CHAPTER III

PROPOSED SYSTEM

Following the analysis about the faced problems in the previous studies and the motivation, this chapter will bring the theoretical design of the intended system. Detailed implementation will be given in chapter 4.

This chapter starts first with the features to be achieved with the proposed solution. Secondly, a review about the basic technologies needed to build the system, and then the draft picture about the whole system is presented. The description about the inside of the system is given in the final part of the chapter.

3.1 System's Features

The system solution is built based on the Ethernet and Internet, allowing users the ability to remotely monitor data and issue the supervisory control commands on field devices or a process in a specific application, via web-enabled interfaces. It can provide the following main functions:

- Automatically collect the latest data from field devices in a real-time manner.
- Real-time data are displayed on the popular web-browser interfaces such as Internet Explorer (IE) or Avant Broswer, for the data monitoring purpose.
- System's users can issue control commands from any place equipped with an Internet connection.

These three features above are the basic functions of any SCADA system and they reflect the nature of SCADA system as mentioned. The solution presented in this research will provide these three functions with the presence of Internet.

- The server/client model is used together with the latest technologies which are .NET Framework 2.0, Internet Information Services (IIS) 5.1, MySQL 4.1, and Active Server Page (ASP.NET) 2.0.

These software tools are developed by Microsoft Corp. For the time being, the version chosen are the most updated ones. The main programming language to be used is Visual C Sharp (VC#). All of these tools once used will give out a web-based application with high performance and a good system management feature.

- System's security issue is carefully considered with two levels of protection:

1. **Router Level →** 2. **Server Application**

Router Level provides the protection with the existing hardware features, **Server Application** will provide the protection by software tools.

- Alarm/Warning/Caution

Whenever the data collected from the device exceed a given limit or threshold, an alarm will be given at both the device side and on the HMI screen. The system operator can then give proper actions to handle the unwanted phenomena.

- Event Logs

With this tool, any event or action which has happened in the system will be recorded.

- Using IP addresses, a new device can be added or deleted or field devices can be tracked without big difficulties.

This is an Internet-based SCADA system where the system's devices are made available in the network by IP addresses. It is conceptually similar to an IP-network where all the entities are managed by their IP addresses.

- The speed and time of transferring data can also be tracked with the software's features.

Once the data are sent into the Internet network, we might not be able to control the transfer speed of that data since the speed depends much on the traffic intensity on the Internet. However, the use of ADSL technology promises to give us an acceptable speed and ensure the real-time fashion of the system performance. The actual data transfer speed and data transferring time are displayed on the HMI screen in order to give a visual view about the operation of the system.

All the system's features are presented above. The following part will be the conceptual presentation about all the basic technologies to be used in designing the system.

1.7 Basic Technologies

The following knowledge is about the related technologies used in building the solution with the focus put on the Client/Server model since it is the core frame of the proposed system. The advantages and the reasons for them to be used are also mentioned.

3.2.2 Internet architecture

Internet is a technical term used to talk about the connection among heterogeneous networks, in order to share resources and perform some common services.

The basic hardware component used to connect heterogeneous networks is a *router.* Each router is a special-purpose computer dedicated to the task of interconnecting networks. Like a bridge, a router has conventional processor and memory as well as a separate Input/Output (IO) interface for each network to which it connects. Computers can be attached to each network. A router can connect two Local Area Networks (LANs), a LAN to a Wide Area Network (WAN), or two WANs.

- LANs may have a variety of designs. LANs normally cover a small geographical area (e.g., a single building or plant site) and provide high bandwidth with low delays.
- WANs: Geographically dispersed hosts and LANs are interconnected by wide-area networks, also called long-haul networks. These networks may have a complex internal structure of lines and packet-switches, or they may be as simple as point-to-point lines

Those networks can be of different technologies, including different media, physical addressing schemes or frame formats.

The general architecture of internet is illustrated in Figure 3.1 below:

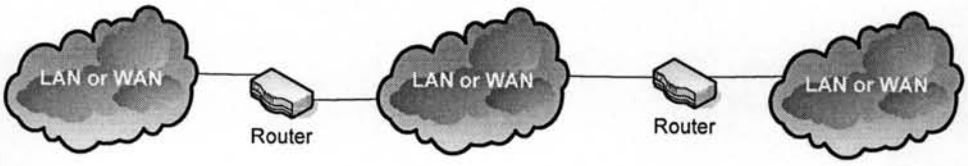

Figure 3.1 Internet Architecture

In Figure 3.1, a router can connect two single networks, but in some cases, a router can connect more than two constituent networks to establish an internet.

By interconnecting among different networks at different places, internet allows the distance-independent communication. The router must agree to forward information from a source on one network to a specified destination on another. This task is complex since the data frame formats and addressing schemes used by the underlying networks may differ. As a result, we need a common protocol on all computers and routers to make it possible to share resources on internet. TCP/IP is now the most common used protocol for all types of communication over internet.

3.2.2 Ethernet

Ethernet is a standard communications protocol embedded in software and hardware devices, intended for building a LAN. Ethernet was designed by **D**igital, **I**ntel and **X**erox; "DIX" Ethernet then became the standard model for LANs worldwide.

A basic hard-wired LAN consists of the following components:

- Two or more computers to be linked together, or networked.
- A Network Interface Card (NIC) in each computer.
- Ethernet cable to connect to each computer.
- A networking switch or networking hub to direct network traffic.
- Networking software.

An NIC is installed in each computer, and is assigned a unique address. An Ethernet cable runs from each NIC to the central switch or hub. The switch or hub will act as a relay, receiving and directing data frames across the LAN. Thus, Ethernet networking creates a communications system that allows the sharing of data and resources, including printers, fax machines and scanners.

3.2.4 ADSL Technology

To understand what ADSL is, we should first understand what DSL is. DSL, which stands for Digital Subscriber Line, is a family of technologies that provides the digital data transmission over the wires of a local telephone network. Typically, the download speed of DSL ranges from 640 kilobits per second (kbps) to 3,000, or exceptionally from 128 to 24,000 kbps depending on DSL technology and service level implemented.

ADSL, which stands for Asymmetric Digital Subscriber Line, is a version of DSL technology. ADSL enables faster data transmission over copper telephone lines by utilizing frequencies that are normally not used by a voice telephone call, in particular, frequencies higher than normal human hearing. This signal will not travel very far over normal telephone cables, so ADSL can only be used over short distances, typically less than 5 kilometers. Once the signal reaches the telephone company's local office, the ADSL signal is stripped off and immediately routed onto a conventional internet network, while any voice-frequency signal is switched into the conventional phone network. This allows a single telephone connection to be used for both ADSL and voice call at the same time.

The distinguishing characteristic of ADSL over other forms of DSL is that the volume of data flow is greater in one direction than the other, i.e. it is asymmetric. ADSL uses two separate frequency bands, referred to as the upstream and downstream bands. The upstream band is used for communication from the end user to the telephone central office. The downstream band is used for communicating from the central office to the end user. With standard ADSL, the band from 25.875 kHz to 138 kHz is used for upstream communication, while 138 kHz – 1104 kHz is used for downstream communication. Each of these is further divided into smaller frequency channels of 4.3125 kHz. During initial training, the ADSL modem tests which of the available channels have an acceptable signal-to-noise ratio. The distance from the telephone exchange, or noise on the copper wire, may introduce errors on some frequencies. By keeping the channels small, an error on one frequency thus needs not render the line unusable: the channel will not be used, merely resulting in reduced throughput on an otherwise functional ADSL connection.

ADSL technologies use a synchronous framed protocol for data transmission on the wire.

3.2.4 Client/Server Structure:

Traditional applications are self-connected monolithic programs that have limited access to one another's procedures and data. They are usually cumbersome to build and expensive to maintain because even simple functional changes require the entire program to be rewritten, recompiled, and re-tested. By contrast, the client/server structure provides the scalability and robustness required to support mission-critical applications throughout the enterprise comprising thousands of users.

Client/server is a network architecture which separates a client (often an application that uses a graphical user interface) from a server. Each instance of the client software can send requests to a server. Specific types of servers include: application servers, file servers, terminal servers, and mail servers. While their purpose varies somewhat, the basic architecture remains the same.

Characteristics of a server:

- Passive (Slave)
- Waits for requests
- Upon receipt of requests, processes them and replies

Characteristics of a client:

- Active (Master)
- Sends requests
- Waits for and receives replies from server

Servers can be stateless or stateful. A stateless server does not keep any information between requests. A stateful server can remember information between requests.

General client/server architectures have two types of nodes on the network: clients and servers. As a result, these generic architectures are sometimes referred to as "two-tier" architectures. Some networks will consist of three different kinds of nodes: server, application servers which process data for the clients, and database servers which store data for the application servers. This configuration is called three-tier architecture.

The advantage of an n-tier architecture compared with a two-tier architecture (or a three-tier with a two-tier) is that it separates out the processing that occurs to better balance the load on the different servers; it is more scalable. The disadvantages of n-tier architectures are:

- It puts more load on the network
- It is more difficult in term of building and testing the system software since more devices need to present in any user's transaction

Advantages of Client/Server model:

- All the data are stored at the servers, so it has better security control ability. The server can control access and resource to make sure that only those permitted users can access and change data
- It is flexible for updating the data or other resources
- There are already many matured technologies designed for Client/Server paradigm which ensure security, the user-friendliness of the interface, and ease of use
- Any element of a C/S network can be easily upgraded

Disadvantages of Client/Server model:

- Traffic congestion has always been a problem. When a large number of clients send requests to the same server at the same time, they might cause a lot of troubles for the server. The more clients there are the more troubles the server has.
- Client/Server paradigm does not have a good robustness. When the server is down, clients' requests cannot be fulfilled.

- The software and hardware requirements of a server are quite strict. A conventional computer might not be able to serve as a server. It needs more upgrades and the cost will increase accordingly.

3.2.5 Network Programming:

Networking enables programs to retrieve information stored in computers located anywhere in the world.

Network programming involves writing computer programs that communicate with other programs across a computer network. The program initiating the communication is client, and the program waiting for the communication to be initiated is the server. By doing so, a communication link called a connection is established. When the client establishes a connection, it is able to send requests which the server fulfills by performing some service to the connecting program.

By nature, network programming refers to the communication among different computers. It brings the ability to open any working network to a wider range, which will better serve for the increasing requirements of industrial processes.

Beside the advantages stated above, network programming is suitable and ideal for the SCADA projects for two reasons:

- The SCADA real-time data can be accessed by an authorized user anywhere. This satisfies the need of gaining access and being able to control the process without being present at the field.
- No special hardware investment is needed for Internet access. This is a big advantage of Internet over other types of network such as radio, GPRS or leased lines. Besides, Internet is a very common term with most people and using Internet enables the easy-to-use feature of the proposed solution.

However, network programming requires more efforts since there are more entities in the network involved in each communication. Working in any type of network brings the worry about the security issue. System's data might be caught by un-wanted people or even outsiders can gain access to take control of the entire system. We may also have to face the attacks whose purpose is to give bad control commands on system's devices or even to destroy the system.

Nevertheless, since network programming is required for the needs of expanding the communicating area, we will have to take the security matter seriously considered and implement more tools to ensure the safe and secure operation of our system.

1.8 General System Architecture

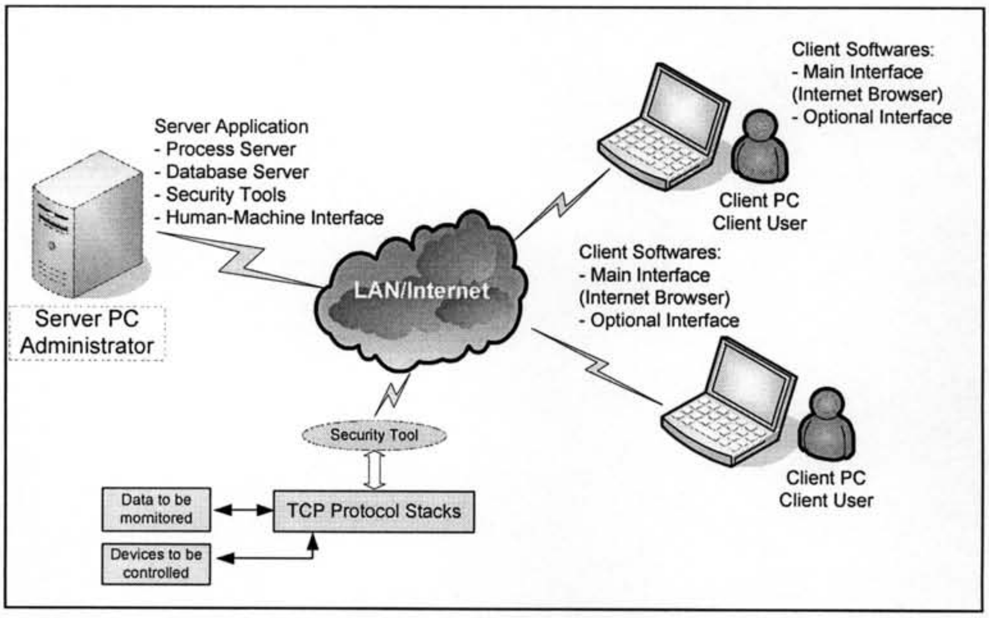

Figure 3.2 General System Architecture

Analysis:

According to the knowledge presented in the previous part, the proposed solution here is built based on the two-tier server/client model with Internet being the communication network (see Figure 3.2). Since there are many computers involving in the system, network programming techniques will be used to develop the system's software.

3.3.1 Network Level

At the Internet level, an Internet Service Provider (ISP) will provide an Internet connection for the system. A router (what the role of a router is has been discussed in the previous part) is used to connect the entire system to the line provided by the ISP and the entire system will be exposed to the Internet afterwards. The router itself will also provide us with some hardware-based tools, which will be explored in the next Chapter of this thesis, to manage our system.

3.3.2 Server Tier

In this system, one computer will act as both application and database server. The Ethernet LAN technology is used to connect this computer with the data acquisition part. All the communication happening among the server and the data acquisition part conform to the Ethernet protocol.

In term of software, the server is built as a Web-based application composed of the following modules:

1. User Management.

This module provides the management on system's users. It includes interfacing and Database (DB) connecting services.

2. Real-time Data Acquisition and Device Control.

This module allows users to have the system's data displayed in real-time and to issue supervisory control command on the field devices.

3. Security Management.

This module provides three security management tools as stated in the system's features. Details will be presented in Chapter 4.

4. Event Logs

This module is to record and back up all the actions that system's users have done on the system. Any control command given on the system's devices are recorded.

3.3.3 Client Tier

There can be more than one client computers in the system, as long as authenticated. Users at the client side can monitor data in real-time and issue supervisory control commands. Users can also perform other management actions on the system, depending on their roles which are defined by the system's administrator.

The main purpose of this research is to bring the users to the place of the system management center, no matter where they are by using Internet network. With the web-based application in the server computer and the IP-supported feature of the data acquisition hardware, there are two ways of performing the communication between client computers and devices:

1. Via Web-browsers

Using popular web-browsers such as IE or Firefox, authorized users can access and use the provided functions of the system through the web-based application built in server computer. Here, all the communications must go through the router at the Internet level, then through the server computer. This way provides better management ability and ensures the security of the system since the IP address of the data acquisition hardware is not made known all over the network.

2. Direct via the IP addresses of the TCP Protocol Stack

Using this method, another software package has to be built, in Visual Basic language for example, instead of using Internet browser. There is no need to go though server computer. However, information about the data acquisition part such as the IP address and port number must be known. Once these parameters are known, unwanted-users can access to the devices without having to pass the security levels in the server computer. Therefore, it reduces the security of the system and this kind of connection cannot be tracked.

3.3.4 TCP/IP Protocol Stack

This is a hardware component embedded with a Dynamic Link Library (DLL) module. It serves as the data acquisition part in the system. Supporting TCP protocol, this module interfaces with the field device, collects data and makes these data available on the Internet. It also has the tasks of receiving the control commands from the users and placing them on the field devices.

This module allows the direct connection to devices without going through the server computer with the high risk as mentioned. Therefore, we have the presence of another security tool as illustrated in Figure 3.2. For both ways of communications, all attempts to connect to the system's devices must pass the security limits as stated in the system's features.

3.3.5 Field Devices

These are the equipments in the real world from which the Protocol Stack collects data. These devices perform the actions following the control commands from users for a specific purpose. Devices will reflect the operation of the entire process, and data collected from them make the users/operators be able to evaluate the system operation and performance whether they conform to a pre-defined criteria and they can finish a specific job or not.