.

[5] **Ethereal:** es un analizador de protocolos, utilizados para solucionar problemas de red, análisis, desarrollo de software y protocolos

CAPITULO V

RESULTADOS

En este capítulo se presentan los resultados obtenidos a lo largo de un año de investigación y desarrollo de este TEG, siguiendo todas las actividades descritas anteriormente a fin de cumplir con el objetivo propuesto. La descripción de los resultados se presenta en el mismo orden de los objetivos específicos planteados, demostrando el cumplimento de cada uno de ellos, que a su vez representa el logro del objetivo general.

V.1 Investigaciones Teóricas

En el Capítulo II del marco teórico se le brinda al lector una muy breve referencia de todos los elementos investigados en este TEG sobre: los sistemas de supervisión y control de señales analógicas y digitales usando unidades de telemetría y haciendo referencia a los protocolos de comunicación necesarios para la implementación de un sistema de supervisión y control vía IP y basado en páginas web y wap.

Toda esta investigación permitió conocer los actuales sistemas SCADA y a la vez brindar la base, junto con los conocimientos adquiridos en la carrera, para la creación del sistema que se desarrolló en este TEG. De cierta manera, la bibliografía que se presenta en este documento no refleja fielmente la cantidad de libros, manuales, tutoriales, investigaciones, consultas en la Web, conversaciones con profesores y otras personas conocedoras del tema que fueron necesarias pero, brinda una buena referencia a quien le pueda interesar indagar más sobre el tema.

V.2 Desarrollo de la RTU

La RTU desarrollada en este TEG maneja las siguientes interfaces:

Tipo de señal	Rango de Voltaje (V) [a]	Max. Corriente (mA) [b]	Máximo BW (Hz) [e]	Acción	Cantidad
Analógica	0 – 5.1	25 [b]	3.8	Entrada	4
	0 – 5.1	40 [c]	3.8	Salida	1
Digital	0 y 5.1	25 [b]	5.9 – 3.8	Entrada	4
	0 -120 [AC] 0 -24 [DC] [d]	2000 [AC] 2000 [DC] [d]	5.9 - 3.8	Salida	4

Tabla 6. Interfaces de la RTU

Nota. [a] Obtenido de valores prácticos medidos. [b] Valores obtenidos de (microchip, 2004, p. 323). [c] Valor obtenido de (*National Semiconductor*, 2005, p. 7). [d] indicado en el Relé [e] Valores obtenidos de pruebas de estrés en condiciones especiales.

Como se puede ver en la Tabla 6, la RTU maneja una variada cantidad de interfaces para monitoreo y control, en total son 13 interfaces para atender diversas operaciones. A fin de garantizar la adecuada operación de la RTU, se debe alimentar con los voltajes que se indican en la siguiente tabla, según el tipo de alimentación que se quiera utilizar.

Configuración	Voltaje (V)	Corriente (mA)
Transformador de Pared	7.5 - 15	340
Desde Fuente regulada	TTL (5)	335

Tabla 7. Características eléctricas del RTU

De esta manera, la remota se puede alimentar utilizando solo una de las dos alternativas: bien sea a través de una fuente que entregue 5V y se conecte a los terminales (*borners)*; o en su defecto a la salida de un transformador de pared que entregue entre 7.5V a 15V. En caso de utilizar la última opción, a la salida de los *borners* se entrega 0V y 4.5V para libre uso. Las características de consumo de

energía se describen en la siguiente tabla, las cuales fueron obtenidas a través de mediciones en pleno funcionamiento de la RTU.

Consumo	Voltaje (V)	Corriente (mA)	Potencia (W)
Mínimo	4.65	210	0.976
Máximo	4.53	320	1.45

Tabla 8. Consumo eléctrico de la RTU

La RTU cuenta con los siguientes módulos de comunicaciones:

Protocolo	Terminal	Max BW [Kbps].	Uso
RS232	DB9	19.2	Configuración vía Terminal
802.3 10BaseT	RJ-45	1.46	Comunicación con la UCC

Tabla 9. Módulos de Comunicaciones

Cabe destacar, que la interfaz serial RS232 solo sirve para la configuración de la unidad remota vía terminal, a través de esta se pueden modificar los parámetros de red que se pueden apreciar en la siguiente gráfica que muestra una sesión en *Microsoft Hiperterminal* con la RTU. Por medio de este terminal también se puede observar el estado de la RTU y las peticiones provenientes de la UCC con sus respectivas respuestas. En cambio, a través de la interfaz Ethernet no se puede configurar estos parámetros de red de la RTU, sin embargo, se puede establecer la comunicación RTU-UCC para las respectivas consultas y controles.

Tal y como se aprecia en la Figura 11, el diseño del circuito desarrollado para la RTU fue realizado utilizando el software *PCBExpress*, después de determinada la correcta interconexión de los elementos que se aprecian con mayor detalle en el Anexo B.

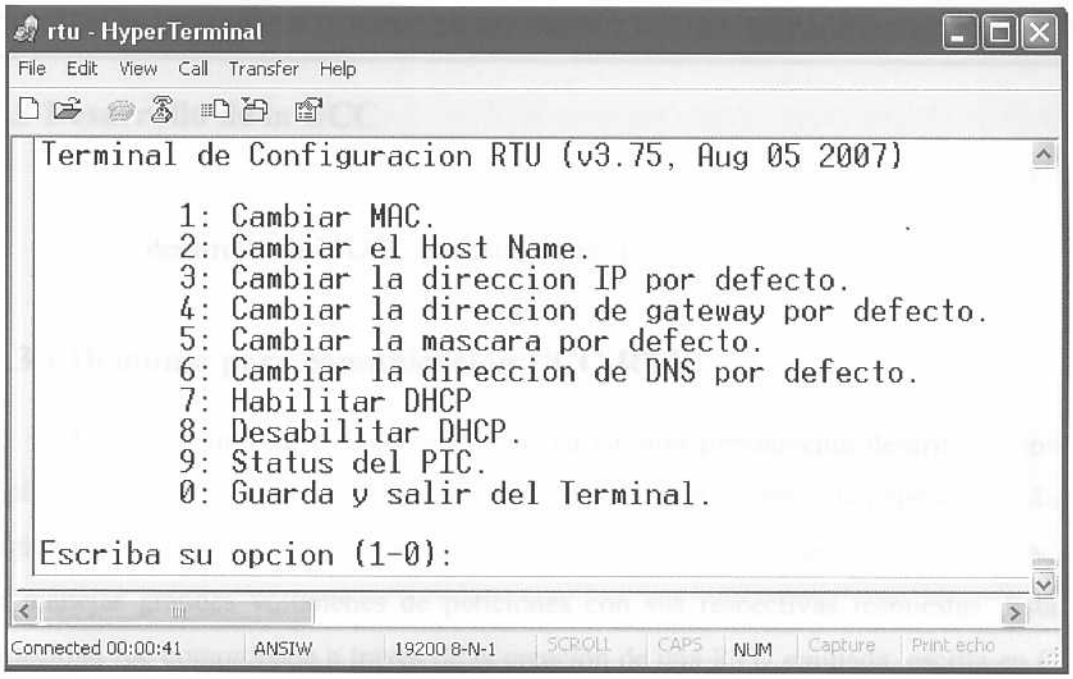


Figura 10. Terminal de Configuración de la RTU

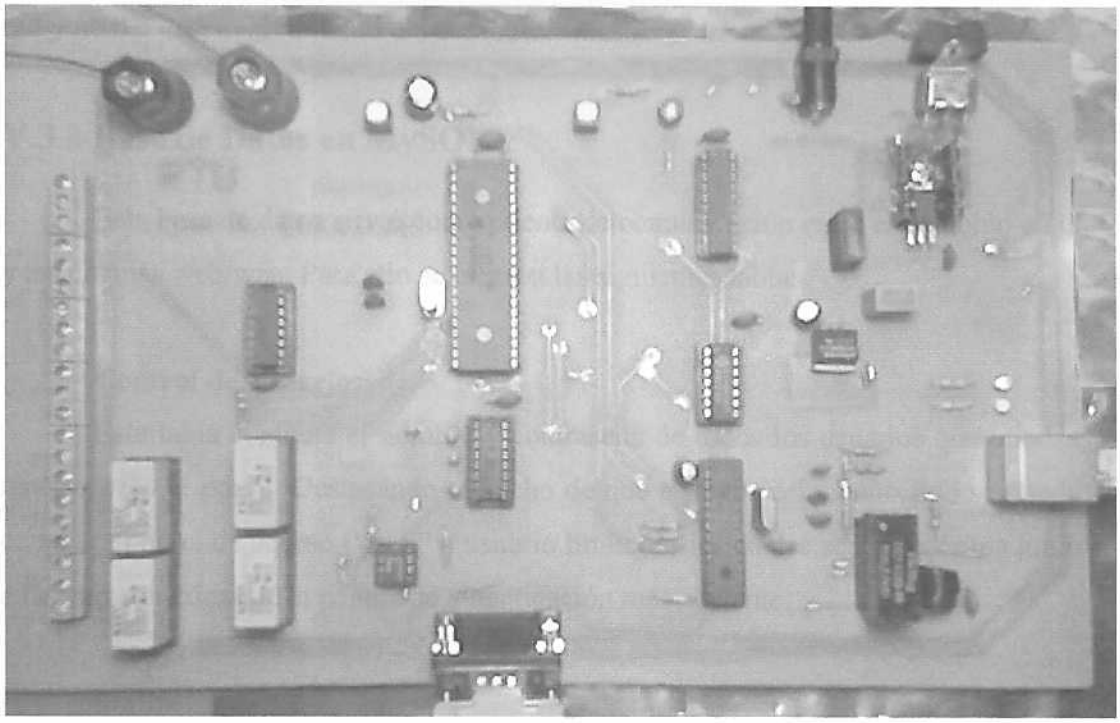


Figura 11. Circuito Impreso de la RTU

V.3 Desarrollo de la UCC

En el desarrollo de la UCC se destacan tres elementos fundamentales:

V.3.1 Demonio para comunicación UCC-RTU

Este demonio, cuyo funcionamiento ya ha sido previamente descrito en los capítulos anteriores, está en código fuente en el CD anexo a este documento y en la página web, sobre la cual se comentará más adelante. El programa tiene la capacidad de manejar grandes volúmenes de peticiones con sus respectivas respuestas. Esta capacidad fue comprobada a través de la creación de una RTU emulada, escrita en C también. Como se puede ver más adelante en los resultados de la intercomunicación RTU-UCC del Anexo E, las limitaciones del sistema vienen de parte del PIC y de la red y no del desenvolvimiento del demonio.

V.3.2 Base de Datos en MySQL

Esta base de datos sirvió como puente de comunicación entre el demonio en C y las páginas web/wap. Para ello se crearon las siguientes tablas:

Control de Usuarios

Esta tabla contiene el nombre y contraseña de todos los usuarios que pueden tener acceso al portal. Destacando el hecho de que a través del campo tipo se puede conocer el nivel de acceso ("root" o usuario limitado) los cuales serán descritos junto a las características de la página de autenticación más adelante.

Status

Esta tabla contiene los valores en vivo de las magnitudes de las señales presentes en la RTU, bien sean analógicas o digitales; de control o de monitoreo. Además, por medio de los campos DC1, DC2, DC3, DC4 y AC se puede asignar los

valores de control que el demonio en C lee para ejecutar las peticiones de control. Junto con estos campos también están: FR, FM y FMC, que contiene los valores de las frecuencias de refrescamiento de la página y de petición de muestras a la RTU respectivamente; en donde a través de FMC se puede fijar esta última frecuencia.

DatosRTU

Contiene el registro de históricos de todas las operaciones realizadas durante el día, bien sean de control o monitoreo, enviadas a la RTU. En pocas palabras, posee los campos descritos en la tabla Status; con la diferencia de que se registran la fecha y hora (hora, minuto y segundo) de cada una de las operaciones realizadas. Pasado el día, se guarda en una tabla aparte titulada con la fecha de todas las operaciones realizadas en tal día y con el mismo formato y campos extraídos de DatosRTU.

ID	Login	Password	Tipo
Int(16)	Varchar(30)		Varchar(1)

DI1	DI2	DI3	DI4	AI1	AI2	AI3	AI4	DO1	DO2	DO3	DO4	DC1	DC2	DC3	DC4	AO	AC	IP	FR	FM	FMC
Int(1)				Float				Int(1)								Float		Varchar(15)	Int(8)		

ID	Fecha	DI1	DI2	DI3	DI4	AI1	AI2	AI3	AI4	DO1	DO2	DO3	DO4	AO
Int(16)	Timestamp	Int(1)				Float				Int(1)				Float

Tabla 10. Campos de las tablas Usuarios, Status y DatosRTU respectivamente

V.3.3 Páginas web/wap

Conforman la interfaz de usuario del sistema SCADA y el servidor web/wap aloja las páginas que se describen a continuación.

Páginas web/wap de autenticación

A través de estas páginas se piden los datos de nombre de usuario y contraseña para el ingreso a las distintas páginas del portal. Automáticamente y según los valores registrados en la tabla de usuarios de la base de datos, se puede conocer si el usuario puede efectuar operación de control y monitoreo ("root"); o si solamente posee permisos para monitoreo de las interfaces (usuario limitado).

Páginas web/wap de monitoreo

En estas páginas se observan los valores de las señales presentes en las interfaces de la RTU. Su veracidad depende de la frecuencia de refrescamiento que el usuario proponga; en el caso de la web se puede ajustar automáticamente en la página de control cambiando el campo de refrescamiento de página; y en el caso wap es necesario que el propio usuario haga la petición de refrescamiento.

Páginas web/wap de control

Aparte de controlar la frecuencia de refrescamiento de las páginas; creación y eliminación de usuarios (estas opciones solo válidas para las páginas web) y ajustes en la frecuencia de peticiones UCC-RTU, permite monitorear y establecer los valores que el usuario desea tener presente en las interfaces de control de la RTU. Además, posee un algoritmo de control de múltiples peticiones de distintos usuarios sobre una misma salida de la RTU al mismo tiempo.

Páginas web de Históricos

Solo disponible vía web, presenta los valores almacenados en las tablas de históricos de la base de datos. Además, publica por cada interfaz las estadísticas de niveles DC, AC; potencias AC y DC; junto con los valores máximos y mínimos y su ocurrencia dentro del periodo establecido por el usuario a través de un formulario de búsqueda. Para cada señal, se presenta una tabla con todos los valores estadísticos descritos y una gráfica de las amplitudes con respecto al tiempo de evaluación. La precisión de la gráfica depende directamente de la frecuencia de peticiones (muestreo).

Todas estas páginas, tanto web como wap, se pueden apreciar ingresando a la dirección http://rtu.servehttp.com, de donde se ha extraído las imágenes de cada una de estas páginas presentes en este documento en el Anexo C.

V.4 Interconexión

Dentro de las actividades involucradas en la interconexión y pruebas se obtuvieron importantes resultados como los que se muestran en el Anexo E, donde se observa que el analizador de protocolos *Ethereal* detecta los flujos de paquetes Modbus/TCP, bien sean de petición o de respuesta, junto con el tipo de petición para señales analógicas o digitales; de control o supervisión. De esta manera, se comprueba que los algoritmos programados, tanto en el UCC como en el RTU, realizan su comunicaciones tal y como establece el protocolo.

Además, se realizó importantes pruebas sobre el comportamiento bajo estrés; ancho de banda y capacidad de respuesta de la RTU, cuyos resultados también están en el mismo Anexo E. De esas pruebas se desprende que: el ancho de banda necesario en la comunicación es directamente proporcional a la frecuencia de peticiones UCC-RTU.

Otro aspecto importante a considerar es, que la capacidad de respuesta por parte de la RTU depende enormemente de las características de la red. Como se puede ver en las imágenes de la Figura E. 1 del Anexo E: en una red en buenas condiciones la RTU puede responder rápidamente luego de realizada la petición; caso contrario ocurre cuando, debido a fallas de la red, el periodo entre mientras se envía la petición y llega la respuesta por parte de la RTU es mayor. Este efecto se debe a la serie de retransmisiones y controles de error por parte del protocolo TCP involucrados en la comunicación, y necesarios para garantizar el envió de los paquetes modbus/TCP en los extremos.

Aparte de las condiciones de la red, las reducidas capacidades del PIC18F limitan la capacidad de respuesta, dada la cantidad y complejidad de tareas que realiza el PIC ante la entrada de peticiones. Como ejemplo se puede ver la diferencia en el tiempo de respuesta cuando solo se atiende monitoreo digital contra cuando se atiende el analógico también. La diferencia de tiempos se debe a que el proceso de mediciones analógicas demanda más tiempo y uso de recursos por parte del PIC. También el uso constante del terminal de estado del RTU vía protocolo RS232 disminuye su capacidad de respuesta, que repercute en un mayor tiempo de respuesta de la RTU.

Como se aprecia en las tablas del anexo E, se puede capturar señales digitales y analógicas con un ancho de banda de hasta 3.8Hz; considerando que la máxima frecuencia de muestreo es de: 7.6 muestras/s. Además, a medida que la frecuencia de peticiones disminuye, la cantidad de muestras obtenidas calculadas y prácticas se van acercando; debido a que a medida que disminuye la frecuencia de peticiones las exigencias en el PIC son menores, traduciéndose en menores retrasos que a tan altas frecuencias son notables. Sepa que el UCC está programado de manera que hasta que no llegue una respuesta a una petición; no se emite la siguiente. De tal manera que cuanto más tarde una respuesta a una petición; esta retrasará la solicitud de la siguiente.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

A lo largo de este capítulo se presenta algunas conclusiones sobre los logros obtenidos tras un año en la elaboración de este TEG, junto con algunas recomendaciones a la hora de la implementación de esta solución y las posibilidades de futuras extensiones y mejoras al sistema propuesto.

Como se ha comentado, el desarrollo industrial trajo consigo la necesidad de poder monitorear y controlar eventos físicos remotamente; a fin de obtener una adecuada respuesta de los procesos que se desarrollan a distancia, que inclusive suelen algunas veces ser inaccesibles al ser humano o implican altos costos. Esta necesidad está siendo cubierta con la introducción de los sistemas SCADA dentro de las industrias. Tales sistemas suelen ser complejos y operados por personal experto en el área de la telemetría.

Sin embargo, con la aparición de las casas y edificios inteligentes; sistemas de seguridad; incendio y otras aplicaciones más, ha llevado a la adopción de estos sistemas en otros ambientes -donde los usuarios no cuentan con la experiencia y conocimientos necesarios para la operación de estos sistemas de telemetría industriales complejos-. Fue esta misma razón la que motivó el desarrollo de este TEG, proporcionando a los usuarios la capacidad de controlar y monitorear cualquier evento a distancia a través de terminales comunes para toda la población (PC y celulares) y con una interfaz web/wap muy intuitiva y de fácil uso. Todo esto con el fin de masificar la utilización de este tipo de sistemas en cualquier ambiente.

La característica principal de este sistema es que está totalmente interconectado a la Internet, lo cual simplifica enormemente la conexión a las RTU en cualquier ambiente. Con tan solo conectar a las interfaces las señales que se desean monitorear y/o controlar, y brindar a la RTU de Internet a través de un cable RJ-45, el sistema automáticamente comenzará a trabajar sin la necesidad de realizar previas configuraciones, solo en el caso que se cuente con una conexión bajo un servidor DHCP. Además de su simplicidad a la hora de poner en funcionamiento la RTU, el hecho de que todos los elementos del sistema estén conectados a la Internet ofrece una gran movilidad de todos los elementos (RTU, UCC, terminales) y a la vez una fácil adaptación a cualquier ambiente.

Sin embargo, el mismo hecho de que este sistema base su interconexión sobre la Internet, implica que este condicionado a las capacidades que ofrece la red en ese instante, es decir, las capacidades del sistema se ven limitadas al: ancho de banda, tráfico y retardos que ofrezca la red a la cual esta interconectada cada uno de los elementos del sistema.

Aparte de las condiciones de la red, la capacidad de procesamiento de la RTU basado en el PIC18F4620 también limita directamente el sistema. Tras pruebas realizadas en condiciones normales de la red de CANTV (ADSL *Uplink*= 1Mb/s y *Downlink*=512Kbps) se logró hasta un máximo de 7.6 muestras/segundo. Es decir, se puede muestrear señales analógicas y digitales con un BW de hasta 3.8 Hz. Este ancho de banda, aunque no es muy grande, es aceptable dentro de la naturaleza de las señales de campo que se manejan en sistemas de telemetría de propósito general. Se recomienda entonces conectar señales de bajo ancho de banda a fin de obtener mediciones precisas durante el tiempo, o ajustar la frecuencia de peticiones dependiendo de las exigencias de medición que el usuario tenga.

Hay que tener en consideración que a medida que se aumenta la frecuencia de peticiones a la RTU, aumentará proporcionalmente el tráfico en la red. Aunque si bien es cierto que el BW máximo necesario de 1.46 Kbps es relativamente bajo; no es el elemento dentro de la red que realmente limita la capacidad del sistema. Por ejemplo la red ADSL de CANTV, por citar alguna, ofrece un buen ancho de banda para esta aplicación, sin embargo, suele a veces tener mucho retardo y por lo general no ofrece un nivel de CIR estable y adecuado a las necesidades de este tipo de transmisión de datos a tiempo real. Se recomienda entonces, más allá de prestar atención al ancho de banda que ofrezca el ISP, tomar precauciones sobre la QoS de la conexión, de manera que ofrezca características adecuadas para conexiones a tiempo real, con bajo retardo y un nivel adecuado de CIR.

VI.1 Posibilidades de Extensión Futura

A lo largo de la experiencia en la elaboración de este TEG y considerando las ultimas soluciones existentes al momento de la redacción de este documento, que no existían previamente, se especifican algunas recomendaciones para extensiones del sistema SCADA que puedan ofrecer ciertas mejoras con respecto al presentado.

Una de ellas es optar por una arquitectura de red diferente: en vez del sistema triangulado Terminal – UCC – RTU; hacer una comunicación directa Terminal – RTU. Para ello es necesario utilizar microcontroladores con mayor capacidad de procesamiento (por ejemplo los anunciados DSPIC con controlador Ethernet integrado) y mayor cantidad de memoria (conexión externa USB de memoria flash de hasta 2GB), dado que todas las tareas en la arquitectura triangulada de este TEG para base de datos y servidor web/wap que estaban en la UCC apoyando a la remota; estarían en esta nueva arquitectura sobre la RTU, cargando nuevos procesos sobre el PIC u otro microcontrolador que ofrezca mejor *performance* al utilizado para este TEG. Sin embargo, ofrece una arquitectura de red más simple y centralizada.

También se pueden utilizar protocolos de comunicación adicionales al Modbus/TCP, como es el caso del SNMP ofrecido en el nuevo Stack TCP/IP 4.0 de Microchip, ofreciendo también el TFTP que sirve para la exportación de la base de datos en la nueva arquitectura comentada. Además, con los nuevos módulos de ZigBee o el desarrollado por Microchip "MiWi" se puede ofrecer una RTU inalámbrica, permitiendo una flexibilidad aun mayor a la del sistema propuesto en este TEG.

Sería también de gran importancia aprovechar las bondades del IPv6 en los futuros sistemas, a fin de establecer en los paquetes de la conexión UCC-RTU un nivel de QoS que garantice poco retardo y un nivel de CIR adecuado para conexiones de tiempo real.

VI.2 Alcances del Sistema

Como se puede ver, la arquitectura planteada en este TEG ofrece la capacidad de adaptar el sistema a prácticamente cualquier ambiente en el cual se cuente con acceso a internet. Cosa que es bastante viable ya que prácticamente en cualquier edificación, bien sea empresas o en los hogares, se cuenta con acceso a internet bien sea inalámbrica o redes ya cableadas de Ethernet. De esta manera, la implementación de este tipo de sistema no implica el tendido de cables o remodelación alguna a la edificación existente.

Además, con este sistema se puede monitorear y controlar desde el estado de un contacto seco (puerta, encendido de luces, alarmas) hasta niveles de temperatura, pesos, cantidad de liquido en los tanques, concentración de gases, presión o cualquier otro fenómeno físico que, a través de la utilización de transductores, se pueda transformar las magnitudes físicas en señales eléctricas o viceversa (en caso de control).

BIBLIOGRAFÍA

- Álvarez, G.; Vázquez, S.; Sierra, P.; Fernández, L.; y Machiran, A. (2003). *Componentes de Hardware para un SCADA*. [Documento en Línea]. Ministerio de Ciencia Tecnología y Medio Ambiente, La Habana, Cuba. Disponible: ed2k://|file|Componentes%20de%20Hardware%20para%20un%20SCADA.pdf|425422|740302C58B7A626C516A52899582B763|/ [Consulta: 2006, Diciembre 18].
- Amodio, J. (2007). *Internetworking with Microchip Microcontrollers*. [Documento en Línea]. Disponible: http://www.amodio.biz/projects/PIC10BaseT/ [Consulta 2007, Febrero 25].
- Apache Software Foundation. (2006). *Using Apache with Microsoft Windows*. Disponible: http://httpd.apache.org/docs/2.2/install.html. [Consulta 2006, Noviembre 20].
- Autómatas Industriales. (2000). *Sistemas SCADA*. [Documento en Línea]. Disponible: http://www.automatas.org/redes/scadas.htm [Consulta 2006, Agosto 15].
- Baca, Mery. (2006). *Servidores web*. [Documento en Línea]. Disponible: http://mery-multi.blogspot.com/2006/12/servidores-web.html [Consulta 2006, Noviembre 18].
- Bavaresco, A. (1992). *Proceso Metodológico en la Investigación. (Cómo hacer un Diseño de Investigación)*. Caracas: Servicios Bibliotecarios de la Universidad del Zulia.
- Booth, D..; Haas, H..; McCabe, F.; Newcomer, E.;Champion,M.; Ferris, C.; Orchard, D. (2003). *W3C: Web Service Architecture*. [Documento en Línea]. Disponible: http://www.w3.org/TR/2003/WD-ws-arch-20030808/wsa.pdf. [Consulta 2006, Septiembre 10].
- Burbano, J. (2006). *Análisis comparativo de bases de datos de Código abierto vs. Código cerrado (determinación de índices de comparación)*. [Documento

en Línea]. Disponible: http://www.monografias.com/trabajos35/comparativa-bases-datos/comparativa-bases-datos.zip [Consulta 2006, Diciembre 18].

- Daneels, A y Salter, W. (2000). *What is a SCADA?*. [Documento en Línea]. European Organization for Nuclear Research. Disponible: http:// ref.web.cern.ch/ref/CERN/CNL/2000/003/scada/ [Consulta: 2006, Septiembre 2].

- Departamento de Tecnoloxías da Información e as Comunicacións de la Universidade da Coruña. (1999). *Sockets en C* (Ap.) [Documento en Línea] La Coruña, España. Disponible: http://usuarios.lycos.es/kondragx1/Manual_Socket_C .pdf [Consulta 2007, Enero 25].

- Freescale (2007). *Freescale Semiconductors Products*. [Documento en Línea]. Disponible: http://www.freescale.com/webapp/sps/library/prod_lib.jsp [Consulta 2007, Agosto 12].

- Gordon, C. y Deon R. (2004). *Modern SCADA Protocols: DPN3, 60870.5 and Related Systems* (2a. ed.) [Documento en Línea]. Mumbay, India: Newnes. Disponible: ed2k://|file|Practical%20Modern%20Scada%20Protocols%20Dnp3,60870.5%20Clarke%20G,%20E537p%20Newnes%20Elsevier%202004.pdf|20336046|EA3F2738ECCF81E3976176AF2CF54459|/ [Consulta 2006, Agosto 30].

- Gracias, Jorge (2002). *Instalación de Apache + PHP + MySql*. Disponible: http://www.webestilo.com/php/php08a.phtml [Consulta 2006, Noviembre 25].

- Gutiérrez, E. (2002). *¿Qué es MySQL? Lo mínimo que debemos de conocer acerca de MySQL*. [Documento en Línea]. Disponible: http://www.mysql-hispano.org/page.php?id=2. [Consulta 2006, Agosto 16].

- Microchip (2006b). *Conectivity TCP/IP*. [Documento en Línea]. Disponible: http://www.microchip.com/stellent/idcplg?IdcService=SS_GET_PAGE&nodeId=1489. [Consulta 2007, Enero 15].

- Microchip (2007a). *Microchip PIC18 MCU product family*. [Documento en Línea]. Disponible: http://www.microchip.com/ParamChartSearch/chart.aspx?branchID=1004&mid=10&lang=en&pageId=74. [Consulta 2007, Junio 15].

- Microchip Technology Inc. (1997). *PICmicro™ Mid-Range MCU Family Reference Manual (DS33023a)* [Documento en Línea]. Disponible:

http://ww1.microchip.com/downloads/en/DeviceDoc/31000a.pdf [Consulta 2006, Septiembre 18].USA: Microchip Technology Inc.

- Microchip Technology Inc. (2004). *PIC18F2525/2620/4525/4620 Data Sheet (DS3962b)*. [Documento en Línea]. Disponible: http://ww1.microchip.com/ downloads/en/DeviceDoc/39626C.pdf. [Consulta 2007, Agosto 18]. USA: Microchip Technology Inc.

- Microchip Technology Inc. (2006a). *Stand-Alone Ethernet Controller with SPI Interface (DS39662b)*. Disponible: http://ww1.microchip.com/downloads/en/DeviceDoc/39662b.pdf [Consulta 2007, Agosto 18]. USA: Microchip Technology Inc.

- MobileFish. (2007). *How WAP Works*. [Documento en Línea]. Disponible: http://www.mobilefish.com/tutorials/how_wap_works/how_wap_works.html. [Consulta 2007, Mayo 4].

- Modbus-IDA (2004). *Modbus Messaging on TCP/IP implementation Guide (V1.0a)*. [Documento en Línea]. USA:Modbus-IDA. Disponible: ed2k://|file|Hardware%20%20Modbus%20Messaging%20On%20TcpIp%20Implementation%20Guide.pdf|422912|70C1EF00C4A948C76C04E2FEB8EF4DB2|/ [Consulta 2006, Febrero 4].

- MySql Lab (2006). *White Papers*. [Pagina web en línea]. Disponible: http://www.mysql.com. [Consulta 2007, Enero 8].

- National Semiconductor. (2005). *LM158/LM258/LM358/LM2904 Low Power Dual Operational Amplifiers* [Documento en Línea]. Disponible: http://www.national.com/ds.cgi/LM/LM158.pdf [Consulta 2007, Agosto 18].

- OMA. (2006). *Open Mobile Alliance*. [Pagina web en línea]. Disponible: http://www.openmobilealliance.org/index.html [Consulta 2006, Agosto 4].

- Postel, J. (1981a). *Internet Protocol Specifications. (RFC 791)*. Virginia, EU: DARPA Information Processing Techniques Office.

- Postel, J. (1981b). Transmition *Control Protocol Specifications. (RFC 793)*. Virginia, EU: DARPA Information Processing Techniques Office.

- Pozo, Salvador (2005). *MySql con clase, gestión de bases de datos.* [Documento en Línea]. Disponible: http://www.conclase.net/c/mysql/index.php [Consulta 2006, Diciembre 15].
- Uribe,L. (2004). *Scada, Master Unit, RTU* [Documento en Linea]. Disponible: GUribe-UCAB@cantv.net.
- Usategui, J. y Martínez, I. (2003). *Microcontroladores Pic. Diseño práctico de aplicaciones Primera parte. El PIC16F84 Lenguajes PBASIC y Ensamblador* (3a. ed.). Madrid, España: McGraw-Hill.
- Webstilo. (2006). *Manual de PHP. Conceptos básicos.* [Documento en Línea]. Disponible: http://www.webestilo.com/php/ [Consulta 2006, Septiembre 1].

ANEXO A

EL MICROCONTROLADOR PIC18F4620

Y CONTROLADOR ETHERNET ENC28J60

En este anexo se presenta toda la información adicional que el lector desee conocer sobre los microcontroladores, específicamente sobre el PIC 18F4620. Este anexo está dividido de tal manera que se comienza explicando la arquitectura del MCU de la Familia PIC18F, incluyendo uno de los módulos externos más importantes en este TEG, como lo es el Controlador Ethernet ENC28J60 y finalizando con las especificaciones técnicas que definen al PIC 18F4620 utilizado en este TEG.

1 La arquitectura PIC18F de Microchip

Microchip ha agrupado sus modelos de MCU de acuerdo a sus prestaciones. La línea PIC18F constituye la línea media de los MCU de Microchip con una longitud de palabra del procesador de 14-bits; 8-bits para la memoria de datos y con velocidades de hasta 50Mhz ofreciendo una excelente relación precio/*performance*.

La excelente capacidad de los MCU de Microchip puede ser atribuida a una serie de características arquitectónicas comúnmente encontradas en los CPU RISC. En (Microchip Technology Inc., 1997, cap. 4, p. 4) se mencionan las características de los MCU PIC18F.

1.1 El Procesador

La arquitectura Harvard. (Ver Figura A. 1) cuenta con la memoria de programa y la memoria de datos por separado y solo accesibles a través de buses distintos. El PIC18F cuenta con un bus de datos de 14-bits para acceder a la memoria de programa y un bus independiente de 8-bits para acceder a la memoria de datos. Esto mejora el ancho de banda con relación a la arquitectura tradicional de Von-Neumann, en la cual la memoria de programa y la memoria de datos son accedidas a través del mismo bus.

Esta arquitectura ofrece la posibilidad de poder acceder a una sola instrucción en un ciclo de reloj: mientras la memoria de programa es accedida, la memoria de datos esta en un bus independiente y puede ser leída y escrita. Esta separación de buses permite que una instrucción sea ejecutada mientras la siguiente es extraída.

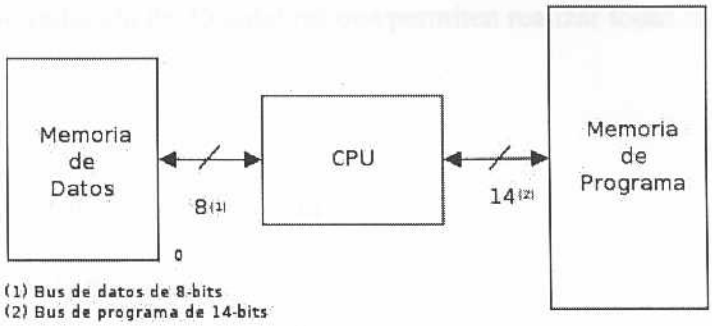


Figura A. 1. Arquitectura del procesador del microcontrolador

Instrucciones en un solo ciclo de máquina. Con la memoria de programa accedida por un bus totalmente independiente, es posible extraer una instrucción en un solo ciclo de máquina. Esta instrucción contiene toda la información requerida y es ejecutada también en un solo ciclo. Puede existir un ciclo de retardo cuando la instrucción modifica el contenido del contador de programa obligando a limpiar el contenido del *pipeline* y a extraer una nueva instrucción.

Segmentación del procesador. Consiste en descomponer en etapas el procesamiento de cada instrucción, solapando cada una de estas y logrando un paralelismo implícito. En el caso de la arquitectura PIC18F se realiza en 2 etapas, en las cuales se solapan la extracción y ejecución de cada instrucción. La extracción de una instrucción demora un TCy[6] y su ejecución demora otro TCy[7]. Sin embargo,

[6] TCy es la abreviatura de Instruction Clock Cycle, que se traduce al castellano como Ciclo de instrucción. En el caso de la arquitectura PIC18F el TCy es de un ciclo de máquina.

[7] En el caso de la arquitectura del 18XXXX cada oscilación es divida en 4 bloques (Q1,Q2,Q3,Q4), en cada uno de ellos el MCU realiza las tareas de extracción, actualización de contador de programa y decodificación y ejecución.

debido al solapado en la extracción y la ejecución de la instrucción previa, mientras una es extraída; la otra es ejecutada en cada TCy.

Set de instrucciones reducidas. Como su arquitectura RISC lo indica, cuenta con un conjunto reducido de 35 palabras que permiten realizar todas las tareas.

1.2 Organización de la Memoria

Memoria de programa. La arquitectura de los PIC18F cuenta con contador de programa de 13bits, el cual es capaz de direccionar hasta 8K x 14 palabras. Dependiendo del modelo del MCU esos 8Kx14 palabras estarían físicamente implementados o no.

Normalmente, la memoria de programa puede ser de tipo EEPROM o FLASH. Esta última resulta la comúnmente usada debido a que puede ser fácilmente re-escrita, lo que permite una modificación del programa sin necesidad de cambiar el chip del MCU. Otra característica importante es que estos MCU cuentan con una *stack* que permite hasta 8 niveles de profundidad. Sin embargo, esta característica no se encuentra en la memoria de programa ni en la memoria de datos, por lo que no es accesible ni para lectura ni para escritura.

Memoria de datos. La memoria de datos está dividida en múltiples bancos, los cuales contienen registros especiales (SFR) y los registros de propósito general (GPR) que pueden ser usados para el almacenamiento de los datos del programa. Estos registros son de 8 bits y cada banco está compuesto por 128 bytes. En la parte inferior de estos bancos se encuentran los SFR y arriba de estos se encuentran los GPR. Los SFR son utilizados por el CPU y los módulos periféricos del MCU para controlar los distintos tipos de operación del MCU.

Memoria EEPROM. Los MCU de la familia PIC18F cuentan con una cierta cantidad de memoria EEPROM dependiendo del modelo, la cual permite guardar datos de manera no volátil. Esta memoria se graba y borra eléctricamente. Sin embargo, no se puede conseguir en grandes capacidades; dependiendo del modelo del MCU pueden llegar a ser de hasta 1024 bytes y su tiempo de escritura y consumo son elevados.

Memoria Flash. Se trata de una memoria no volátil y de bajo consumo que se puede escribir y borrar en circuito al igual que las EEPROM, pero suelen disponer de mayor capacidad que estas últimas. Son recomendables para aplicaciones en las que es necesario modificar el programa a lo largo de la vida del producto. Por sus mejores prestaciones están sustituyendo a la memoria EEPROM para contener instrucciones.

1.3 Líneas de entrada y salida.

Las líneas de E/S generales pueden considerarse los periféricos más simples con los que cuentan los MCU PIC18F permitiéndole monitorear y controlar otros dispositivos. Cada uno de los pines del MCU se agrupan para formar lo que se denomina puertos. Para la mayoría de estos puertos, los pines pueden configurarse para funcionar como líneas de entrada o salida de señales digitales TTL de acuerdo a las necesidades de cada caso a través de un SFR llamado TRIS<X>, el cual se encargará de establecer la dirección del PUERTO<X>.

Inclusive, cuenta con entradas analógicas las cuales son traducidas en señales digitales para el procesamiento dentro del PIC. Los modelos de 40 pines de la familia PIC18F no cuentan con salidas analógicas; para ese tipo de necesidades se puede utilizar un DAC[8].

[8] DAC: *Digital to Analog Converter*

Para agregar funcionalidad y flexibilidad, muchos de los pines de los MCU están multiplexados con funciones alternativas. Mediante diversos SFR se pueden activar o desactivar dichas funciones, en esos casos las funcionalidades de los pines de E/S cambiará para ajustarse al nuevo módulo.

1.4 Módulos auxiliares

Muchos de los módulos mencionados dependen del modelo de PIC que se elija. Algunos de estos módulos que fueron aplicados en el desarrollo de la RTU de este TEG son:

Conversores analógicos. Este módulo permite la conversión de una señal analógica a su correspondiente representación digital de 8 ó 10 bits. La salida del *"sample and hold"* es enviada al conversor que generará el resultado por sucesivas aproximaciones. El voltaje de referencia analógico es seleccionable al voltaje del dispositivo (VDD) o usando el voltaje enviado en el pin VREF. El conversor analógico digital tiene la particularidad de poder funcionar mientras el MCU se encuentra en modo *SLEEP* (Microchip Technology Inc., 1997, Cap. 4, p. 4).

Comparadores analógicos. El comparador analógico se encuentra multiplexado en los pines del MCU. Se utiliza para poder verificar el valor de una señal analógica.

Transmisor y receptor Síncrono / Asíncrono Universal (USART).

También conocido como la interfaz de comunicación serial, este módulo puede configurarse para funcionar como un sistema *full duplex* asíncrono capaz de comunicarse con dispositivos como: terminales CRT o PC. También puede ser configurado como un *half duplex* síncrono que le permite establecer comunicación con circuitos integrados de conversión Analógica/Digital, memorias EEPROM seriales, etc. (Microchip Technology Inc., 1997, cap.18).

Temporizadores. Los temporizadores están orientados al control de tiempo. Estos temporizadores pueden ser de 8 a 16 bits con la posibilidad de ser accedidos para la escritura y lectura. También es posible seleccionar la fuente de reloj para que esta sea interna usando directamente el reloj interno del MCU o a través de un reloj externo. Además, el PIC cuenta con unos pines en los que se les puede conectar un reloj externo (Microchip Technology Inc., 1997, cap. 11).

2 Módulos Auxiliares externos (ENC28J60)

Todos los módulos descritos anteriormente están integrados al MCU sin embargo, el siguiente módulo no está incluido dentro del microcontrolador y debe ser conectado físicamente para su operación.

Controlador Ethernet ENC28J60. Es un módulo vital para el desarrollo de este TEG, ya que este controlador permite dotar de conectividad al MCU utilizando Ethernet, un estándar reconocido y ampliamente difundido. (Microchip Technology Inc., 2006a, p. 3).

El ENC28J60 se conecta con el MCU a través de una interfaz SPI[9], que requiere del empleo de sólo 4 líneas del microcontrolador, como se muestra en la Figura A. 2. Entre las características principales de este controlador se encuentran:

- Controlador Ethernet compatible con IEEE 802.3.
- Dirección MAC y 10BaseT integrados.
- *Buffer* dual SRAM para transmisión/recepción de 8 kilobytes.
- Retransmisión en caso de colisión programable.
- Generación del CRC.
- Rechazo automático programable de paquetes erróneos.

[9] SPI: Serial Peripheral Interface

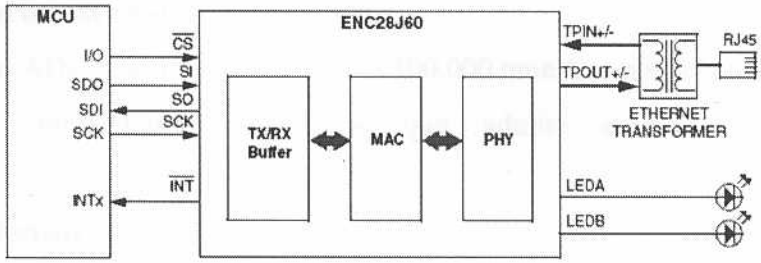


Figura A. 2. Esquema de conexión del controlador Ethernet al MCU

Figura tomada de: (Microchip Technology Inc., 2006, p. 4)

Protocolos que soporta el controlador:

- ARP
- IP
- ICMP
- UDP
- TCP
- DHCP
- HTTP
- FTP

3 El PIC18F4620

Detallando más en este MCU PIC18F4620 (Microchip Technology Inc., 2004), podemos ver que entre sus características más notorias están:

CPU

- Capacidad de procesar hasta 10 MIPS.
- Arquitectura RISC optimizada para código en C.

Sistema

- Oscilador interno desde 31 KHz hasta 8 MHz, llegando hasta 32 MHz utilizando el 4X PLL.
- Monitor de seguridad del *clock*, permite salvar el estado del PIC y reiniciarlo en caso de que el *clock* del PIC falle.
- *Watchdog Timer.*
- Gran rango de voltaje de operación; Desde 2.0V hasta 5.5V.

Características analógicas

- 10-bit ADC, con 13 canales y hasta 100.000 muestras por segundo.
- Dos comparadores analógicos que admite entradas multiplexadas.

Periféricos

- Soporta la interfaz *Master Synchronous Serial Port* SPI ™ y la I^2C™ tanto en modo maestro como esclavo.
- Módulo EUSART con soporte a bus LIN.
- Cuatro temporizadores.
- Hasta 5 salidas PWM.

Sin embargo, ningún modelo PIC cuenta con salidas analógicas. Para resolver este problema se puede utilizar un DAC externo que permite la salida de una señal analógica de calidad. Como se puede ver en el siguiente diagrama, se cuenta con suficiente cantidad de interfaces para conectar: las salidas y entradas analógicas y digitales, el puerto EUSART y toda la conexión necesaria para establecer la comunicación con el ENC28J60.

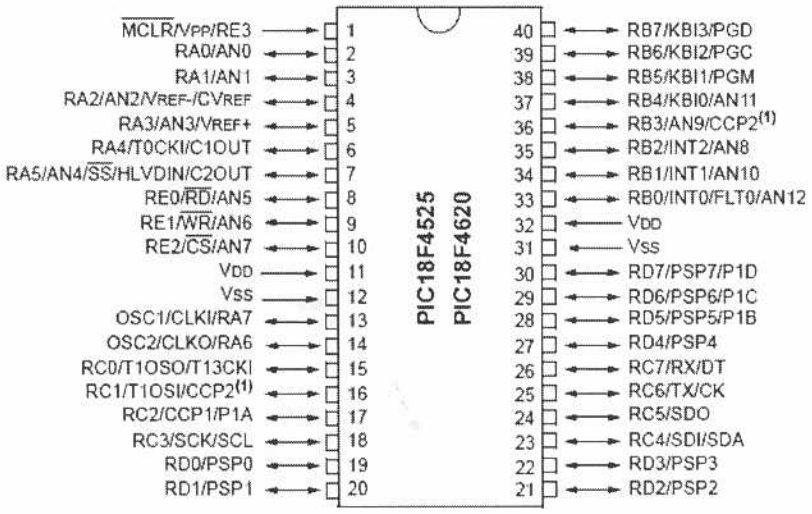


Figura A. 3. Distribución de los pines de MCU PIC18F4620

Figura tomada de (Microchip Technology Inc., 2004, p. 2)

ANEXO B

DESARROLLO DE LA RTU

En este anexo se presentan las imágenes referentes al diseño del circuito de la RTU. Las siguientes dos figuras son las caras superior e inferior, respectivamente, del circuito impreso hecho en *ExpressPCB*. Ambas caras del circuito se pueden apreciar en la **Figura B. 3**. La Figura B. 4 representa el esquema de interconexión de todos los elementos que conforma el RTU.

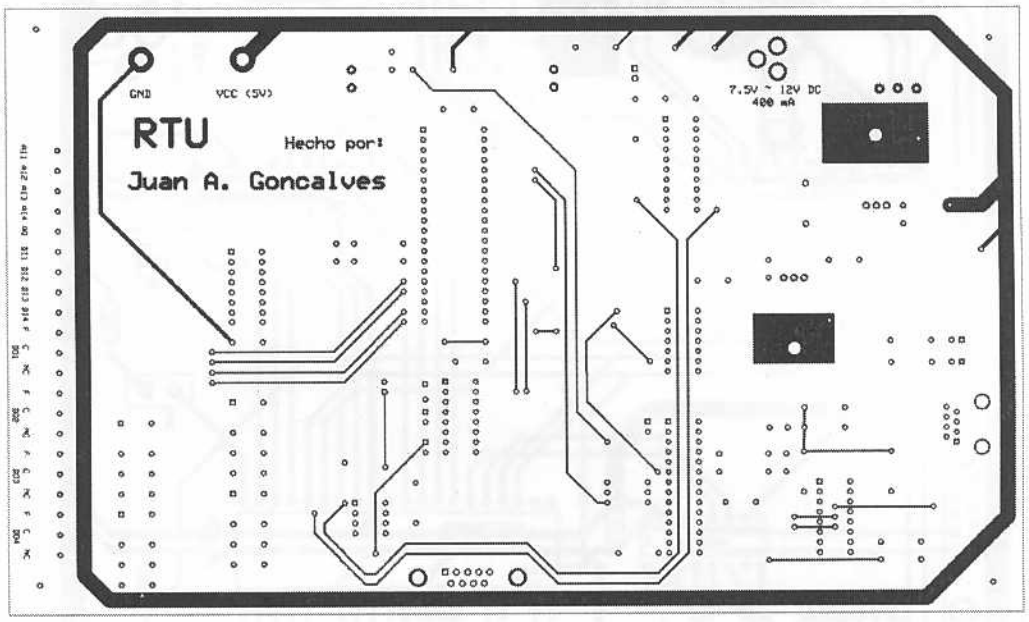


Figura B. 1. Capa superior del circuito impreso de la RTU

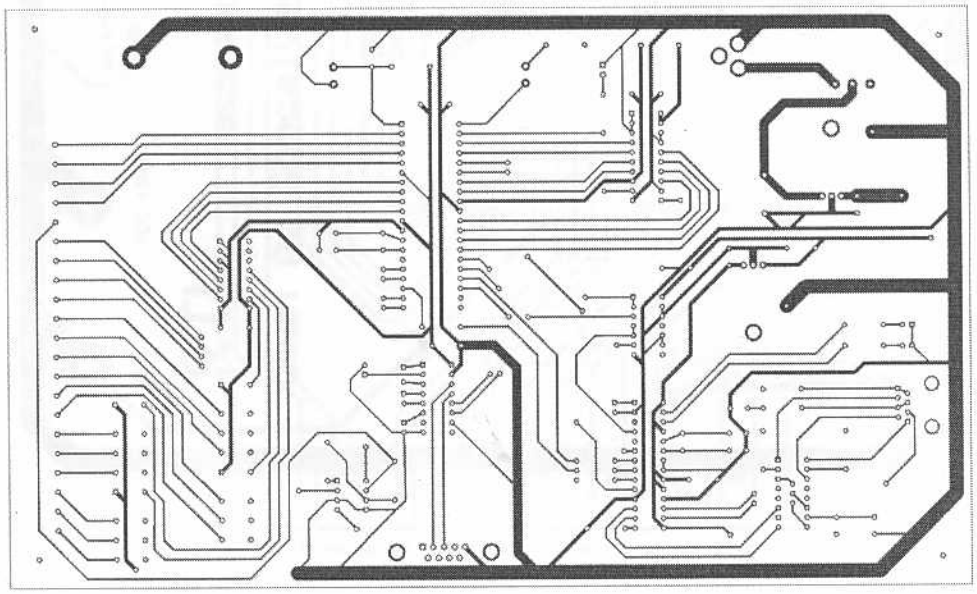


Figura B. 2. Capa inferior del circuito impreso de la RTU

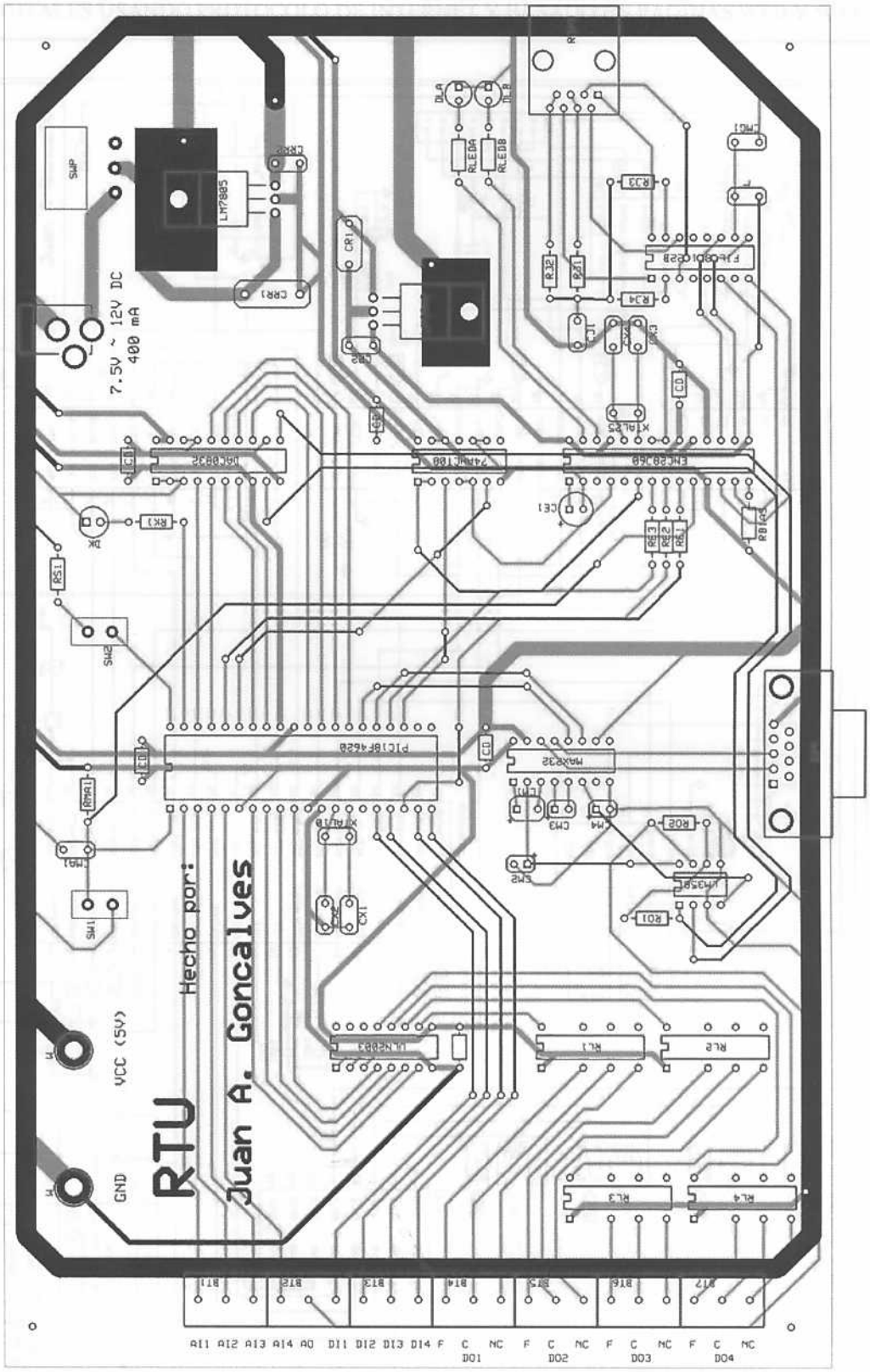


Figura B. 3. Caras del circuito impreso de la RTU

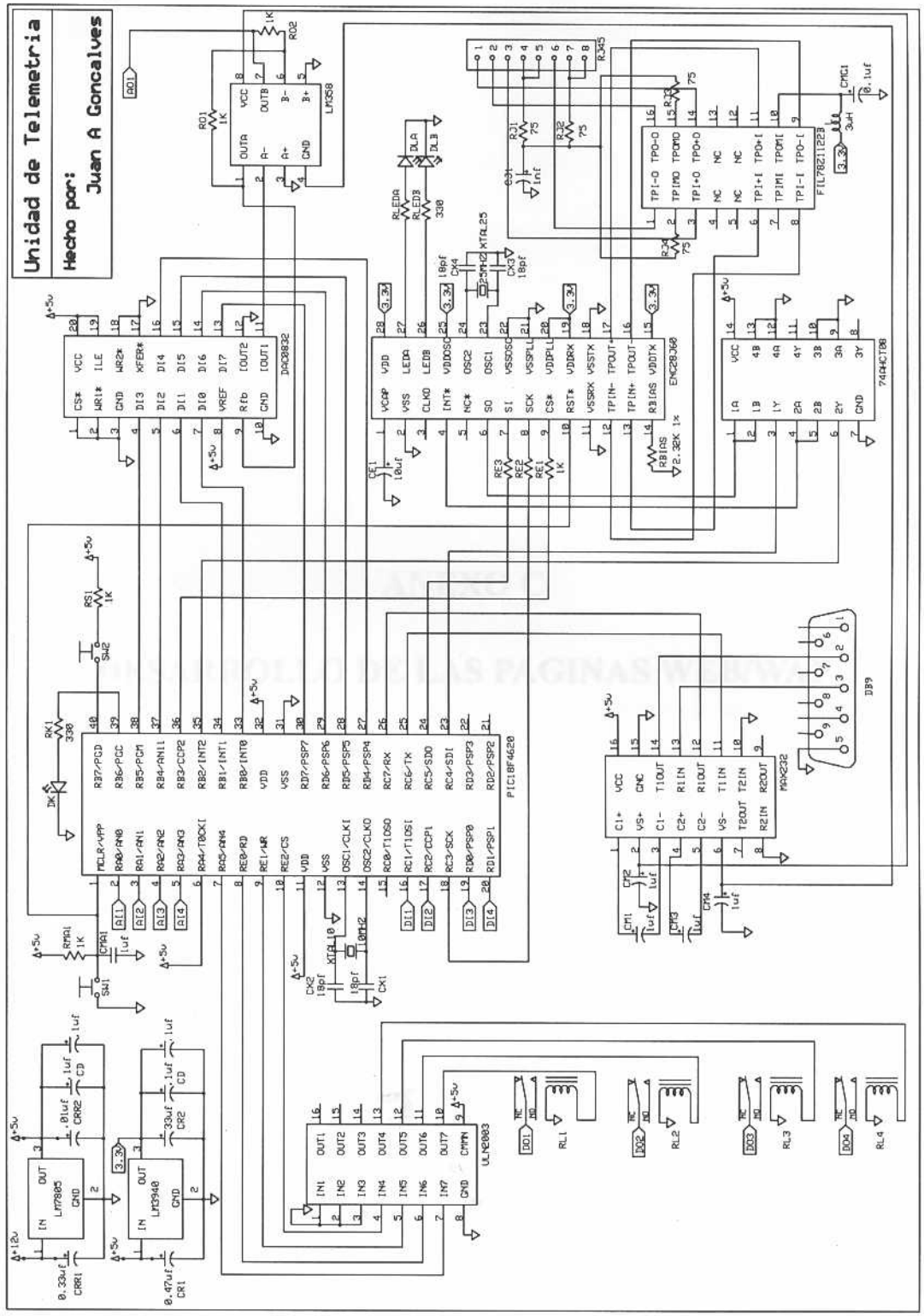


Figura B. 4. Diagrama de Interconexión de los elementos de la RTU

ANEXO C

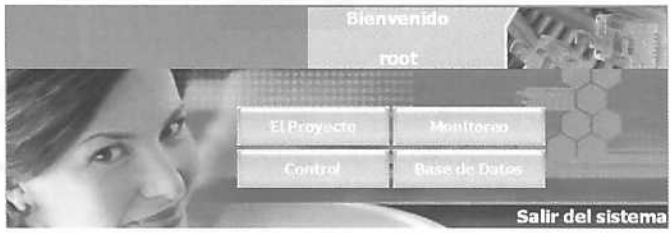
DESARROLLO DE LAS PAGINAS WEB/WAP

En este anexo se presentan un conjunto de imágenes que hacen referencia a los resultados de las páginas web/wap anteriormente comentados en el Capítulo de Resultados. Todas estas páginas están ubicadas en: http://rtu.servehttp.com y tienen como objetivo permitir el control y monitoreo de las señales en las interfaces de la RTU de una manera amigable con el usuario.

(a) (b)

Figura C. 1. Página web de autenticación

Nota. (a) Página para la autenticación (b) Formulario para el ingreso de usuario y contraseña



(a)

(b)

Figura C. 2. Accesos a las páginas según el tipo de usuario

Nota. (a) Acceso para usuarios "root" (b) Acceso para usuarios restringidos

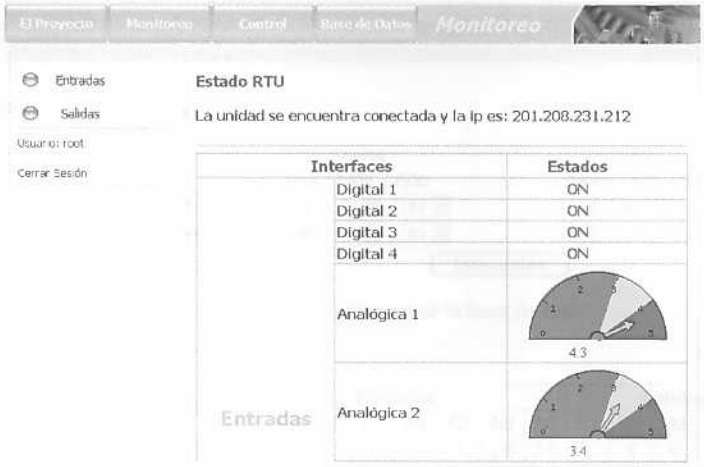


Figura C. 3. Página web para monitoreo analógico y digital

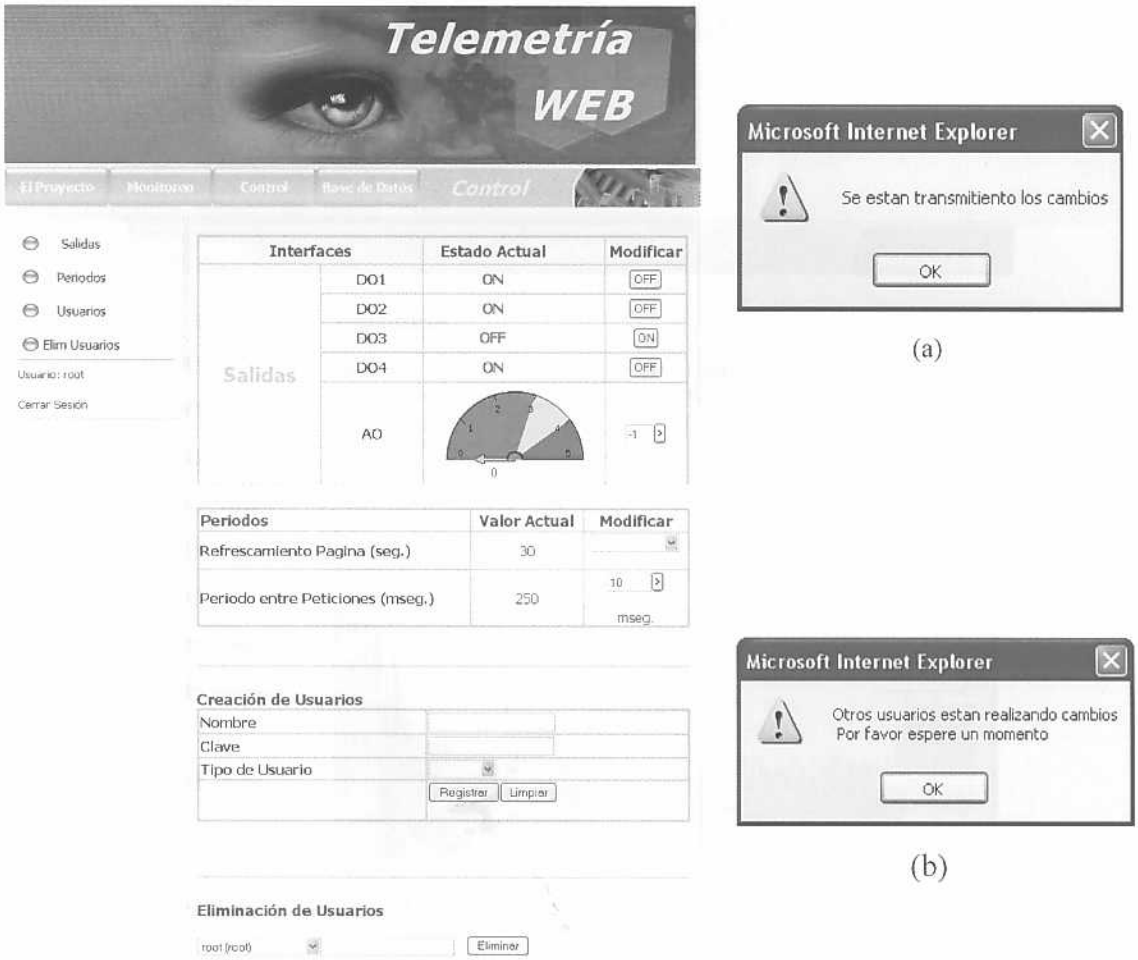


Figura C. 4. Página web para control de señales, usuarios y frecuencias

Nota. (a) Aviso de control de señales exitoso (b) Control de múltiples usuarios

Figura C. 5. Fragmento de página web de históricos almacenados en la base de datos

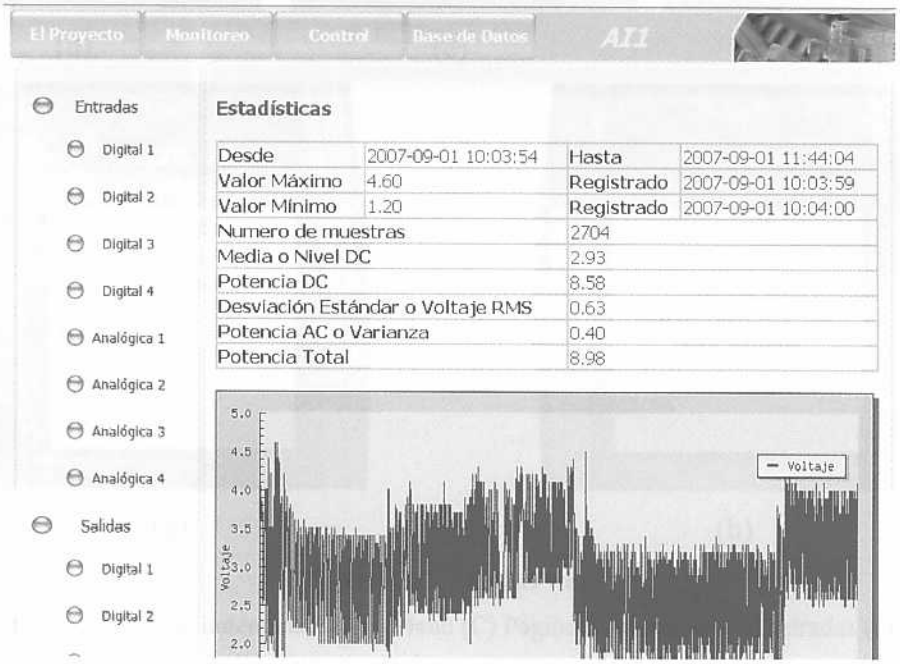


Figura C. 6. Fragmento de página web del estado estadístico de la interfaz analógica de entrada (1)

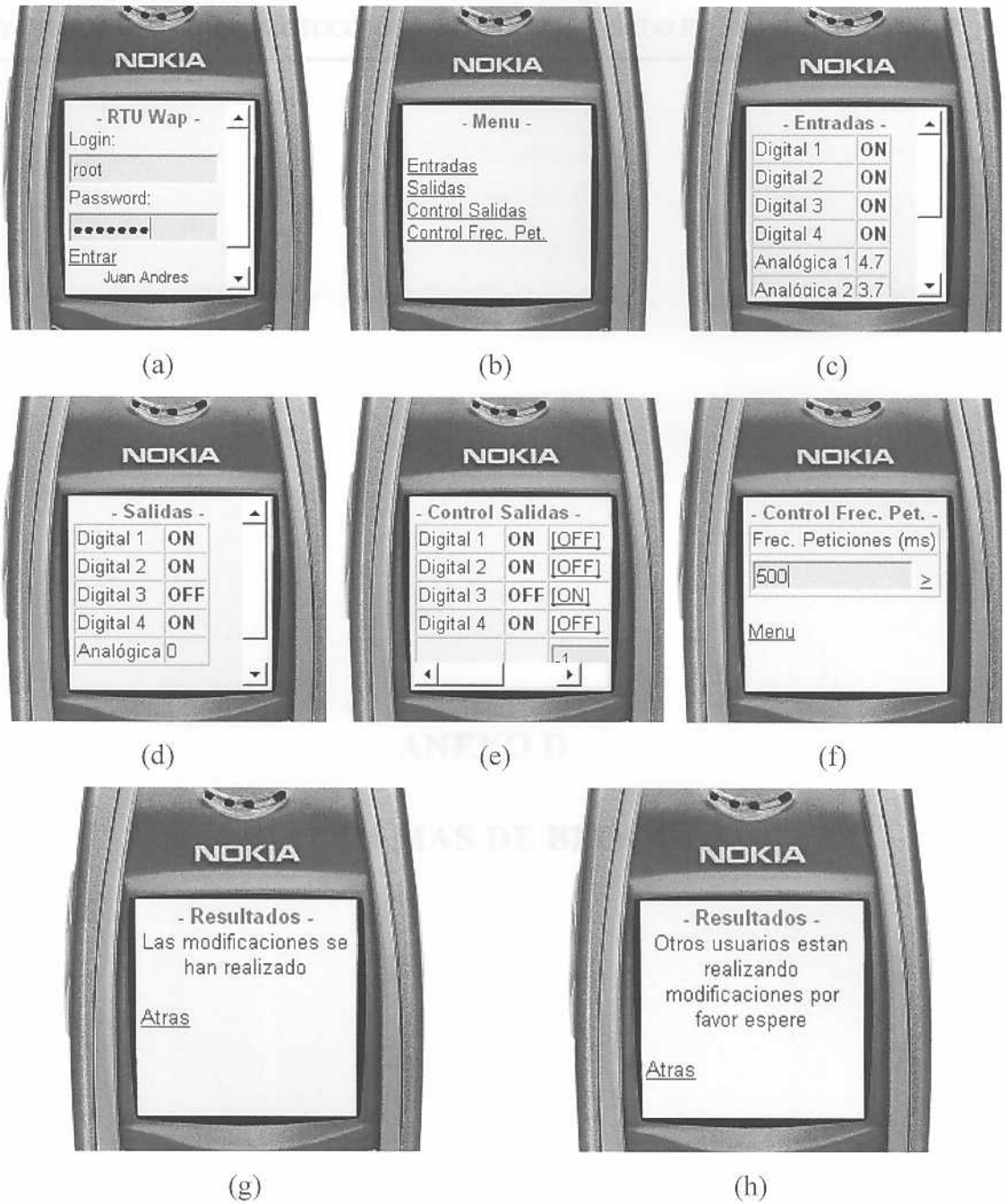


Figura C. 7. Páginas wap

Nota. (a) Página de autenticación (b) Menú (C) Página de monitoreo de entradas (d) Página de monitoreo de salidas (e) Página para control de salidas (f) Página para establecimiento de frecuencia de peticiones del UCC al RTU (g) Aviso de control exitoso (h) Control de múltiples usuarios sobre una misma interfaz

ANEXO D

DIAGRAMAS DE BLOQUES

Las siguientes imágenes son esquemas que ayudan a comprender el funcionamiento del sistema SCADA. Para empezar, la Figura D. 1 muestra el flujo de mensajes que existe entre todos los elementos del sistema SCADA interconectados en la red. Se puede apreciar como en un periodo de peticiones es necesario preguntar por el estado de las señales analógicas y digitales de entrada por separado, respetando los lineamientos del protocolo Modbus/TCP.

En las figuras D.2 y D.3 se representan, a través de diagramas de flujo, el algoritmo del demonio en el UCC y el algoritmo en el PIC respectivamente, a fin de que el lector tenga una noción general del funcionamiento de estos elementos.

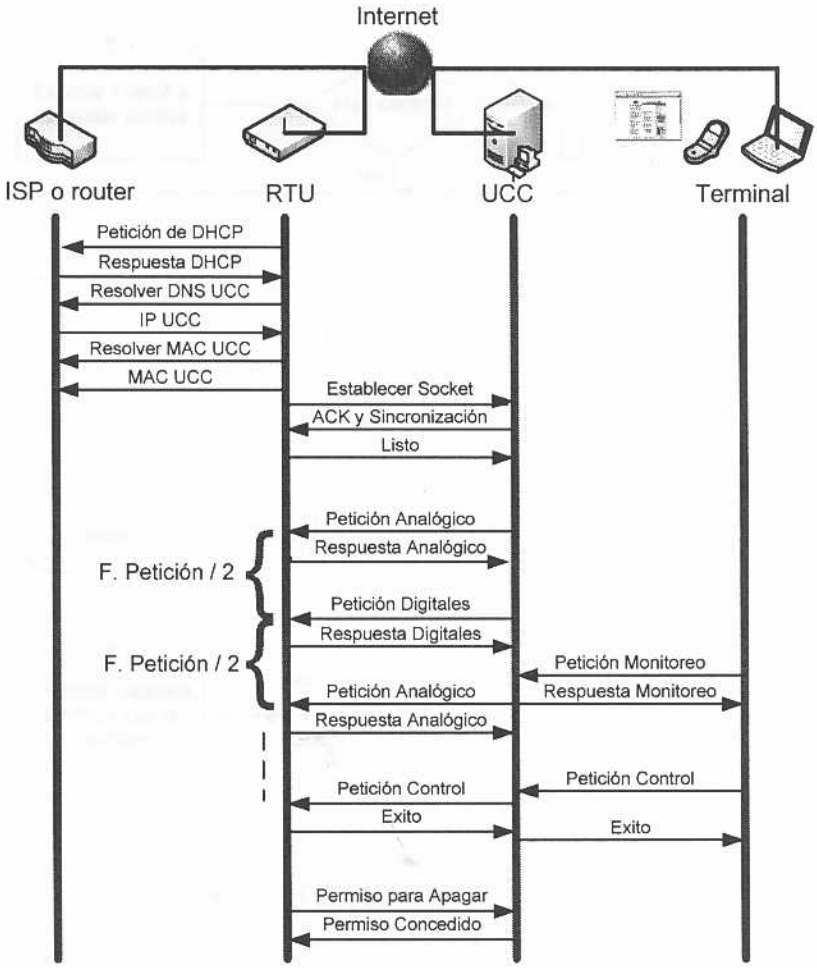


Figura D. 1. Flujo de comunicaciones del Sistema SCADA

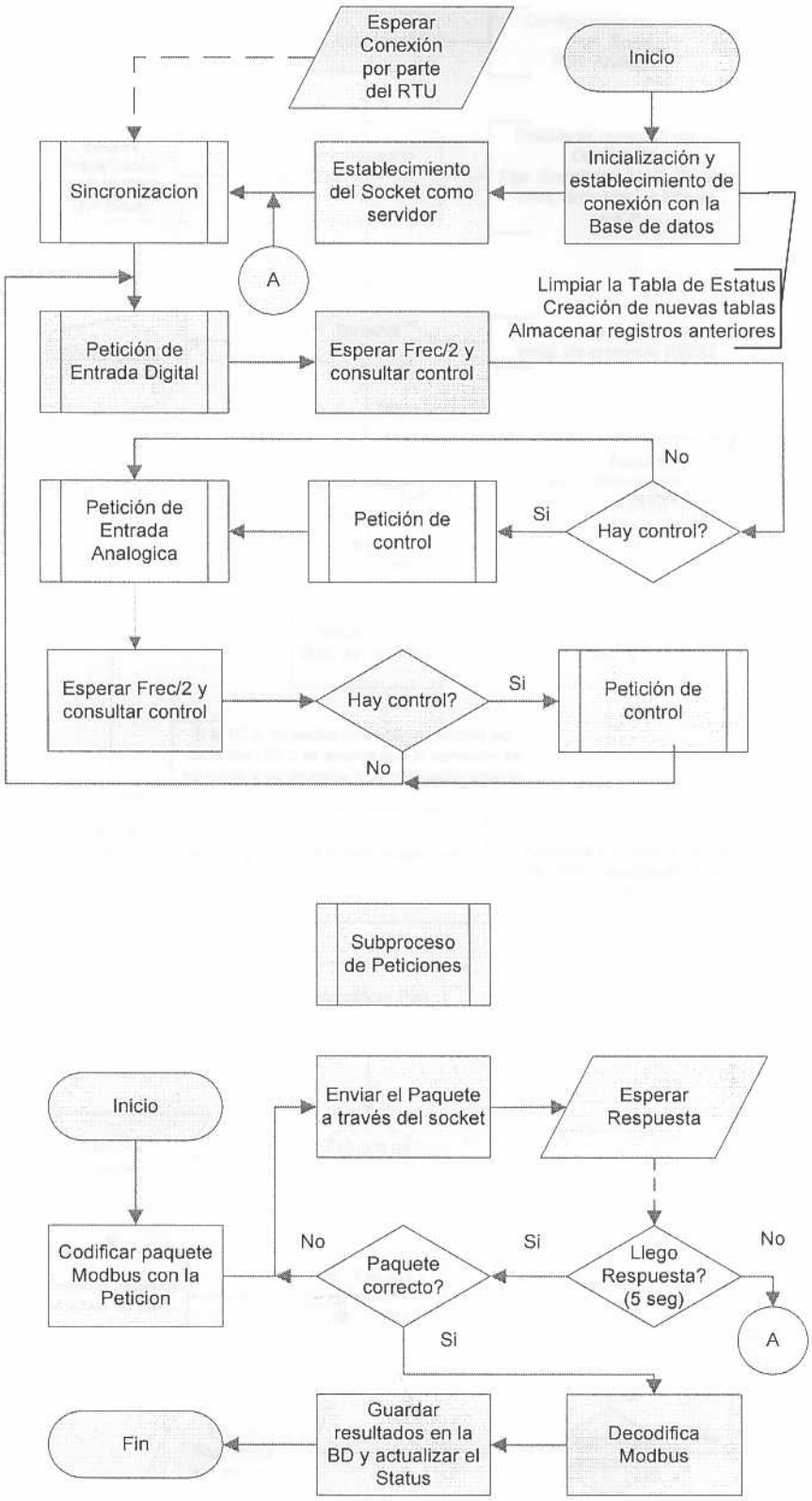


Figura D. 2. Diagrama de Flujo del algoritmo del Demonio en el UCC

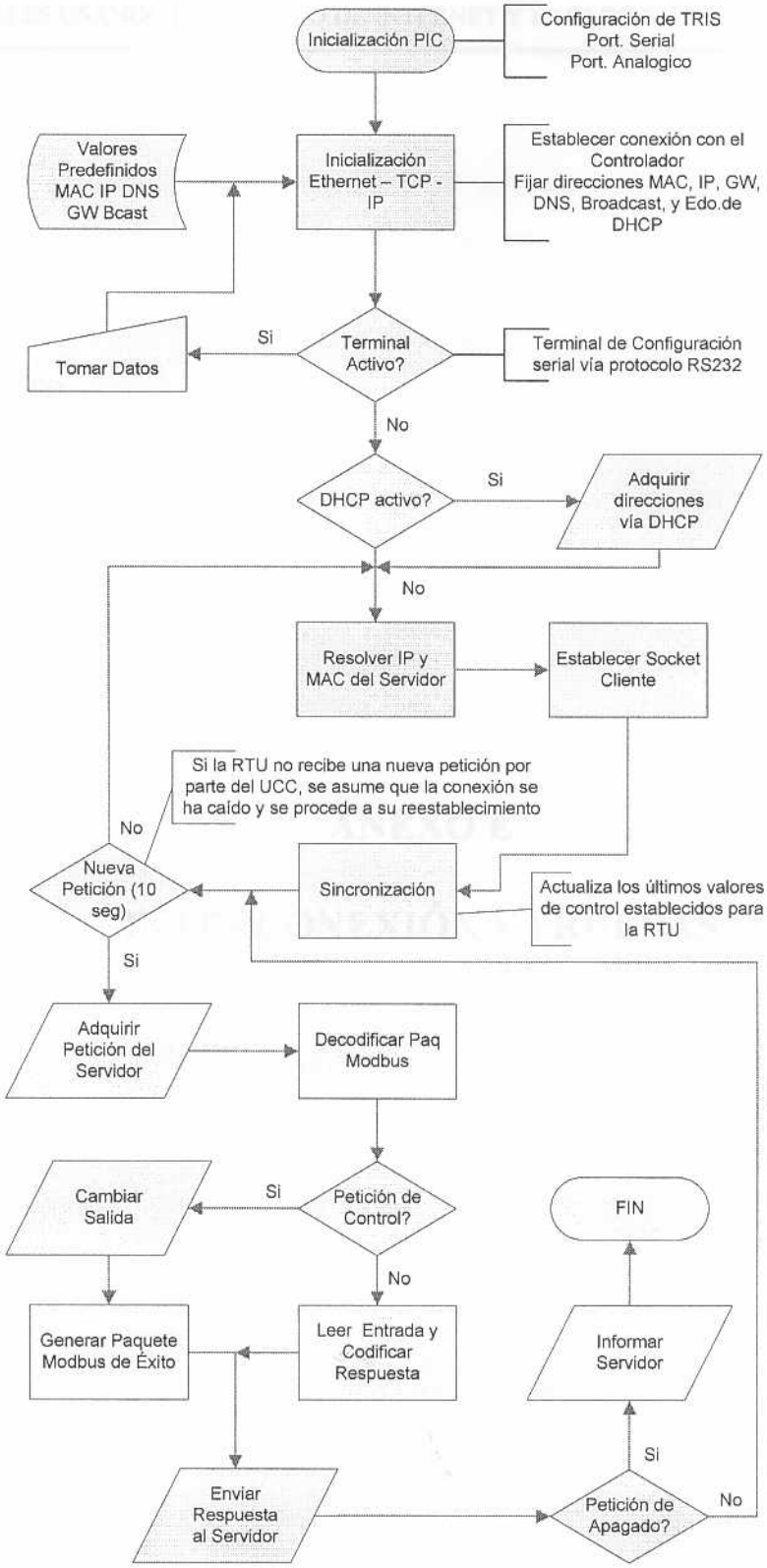


Figura D. 3. Diagrama de Flujo del algoritmo de la RTU almacenado en el PIC

ANEXO E

INTERCONEXIÓN Y PRUEBAS

1. Ambientes de Interconexión

Para las pruebas de interconexión del sistema SCADA desarrollado en este TEG, se plantearon los tres ambientes que se describen en las siguientes figuras:

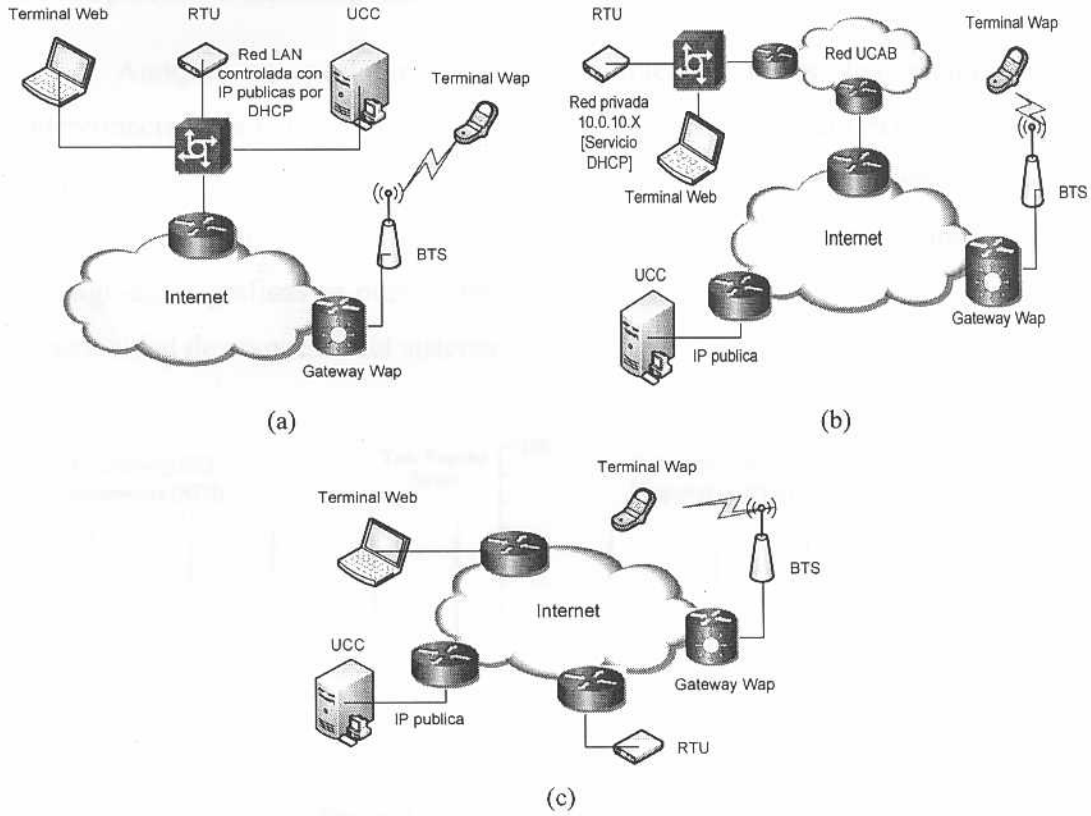


Figura E. 1. Ambientes de interconexión

Nota. (a) LAN controlada, (B) Caso UCAB, (C) Todos los elementos remotos

Para el primer caso de la LAN controlada con acceso a Internet, se contaba con un enrutador que asignaba direcciones IP vía DHCP a los tres elementos del sistema, estando directamente conectados a la red. A diferencia del mencionado ambiente, se realizaron también pruebas en la UCAB donde el UCC estaba ubicado remotamente del RTU y el Terminal; estos dos últimos detrás de la red privada de la UCAB donde la RTU y el equipo terminal tenían acceso a la red transparentemente a través del NAT de la red de la Universidad.

En el último caso, donde todos los elementos estaban conectados remotamente, era más notoria la incidencia de los retardos de la red sobre las capacidades de respuesta del sistema.

2. Capacidad de Respuesta del Sistema

Aunque en cualquiera de los ambientes todos los elementos están interconectados a la Internet, y cualquier arquitectura de interconexión es transparente para el usuario final; es obvio que la primera arquitectura le permite una mayor capacidad de respuesta al sistema en contraste con la última arquitectura. A través de las siguientes gráficas se puede observar las incidencias en el retardo de la red sobre la velocidad de respuesta del sistema.

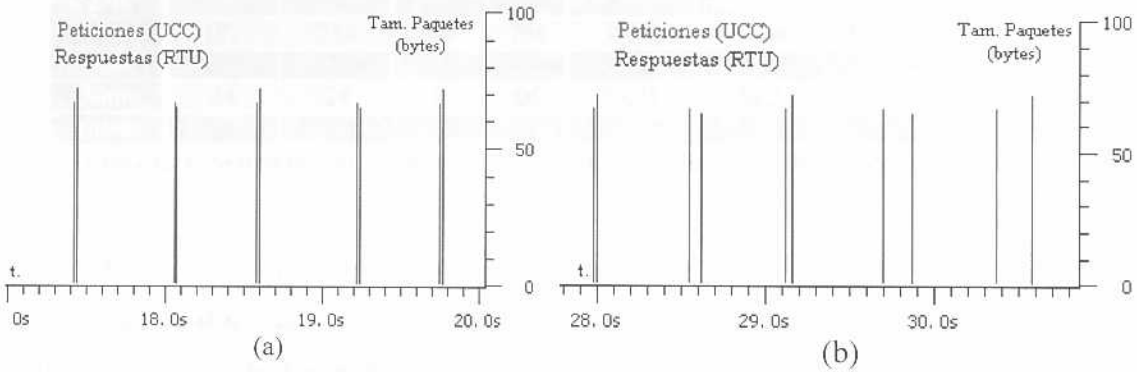


Figura E. 2. Capacidad de respuesta del RTU

Nota. Imágenes tomadas de parte de una sesión de 2 minutos de la RTU-UCC usando el software *Ethereal*. (a) LAN controlada con acceso a internet (b) todos los elementos conectados remotamente.

Se puede ver claramente como en una sesión con la RTU a un periodo de peticiones de 1seg (500ms de petición analógica, 500ms. de petición digital) el bajo retardo de la red controlada de la figura de la izquierda permite una alta capacidad de respuesta; a diferencia de lo que se puede apreciar en la otra figura, que es el caso más común cuando todos los elementos están remotamente interconectados a la Internet. Dadas las condiciones de la red por donde atraviesan los paquetes en la

última arquitectura, se pueden conseguir con retardos que alteran las capacidades de respuesta del SCADA.

No solo la red es la culpable de los retrasos en el proceso de petición y respuesta del sistema SCADA, la carga de trabajo a la que se somete el PIC influye también directamente en el desempeño del sistema. A través de las siguientes tablas se puede observar como a medida que se le exige más a la remota -a través de peticiones más frecuentes- el MCU no puede ofrecer respuesta a la cantidad de paquetes que teóricamente se espera que pueda atender.

Periodo (ms)	Muestras (2 min)		Error	Paq.	Prom. bytes/paquete		Prom bytes/s.	
	Medido	Teórico			Subida	Bajada	Subida	Bajada
Min	912	-	-	3648	59,99	63,73	1823,70	1937,39
250	312	480	168	1248	59,98	63,7	623,79	662,48
500	192	240	48	768	59,96	63,68	383,74	407,55
1000	111	120	9	444	59,93	63,63	221,74	235,43
5000	24	24	0	96	59,91	63,5	47,94	50,8
10000	12	12	0	48	59,85	63,3	23,94	25,32

Tabla E. 1. Sesión de dos minutos (RTU atendiendo peticiones digitales y analógicas)

Entre una de las tareas que ofrece más retraso en la RTU está la medición de las señales analógicas por parte del PIC, esto se aprecia en la siguiente tabla que refleja una sesión de 2 mín. donde la RTU solo atiende peticiones digitales.

Periodo (ms)	Muestras (2 min)		Error	Paq.	Prom. bytes/paquete		Prom. bytes/s.	
	Medido	Teórico			Subida	Bajada	Subida	Bajada
Min	1418	-	-	2836	59,99	61,99	1417,76	1465,03
250	421	480	59	842	59,95	61,63	420,65	432,44
500	208	240	32	416	59,93	61,21	207,76	212,19

Tabla E. 2. Sesión de dos minutos (RTU solo atendiendo peticiones digitales)

Si aparte de la carga de trabajo normal por parte de la RTU -atendiendo los paquetes Modbus/TCP- se le suma otras actividades como: ofrecer respuesta a

paquetes ICMP de la red; se presentará una disminución de sus capacidades de respuesta, la cual es más notoria a mayores frecuencias de peticiones tal y como se puede ver en las siguientes tablas.

Periodo (ms)	Muestras (2 min)		Error	Paq.	Prom. bytes/paquete		Prom. bytes/s.	
	Medido	Teórico			Subida	Bajada	Subida	Bajada
Min	749		-749	3116	60,53	64,14	1571,79	1665,53
250	290	480	190	1280	61,29	64,67	653,72	689,77
500	186	240	54	864	61,99	65,22	446,34	469,61

Periodo (ms)	*Pings*	% Respuesta *Pings*	Prom T Resp. (ms)	% de caída de la capacidad de Resp.
Min	120	100	2	17,87%
250	120	100	2	7,05%
500	120	100	2	3,13%

Tabla E. 3. Sesión de dos minutos (RTU atendiendo también ICMP)

A fin de evitar mayores retrasos en el sistema, se aconseja apagar el terminal de la RTU vía interfaz serial, la cual también ofrece grandes retrasos como los que se pueden contrastar entre la Tabla E. 1 y la siguiente tabla, que muestra una sesión de dos minutos a distintas frecuencias de peticiones con el terminal operando.

Periodo (ms)	Muestras (2 min)		Error	Paq.	Prom. bytes/paquete		Prom bytes/s.	
	Medido	Teórico			Subida	Bajada	Subida	Bajada
Min	510		-510	2040	59,99	63,75	1019,83	1083,75
250	286	480	194	1144	59,97	63,70	571,71	607,27
500	178	240	62	712	59,96	63,68	355,76	377,83
1000	101	120	19	404	59,94	63,63	201,80	214,22
5000	23	24	1	92	59,73	63,29	45,79	48,52
10000	12,00	12,00	0	48	59,30	62,66	23,72	25,06

Tabla E. 4. Sesión de dos minutos (RTU con el terminal serial activado)

3. Anchos de Banda

Otra conclusión que se extrae de todas estas tablas es el ancho de banda por paquete y por segundo que consume los procesos de comunicación UCC-RTU, los cuales concuerdan con los calculados teóricamente:

Protocolo	Tamaño del encabezado (bytes)
Paquete Modbus	2 - 9
Frame TCP	20
Datagrama IP	20
Paquete Ethernet	14
Total	64 – 71

Tabla E. 5. Tamaño por paquete estimado teóricamente

La cantidad de bytes por paquete que consume Modbus/TCP es variable y depende de su función y si es un paquete de petición o respuesta:

Campo	ID de Transacción	ID Protocolo	Tamaño	ID de la Unidad	Código de la Función	Data
Tamaño (bytes)	2	2	2	1	1	*

Tabla E. 6. Tamaño del paquete Modbus/TCP

Función	Código	Tamaño Petición (b)	Tamaño Respuesta. (b)
Lectura Digital	01h	4	2
Lectura Analógica	04h	4	9
Control Digital	05h	4	4
Control Analógico	06h	4	4

*** Tabla E. 7. Tamaño del campo de datos Modbus/TCP**

Como se puede ver, el ancho de banda máximo, medido utilizando la herramienta *Ethereal,* es de: 1.46Kbps (en el caso que solo se atiendan peticiones de señales digitales a una tasa de 11.8 muestras por segundo). De esta manera, se pueden

muestrear perfectamente señales digitales con un BW de 5.9Hz, con condiciones adecuadas de la red.

Sin embargo, es importante considerar que en el caso que se estén muestreando señales digitales y analógicas al mismo tiempo, estas no podrán ser de un ancho de banda mayor a: 3.8Hz, siempre y cuando se desee una muestra fidedigna de las señales tanto analógicas como digitales en las interfaces de la RTU, en condiciones adecuadas de la red.

4. Funcionamiento del Protocolo Modbus/TCP

Todas estas pruebas también permitieron corroborar el correcto funcionamiento de las funciones programadas, tanto en la RTU como en el UCC, encargadas de establecer las sesiones Modbus/TCP. A través del analizador de protocolos *Ethereal,* se constató la correcta formación de estos paquetes, ya que el analizador es capaz de determinar la naturaleza de los flujos de paquetes Modbus/TCP, tal y como se aprecia en la siguiente figura.

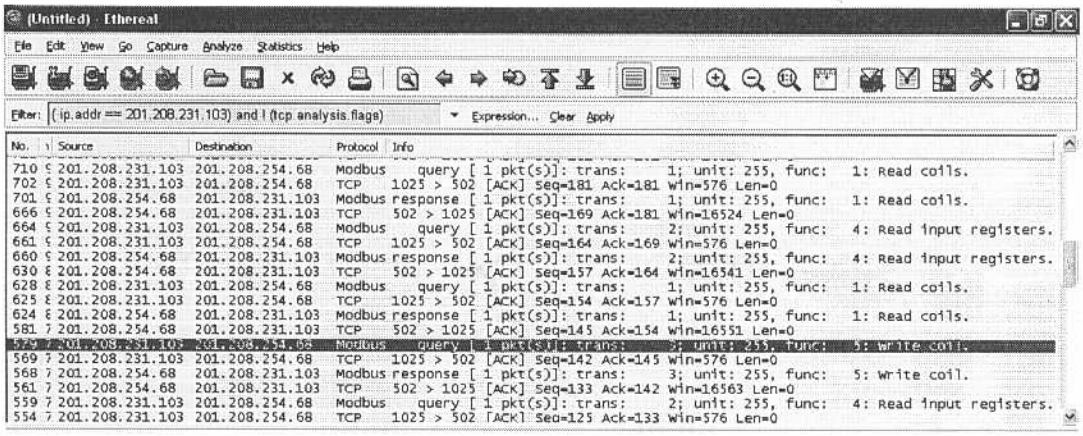


Figura E. 3. Flujo de paquete en sesión Modbus/TCP

Imagen tomada de una parte de una sesión de dos minutos entre el UCC-RTU utilizando *Ethereal* y filtrando solo los paquetes desde y hacia la RTU

ANEXO F

REFERENCIAS TÉCNICAS

En este anexo se describen las características técnicas del sistema, que pueden ser útiles para el mejor uso del sistema de telemetría. Este anexo está estructurado de tal manera que comienza con la descripción de cada interfaz de control y supervisión de la RTU, terminando con los ajustes que el usuario puede realizar al sistema desde los portales.

1. RTU

La unidad cuenta con las siguientes interfaces de monitoreo y control

Tipo de señal	Rango de Voltaje (V) [a]	Max. Corriente (mA) [b]	Máximo BW (Hz) [e]	Acción	Cantidad
Analógica	0 – 5.1	25 [b]	3.8	Entrada	4
	0 – 5.1	40 [c]	3.8	Salida	1
Digital	0 y 5.1	25 [b]	5.9 – 3.8	Entrada	4
	0 -120 [AC] 0 -24 [DC] [d]	2000 [AC] 2000 [DC] [d]	5.9 - 3.8	Salida	4

Tabla F. 1. Interfaces de la RTU

Nota. [a] Obtenido de valores prácticos medidos. [b] Valores obtenidos de (microchip, 2004, p. 323). [c] Valor obtenido de (*National Semiconductor*, 2005, p. 7). [d] indicado en el Relé [e] Valores obtenidos de pruebas de estrés en condiciones especiales.

La interconexión de las señales se puede hacer a través de los bloques terminales, los cuales tienen impreso el tipo de señal que trata, tal y como se aprecia en la siguiente figura.

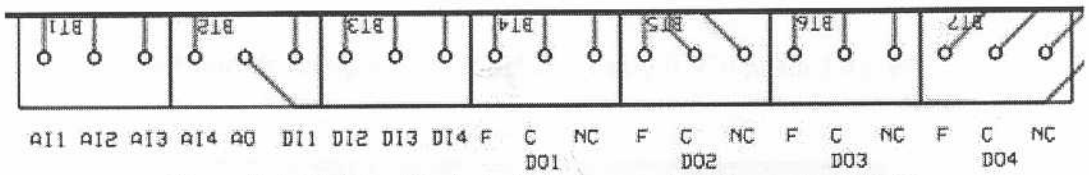


Figura F. 1 Distribución de las interfaces en los bloques terminales

Donde las siglas representan:

AIX: Entrada analógica (4 entradas). Utilizado para medir temperatura; intensidad de corriente o de voltaje; presión; peso; entre otras señales fluctuantes de baja frecuencia que, a través de transductores, son transformadas las magnitudes de los fenómenos físicos y químicos en señales equivalentes eléctricas analógicas.

AO: Salida analógica (1 salida). Utilizado para controlar presión; temperatura; luminosidad; velocidad de motores, ente otros equipos que admiten valores fluctuantes. Estos dispositivos se basan en el mismo procedimiento de las entradas analógicas, pero envían un valor escalable eléctrico al equipo terminal conectado.

DIX: Entrada Digital (4 entradas). Ideal para conocer los estados de interruptores, válvulas, motores; alarmas; entre otras señales de naturaleza binaria.

DOX: Salida Digital (4 salidas). Empleado para comandos de apertura y cierre de interruptores; encendido/parada de motores; válvulas; etc. En esta interfaz, la conexión se realiza a través de un relé. En los bloques terminales se tiene acceso a los terminales fijos (F), conectados (C) y no conectados (NC) de los cuatro relés que representan las salidas digitales controladas por la unidad remota.

En cuanto a la alimentación de la unidad remota se ofrece dos medios, descritos en la siguiente tabla y dispuestos en el circuito de la RTU como se aprecia en la figura.

Configuración	Voltaje (V)	Corriente (mA)
Transformador de Pared	7.5 - 15	340
Desde Fuente regulada	TTL (5)	335

Tabla F. 2 Características eléctricas del RTU

El consumo de energía de la RTU está entre 0.976 hasta 1.45 W

Consumo	Voltaje (V)	Corriente (mA)	Potencia (W)
Mínimo	4.65	210	0.976
Máximo	4.53	320	1.45

Tabla F. 3 Consumo eléctrico de la RTU

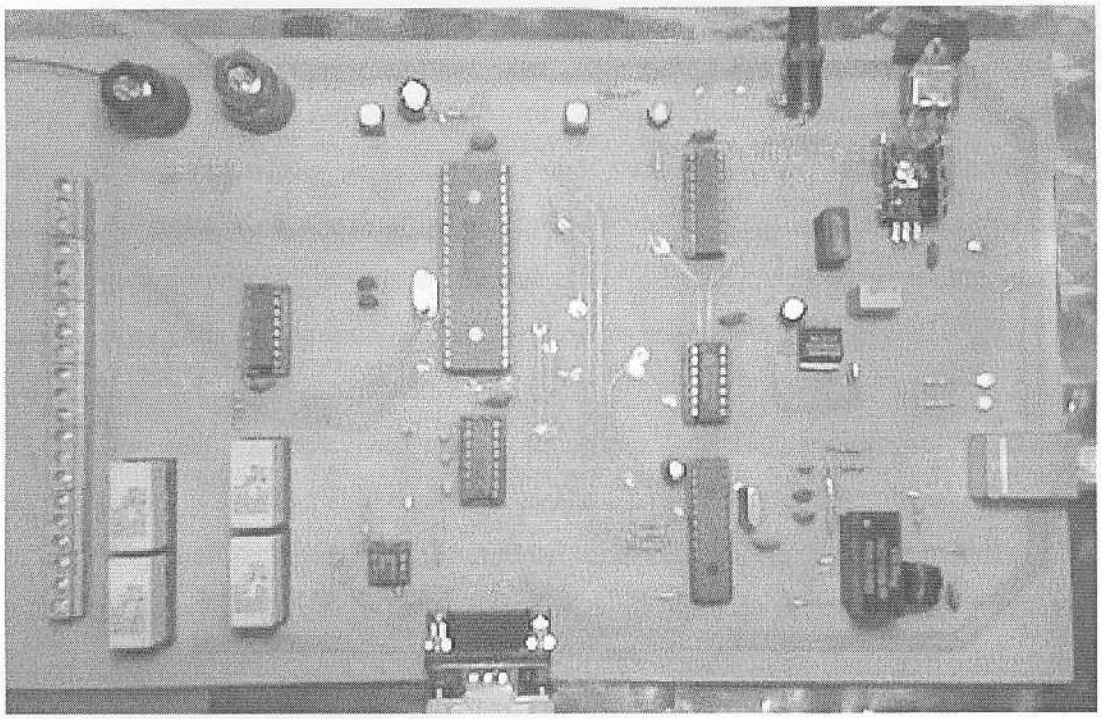


Figura F. 2 Distribución de las interfaces en la RTU

Para dotar de conectividad a la RTU, se emplean los siguientes módulos de comunicaciones para las operaciones que se indican:

Protocolo	Terminal	Max BW [Kbps].	Uso
RS232	DB9	19.2	Configuración vía Terminal
802.3 10BaseT	RJ-45	1.46	Comunicación con la UCC

Figura F. 3 Módulos de Comunicaciones

Dispuestos como se ve en la Figura F. 2, el módulo 802.3 10BaseT -vía terminal RJ-45- permite el establecimiento de la conexión RTU-UCC para las respectivas peticiones de supervisión y control; en cambio, el módulo RS-232 –vía conector DB9- se utiliza solo para configuración de parámetros de red de la RTU utilizando un terminal serial a 19200 bps 8N1 y sin control de flujo.

2. Páginas de Control

Con el fin de ajustar los periodos de peticiones de medición de las señales ubicadas en las interfaces de la RTU, se puede modificar estos valores en la página de control del portal web. De esta forma, dependiendo de la naturaleza de la señal digital o analógica de entrada, se puede adecuar el periodo de muestreo para obtener desde una muestra cada 20 segundo, hasta 7.6 muestras/segundo.

De esta manera, se puede muestrear señales analógicas y digitales simultáneamente con un BW de hasta 3.8 Hz. En caso de atender solo mediciones de señales digitales, se puede perfectamente muestrear dichas señales a hasta 5.9Hz modificando adecuadamente los parámetros de periodo de peticiones del portal web. De esta manera, el usuario puede introducir una frecuencia de muestreo adecuada en casos de señales de naturaleza muy variante con respecto al tiempo y así obtener una fiel representación de la señal.

3. Conexión

Se recomienda prestar atención a los retardos que pueda tener la red de interconecta todo el sistema, sobre todo en caso de realizar monitoreo y control a señales muy variantes con respecto al tiempo.

Se hace esta advertencia ya que en condiciones adversas de la red, el sistema no puede muestrear las señales a la frecuencia máxima esperada. Este efecto se debe a los retrasos en la transmisión de los valores desde la RTU hasta la UCC. En conclusión, en caso de realizar monitoreo a señales con anchos de banda exigentes, se recomienda la interconexión de todos los equipos involucrados en una LAN controlada con un retardo reducido. En caso de que las exigencias sean mínimas, el sistema se comporta muy bien en cualquier tipo de conexión a nivel de LAN o WAN.

ACRÓNIMOS

ADSL: Asymmetric Digital Subscriber Line

API: Application Programming Interface

ARP: Address Resolution Protocol

BD: Base de Datos (DB en Ingles)

CAN: Controller Area Network

CGI: Common Gateway Interface

CIR: Commited Information Rate

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

EUSART: Enhanced USART

FTP: File Transfer Protocol

HTML: Hyper Text Markup Language

HTTP: Hyper Text Transfer Protocol

HTTPS: HyperText Transfer Protocol Secure

I2C: Inter-Integrated Circuit

ICMP: Internet Control Message Protocol

IDE: Integrated Development Environment

IP: Internet Protocol

ISP: Internet Service Provide

MIME: Multipurpose Internet Mail Extensions

NNTP: Network News Transport Protocol

PDIP: Plastic dual in-line package

QFN: Quad Flat pack No lead

QoS: Quality of Service

RTU: Remote Terminal Unit

SCADA: Supervisory Control and Data Acquisition

SMTP: Simple Mail Transfer Protocol

SO: Sistema Operativo (OS en ingles)

SPI: Serial Peripheral Interface

SPI: Serial Peripheral Interface.

TCP: Transmission Control Protocol

TEG: Trabajo Especial de grado

TQFP: Thin Quad Flat Pack

UCC: Unidad Central de Control

UDP: User Datagram Protocol

URL: Uniform Resource Locator

USART: Universal Synchronous / Asynchronous Receiver / Transmitter

WML: Wireless Markup Language

XML: eXtensible Markup Language