# CHAPTER II

# LITERATURE REVIEW

There have been a number of researches and case studies taken on how to make use of Internet as the communication network in designing and implementing SCADA systems. The following part is a discussion about what have been achieved and the problems faced in some of the outstanding researches. Each case study is pointed out with a general view followed by a description about what have and what have not been done. A conclusion is drawn afterwards.

In [1], Andrew et al presented a remote data acquisition system (Figure 2.1) for experimenting using power system's hardwares.

➢ **System Architecture:**

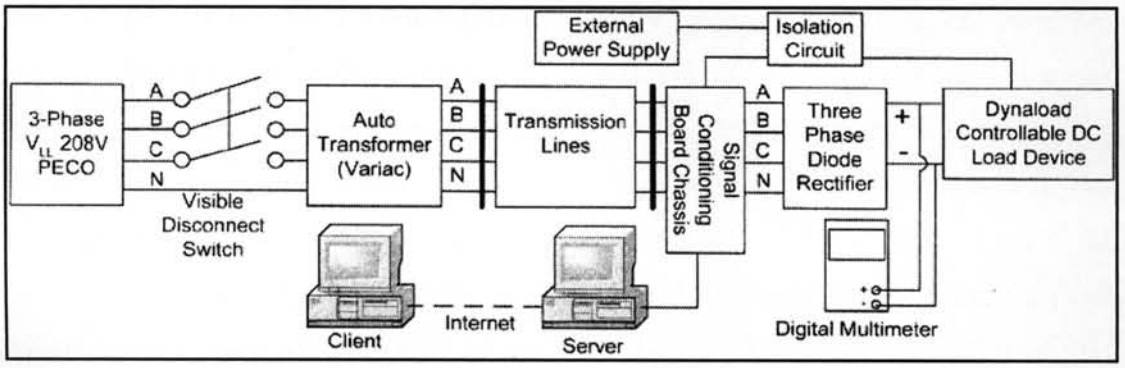


Figure 2.1 SCADA System Architecture proposed by [1]

There are four main components in the system: first, the experimenting hardwares; second, the data acquisition hardware; third, the application software based on the server/client module, having the task of performing the data communication over the Internet; and fourth, a safety system. In this research, there is no special hardware. The main point in the software is that the authors used the Data Socket Server module created by National Instruments, which eliminates the difficulties of Transmission Control Protocol (TCP) programming.

The server module has to perform five functions which are Data Acquisition (DAQ) and Processing, Measurement Display, Networking Function, Hardware Control and With-Human Interface. Sampled data acquired by the DAQ card are then displayed numerically and graphically. User interface manages the connections to

Data Socket Server and displays the connection status. Acquired data are written to Data Socket Server and control inputs are also read from there. To control hardware devices, the control inputs are to be written to the DAQ card, then are converted, amplified and sent to the loads with the help of some external electronics.

The client module also displays data as at the server side, but these data are not the real-time data in order to prevent the bottle neck on the communication channel. Data Socket Server creates the communication channel from the client users to the server side, allowing the user to issue control commands on the loads.

The system is protected by password-authentication, approved Internet Protocol (IP) addresses and a physical protection scheme for the power hardwares. The system provides many ways of configuring the hardware. Remote users once authenticated can perform all allowed actions. Data are displayed as desired and control inputs can also be placed on loads. However, the use of Data Socket Server led to difficulties and dependency for users. In the research, the technology used for connecting the system to Internet had not been mentioned, the real time issue had not been considered either and that led to the doubt whether the response of the system was fast enough to be applied in power system or not.

Again in power system's application, Zhang Donglai et al [2] proposed an internet-based SCADA system (Figure 2.2).

- **System Architecture:**

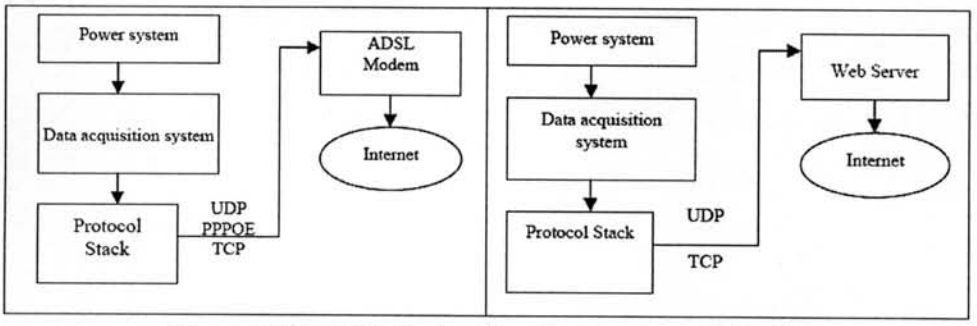


Figure 2.2 SCADA System Architecture proposed by [2]

About hardware components, a TCP module, which is manufactured by Ubicom, namely IP2012, is used to collect necessary data and transmit those data to the Internet. This module also supports the User Datagram Protocol (UDP). However, UDP is not as reliable as TCP, and it is not preferably used in Internet-based telemetry systems. There are two ways to connect the data to the Internet: first, using an

Asymmetrical Digital Subscriber Line (ADSL) modem, this gives high speed communication and makes it possible to monitor in real time; second, using PPPoE (Point to Point Protocol over Ethernet) to connect the data in the IP2012 directly to the Internet. Nevertheless, the second option, while being a broadband connection, is complex and unusual in term of programming. With ADSL technology, the system brought a fast communication channel, but this issue was not mentioned and the readers still do not know the data transfer speed actually achieved. Experimental results had not been stated in the research. The content of the research seemed to be in the draft stage. In addition, the system's security issue, which is the very important concern when working with such a public network as Internet, had not been considered either.

The same idea was proposed using the laboratory equipment, Wei-Fu Chang, Yu-Chi Wu and Chui-Wen Chiu [3] built a model of a web-based remote load supervision and control.

The system is illustrated in Figure 2.3 below:

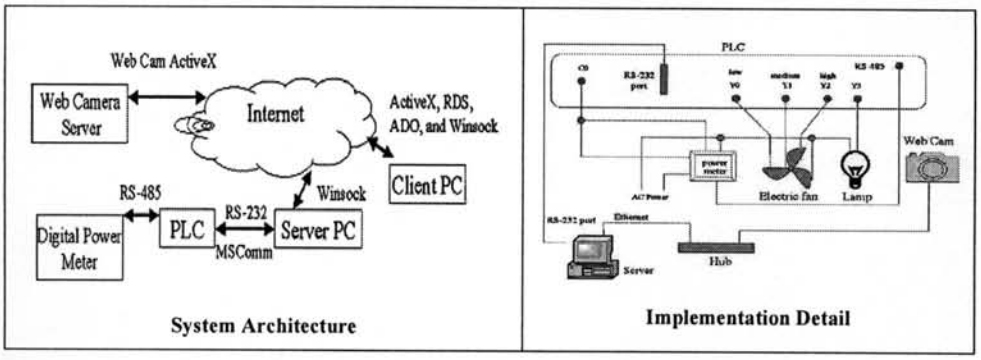


Figure 2.3 SCADA System Architecture proposed by [3]

Programmable Logic Controllers (PLCs) were used to collect data from and give control to field devices. The server/client model was used again with two options: first, the PLC is connected to a RS-232/TCP-IP converter for the data to be sent to the Internet, and remote users can both access the data directly via the IP address of the converter and the server's database; second, there was no converter, but the PLCs are connected to server PC and the data is stored right in the server's database. The implemented system followed the second option. A Visual Basic (VB) program was developed in the client PC allowing the client users to connect to the database in the

server PC. The data were both displayed on the VB screen and the web-browsers. The control commands to the loads were also issued via these two kinds of interfaces.

The research had mentioned in quite a deep detail about both how the system's software was built and how to setup the experimental hardware with the laboratory equipment. However, the use of non-web-enabled PLCs is not common today, since most PLCs today are equipped with the Internet connectivity and we may only need to deploy this feature to build up a similar system. Besides, some sort of Internet-connected PLCs today also contains a built-in web server, and in this case, the presence of the server computer may not important anymore. The security was not mentioned in this research, even as stated, it is of the most concerning problems when using Internet.

In a more general sense, M. Mahmud et al [4] used both Ethernet and Internet to build a SCADA system (Figure 2.4). Under the server/client model, it consists of several RTUs (Remote Terminal Units) and one SCU (SCADA Central Unit).

- **System Architecture:**

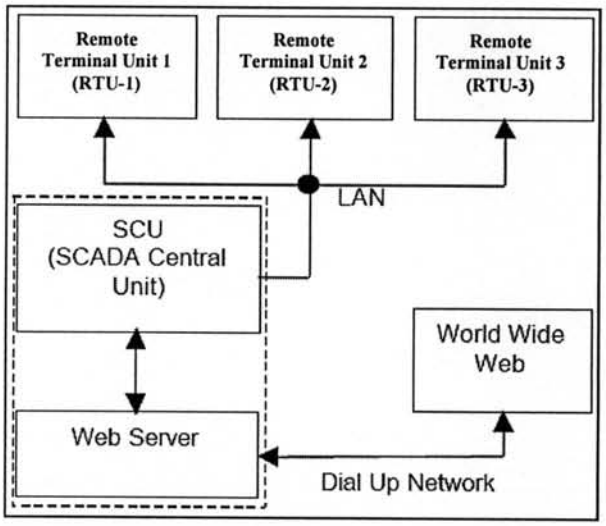


Figure 2.4 SCADA System Architecture proposed by [4]

The SCU is connected in the same Ethernet/LAN network with the RTUs. A data acquisition card is used at each RTU to collect the data, and then these data will be sent to the SCU to be stored for further use. The system's software is written using Visual Basic (VB) and Active Server Page (ASP) languages, running on windows platform. A VB program is developed in both computers at RTU side and SCU side for data monitoring and remote control. Users at any place can also access the SCU database using web-browsers.

The Internet interface was used also, but the main functions of the system are done via a VB program. This caused trouble in operating the system, and it also took more time in the designing stage. The security issue was not strictly considered in this research. Being proposed in the year 2002, the dial-up technology was used to connect the SCU to the Internet, and it might not have brought the belief with the speed of transferring data to ensure the real-time issue, since the dial-up network is quite slow.

A more thorough theoretical analysis about the advantages of utilizing Internet in SCADA applications and a comparison between Internet and other communication options was given in [5], by Robert H. McClanahan. Under the view from this author, there has been three generations of SCADA systems. The overall picture about each generation is in Figure 2.5 below:

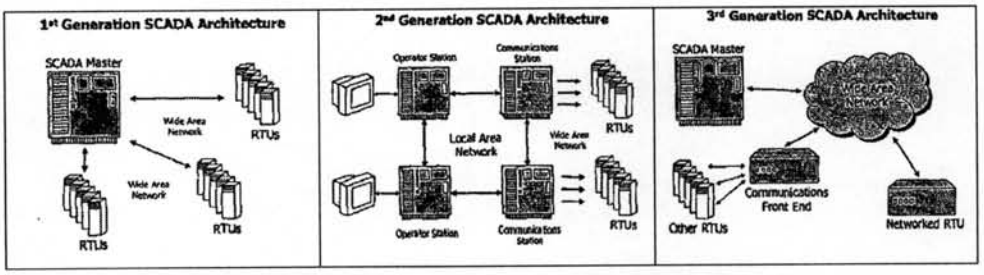


Figure 2.5 SCADA System Architecture proposed by [5]

The first generation is monolithic. In this stage, SCADA systems were standalone systems. The Wide Area Networks were designed with a single purpose in mind, which was of communicating with RTUs in the field. The WAN protocols used today were rarely known at that time. The protocols used that time were developed by RTUs vendors and this led to vendor-dependence. It was hard then to upgrade the system into another level with the communication expansion. In case of without connectivity, the communication to the Master station was based on the bus level. Here, at this stage, we had to face the redundancy since we had to build two systems operating together which are the primary system and the standby one and the standby system was to monitor the primary one and was activated in case of failure detection. There was not much processing done in this standalone system.

In the second generation stage, LAN networks were used allowing stations to share information in real time. LAN protocols were used and the systems were not

able to reach out the limit of local environment. Vendors could optimize their systems though it could limit other vendors by doing so.

The distributed architecture allowed states of all stations in the LAN to be online. If one Human-Machine Interface (HMI) fails to operate, another could be used without waiting for the back-up system. WAN communications were largely changed by LAN technology although they were still limited by RTU protocols. Such kinds of SCADA systems were still limited to hardware, software and peripherals which are dependent on or selected by vendors.

The third generation is the time where many big changes have been made. Those changes are in system architecture, standardized protocols usage and WAN communication. 3rd party peripheral devices and protocols are allowed to be interconnected into the system. WAN protocols such as IP are used for communication between the Master station and RTUs. RTUs produced at this stage are capable of communicating with each other via Ethernet network and even communicate with the Master station via IP protocol. The wider use of WAN network here reduces the loss of the entire system in case of failure.

The later part in the study is an analysis about some specific communication networks including Internet, which is the network to be chosen in this thesis. The content of this part has already been depicted in chapter 1. Here, we can have a look on the pros and cons of each choice and the great advantages of Internet that has placed a big motivation on this thesis.

Medida, et al. [6] presented a SCADA system based on the Internet for energy management system (EMS).

The system hardware and software are in Figure 2.6 below:

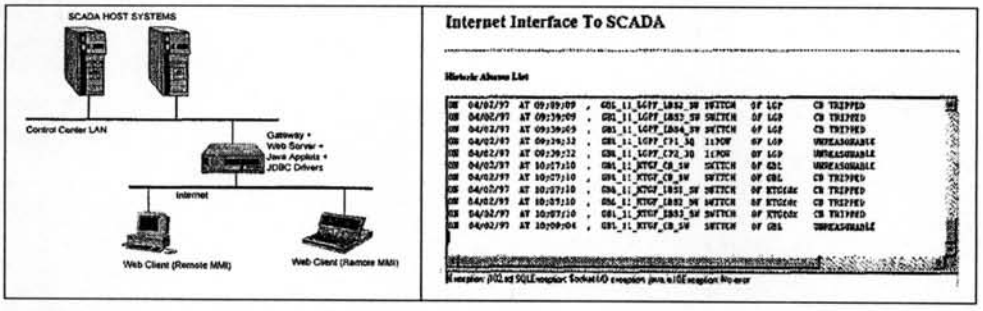


Figure 2.6 SCADA System Architecture proposed by [6]

This research used quite modern technologies with Oracle for database building and Java to make the SCADA database accessible and available to the remote Human Machine Interfaces (HMI) through web-browsers. No vendor dependent hardware, software and application are required at the remote location for SCADA but an Internet connection to gain access to the system from any corner of the world. Though the HMI is quite simple, but we can perform almost every function of an Internet-based SCADA system.

In this research, we could find the concern about the future of Internet-based SCADA solution with the time constraint. We might have to face the problem that the system's response time is not the same at different time in a day. However, we can ask the Internet Service Provider (ISP) to increase the bandwidth and we still can achieve the response speed as high as desired.

In [7], Duo Li, et al. proposed a conceptual design for SCADA system with regards to all available Internet technologies.

Several architectures of Internet-based SCADA systems are in Figure 2.7 below:

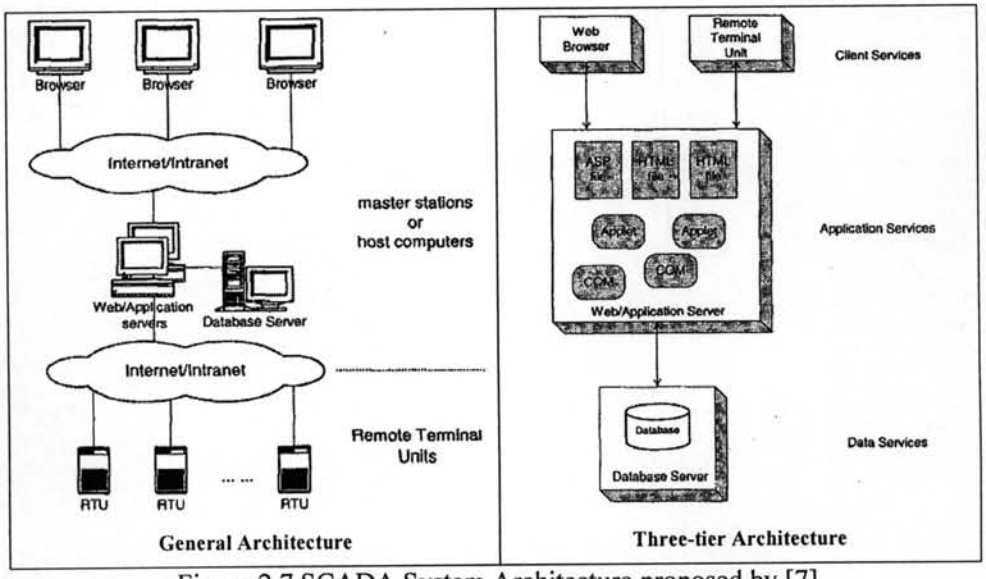


Figure 2.7 SCADA System Architecture proposed by [7]

In the general architecture, the master station or host computers are implemented with web application server. They provided open interfaces to all other devices based on HTTP protocol. RTU used HTTP packages to communicate with the server and work in the similar way as the web browsers.

From the three-tier point of view, web browsers and RTUs lie in the Client Services to provide the interfaces to applications and other operators; web servers lie in the Application Services to realize all application programs and a database server locates at the Data Services to provide storage and manipulation for data. This kind of architecture is named service-layer architecture and for its nature, it can bring many advantages.

In this research, the security and real-time issue were talked about, but not much. An implementation example was also given with Java and a web-based server application, Internet browser was used as the interface between system and users.

In [8], a very deep analysis about the security of Internet-based systems was presented. Here, the authors first talked about how the hacking level has been rising in recent years, then they introduced some of the existing vulnerability assessments and finally, they stepped through several strategies for designing the defense for SCADA systems. For the first point, it was mentioned that there is no doubt that the risk of losing information and even the full control of the system might occur at any time. At the second point, the authors mentioned about some loss on the Oil and Gas system in the US, with lost information and illegally sold items. The most important part in this research is depicted in Figure 2.8 below:

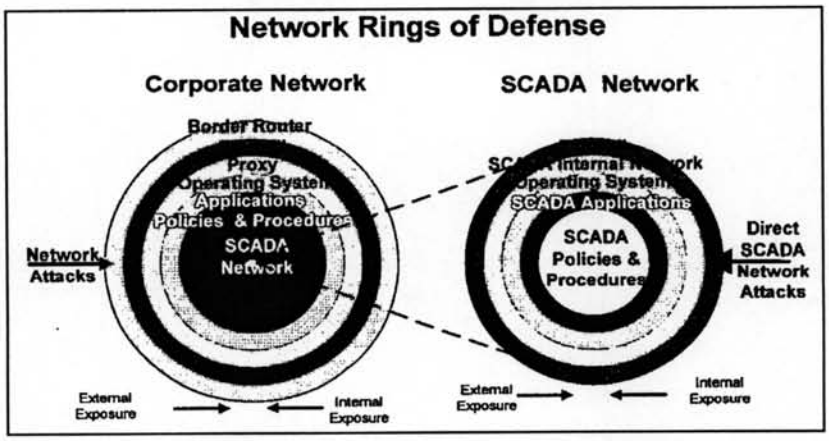


Figure 2.8 SCADA System Architecture proposed by [8]

From this figure, we can see there are the following rings of the entire strategy:

- Border Router and Firewalls
- Proxy Servers
- Operating Systems

- Applications
- Policies and Procedures

There have been 5 layers proposed and attacks can occur at any layer. In each layer, we need the necessary software tool to protect the system. The final part of the research is a deeper discussion from some other researches to which we can refer about the on-going potential risk occurring on SCADA and Control systems.

A couple of researches picked up and analyzed as above has given us a more obvious view on the stated issue. Based on this, we have several conclusions:

There are still a number of problems faced in those researches which are:

2. Low data transfer speed when using dial-up network.
3. Complex programming techniques are required when using PPPoE for Internet connection and when using Data Socket Server for server-to-client communication.
4. Hard to add or remove a new site to or from the entire system as well as to track devices attached to the system when using traditional wiring for the data acquisition part in the entire system.
5. The security issue was not discussed deeply and clearly, even though it is one of the most important things to be considered when using such a public communication network as Internet.
6. No researches mentioned about the cost of the solution given. Cost is a very important factor that needs to be considered whenever a solution is proposed. It says the solution is either practical or economical to be implemented or not.

This research will explore more the power of and give more understandings on Internet as well as present a deeper analysis on the existing problems above. Some new features will also be added to improve these problems. The solution for an Internet-based SCADA system with the help of the advances in hardware and Internet technology is presented with the motivation of being able to perform the followings:

1. Increase data transfer speed by using ADSL technology.
2. Increase the system's flexibility by using IP-supported hardware device.
3. Increase the system's security level with the security layers stated in Chapter 1
4. Increase system management ability by using the latest Microsoft technologies in building application software.

5. The data transfer speed and time are also given on the system interface.
6. Cost estimation is discussed. We can then evaluate the overall performance of the solution in all aspects.

If successful, the research will make the Internet-based solution for SCADA systems more complete. Furthermore, we can make use of the public tools such as Instant Messaging or Email without paying any more fees. This helps improve to interaction ability among system's users and give the low-cost feature to the solution.