CHAPTER 5

STUDY AND IMPLEMENTATION OF WBSCIS IN TEMPERATURE PROCESS CONTROL
EXPERIMENTAL SETUP

5.1 INTRODUCTION

There is a great deal of benefit for process plants in adopting the Internet to control systems. Over the years, there has been a constant increase in the development of industrial automation through remote monitoring and diagnosis virtually. By surveying the existing remote monitoring system that is used for process plant equipment, this system tends to focus on the recent trends and developments in the control of equipments and devices in the industries by remote monitoring through Internet.

The Internet based automation is made possible by the use of Programmable Logic Controller (PLC), Supervisory Control and Data Acquisition (SCADA), Virtual Private Network and other network elements. The objectives of remote monitoring and diagnosis are prevention of unplanned downtime, making optimal control operation and maximizing the operational life of plant assets. An online integrated web based remote supervisory control and information system takes real-time data on the process control of the performance of a unit and helps the remote expert for carrying out further analysis, thereby supporting the plant engineer. The design, Internet security and user interface challenges are focused in this experimental implementation.
A Programmable Logic Controller is programmed to control the operation of the plant and a SCADA system is implemented to monitor and control the process as stated by Aydogmus and Aydogmus (2009). The proposed system offers an economical solution for multiple users in the Laboratory Environment. In the fault diagnosis of the power electronic equipment in the industry, the technical requirements are greatly reduced, but the provision for backup in case of a communication failure has not been considered by Hurley and Lee (2005).

The collection of complete real-time data from different source systems such as SCADA, databases and Internet which is pushed into an online transaction process and its immediate acquisition into online analytical process are addressed by Raghavendra Nagesh et al (2008). The real time data is compared with forecasted data and historical data for effective online energy management information reporting system and the end-to-end energy information for better decision making is analyzed. The condition monitoring and fault diagnosis for growing figures of power generation systems which use components embodying intelligent computing models, structure with local and central information system is discussed by Wang et al (2007).

The research, based on real-time web based machine tool and machining process monitoring system and the steps for implementing e-manufacturing system are explained Shin et al (2006). The system architecture of a multi layered distributed SCADA system used for monitoring, controlling and establishing the link with icons on graphics panels that integrates all three levels of process control from operator panel with the distributed PLC system is explained by Salihbegovic et al (2009).

The online controlling of industrial process via GPRS enabled mobile phone is demonstrated using a prototype by Ozdemir and Karacor (2006). It provides the selection of process values, alarms with graphical user
interface and remote control in user defined time. The online report diagnosis and GPRS network latency issues are not considered. The concept of E-automation, in which computer networking and distributed intelligence agent technologies are applied to industrial automation systems and the hardware, software architectures are proposed by Lee (2003).

E-automation architecture permits greater configurability than a traditional system. The growing need for better monitoring of process plants, improved operations, safety and detailed knowledge of critical supervisory control and monitoring is becoming increasingly important. This makes the implementation of web based remote supervisory control and information system the best solution. The design challenges, network security issues, user interfaces and possible solutions are focused in this research. The further sections present the experimental approach that was carried out and the results that were obtained.

5.2 EXPERIMENTAL SETUP

In this research, in order to show the applicability and effectiveness of the design and implementation, real-time experiments have been carried out on a real process control unit in the Interface and Automation Laboratory at Department of Mechatronics Engineering, Kongu Engineering College, Perundurai. Figure 5.1 and Figure 5.2 show the layout of the experimental system and real time photographic view of the experimental setup, which includes the process control unit and a PC with SCADA. The process control unit includes a heating tank and two water tanks: one at the bottom acting as a reservoir and another as an overhead tank. PLC functions as a local control system.
The reservoir tank contains a pump to circulate water to the overhead tank. From the overhead tank, water flows to the heater tank. Based on the level of the liquid of tank 1, water is pumped to tank 2. The sequence of these operations is controlled by the PLC. The objective is to control the liquid level in the three tanks by regulating the flow rate of the pump. Temperature monitoring and control plays an important role in the industry and it is one of the major industrial control parameters. Hence temperature is taken as the parameter to be controlled using this experimental setup.

Figure 5.1 Functional diagram of developed temperature process control experimental setup
Level sensor monitors the water level in the tank2 and thereby water flow to the tank is controlled by the pump. Water from the tank 2 reaches tank 3 where it is heated above the boiling point. The temperature of the liquid in the tank3 is measured by using a temperature sensor. The outputs from all the sensors are fed to the PLC. The set temperature is controlled through the ladder logic program with the PID function incorporated in it.

Figure 5.2 Photographic view of Real-Time experimental setup with LCU and 3G - GPRS Gateway device

1. Control panel  
2. Thermostat  
3. Base water tank  
4. Over head water tank  
5. Solenoid valve  
6. Local control unit  
7. Pump  
8. GPRS gateway device  
9. RTD with transmitter
PID controllers are used for controlling almost all process variables like temperature, flow, level and pressure etc., in a continuous or batch process.

The output of a PID controller is given by

\[
OP = b + 100/PB \left[ e + \frac{1}{T_i} \int e \, dt + T_d \frac{de}{dt} \right]
\]

Where \( OP \) is the output, \( b \) is the bias, \( PB \) is the proportional band in \( \% \), \( e \) is the error signal, \( T_i \) is the integral time and \( T_d \) is derivative time. Selection of proportional band, integral time and derivative time to achieve desired process response to changes in load is called tuning of the controller.

The desired set point values are achieved by proper tuning of PID parameters through process reaction. The tuned output from PLC is fed to the variable power mode controller which in turn controls the operation of the electric heater. Thus the desired temperature is achieved by using the tuned output from PLC.

5.3 POSSIBLE IMPLEMENTATION OF PROPOSED ARCHITECTURE

The design and development process for the web based remote supervisory control and information system includes requirement specifications, architectural design, control algorithm design, user interface design and security issues. Figure 5.3 shows various levels of system monitoring and control requirements in the automation hierarchy architecture. Considering the architecture, a possible implementation of a web based remote monitoring system is essential to meet all the requirements.
5.3.1 Requirement Specifications

In general, a system comprises of a set of components working together to achieve web based remote supervisory control. The experimental pilot plant is an example here to describe the procedure for specifying requirements for a web based remote supervisory control.

![Integrated web-based automation hierarchy](image)

**Figure 5.3** Integrated web-based automation hierarchy

In this system, the goal is to maintain a particular relationship between input to the system and output from the system when the process is critically disturbed. As shown in Figure 5.4, the web based supervisory control and information system is based on a web client / server configuration.
Information exchange between experimental pilot plant and Internet-based clients allows the client to remotely monitor, control and thereby modify the parameters of the process plant. Web based supervisory control and information system strategy must be employed towards solving the problems associated with communication latency, security and user interface issues. The design of web-based remote supervisory control and information system, implementing the effective point-to-point network communication architecture and ideal control strategy, aids in decreasing the Internet latency and maintains system stability.

Figure 5.4 Web-based supervisory control over the Internet

5.4 PROPOSED WBSCIS ARCHITECTURE

The proposed architecture of the web based remote supervisory control and information system is shown in Figure 5.5. It consists of a pilot experimental plant, local control unit, work station and Ethernet based Gateway device for Internet connectivity with other network elements. The pilot plant is controlled by Programmable Logic Controller. The Programmable Logic Controller is connected with the Gateway device to establish wireless Internet connectivity.
The Ethernet based Gateway device can be expanded over high speed wireless networks and integrated as a part of internal network. At the remote location both the Ethernet and serial devices can be connected with the Gateway device unit to the central site of the global systems which is possible with the most common wireless networks.

The remote monitoring station consists of a local work station and Machine to Machine (M2M). The importance of M2M is that it offers secured two-way communication (static IP address) between machines without human intervention.

Development and deployment of M2M system is necessary for creating a pervasive and intelligent environment. M2M is a combination of various heterogeneous electronic communication and software technologies.

The key features for the proposed architecture are:

- Eliminates distance limitations - Global systems are possible if GSM/GPRS-2G/3G networks are available.
- Provides secured two-way communication (Static IP and Public IP).
- Expands Ethernet over GPRS network.
- Offers mobile operator independent static IP addressing for connecting remote gateway devices.
- Has Firewall and VPN for secured communication.
5.4.1 ROLE OF SUPERVISORY CONTROL AND DATA ACQUISITION

SCADA generally refers to an industrial control system: a computer system monitoring and controlling a process. It usually refers to a system that coordinates, but does not control processes in real time. A SCADA system allows users to monitor an entire plant or individual pieces of equipment and processes by collecting real-time data from various sensors through a network. It is very important for organizations to monitor these network activities and doing so informs them of problems with their mission-critical processes. By monitoring these processes, organizations can quickly respond when there are problems within their network. Effective monitoring saves significant expenditures on repairs and lost revenue due to network downtime. An effective combination of SCADA with wireless remote monitoring makes the proposed system efficient in monitoring the real-time critical processes.

5.4.2 Challenges of Web-Based Remote Supervisory Control System

The challenges of successful implementation of web based supervisory control for an application is the provision of effective real-time processing and data transfer over the Internet. In order to obtain reliable data transmission over Internet a novel web based supervisory control is proposed to minimize the effect of Internet time delay and data loss. There are various risks including the operational difficulties such as cyber hackers, especially in the systems linked to industrial operations which result from the application of network technologies. Therefore Internet enabled plant will never be absolutely safe and secure if a remote user is allowed to directly access and make changes to the local control system. In order to overcome these security challenges, VPN based authorized remote user access level is considered the best solution.
5.5 **TYPICAL IMPLEMENTATION**

In the last decade, the most successful network development is the Internet. It is widely used as a communication and data transfer mechanism. The Internet is a global platform for information retrieving and also for web based remote control. The objective of this implementation focuses on providing a flexible graphical user interface over Internet environment, enhanced security to access the remote pilot plant and reducing the Internet latency. The main goals for applying graphical user interface over Internet in process control interface are as follows:

- To enable the remote expert and plant engineer operators to appreciate more rapidly what is the present state of the process dynamic system.
- To provide more information on the process i.e., online/offline trend analysis.
- The graphical user interface and program logics are developed in SCADA.

5.5.1 **Ensuring Security between Plant and Remote Client**

The real-time implementation to ensure plant security and end user access level is focused. A typical OpenVPN is used to ensure security between plant and remote end user.

VPN uses relatively low-cost, widely available access to public networks like the Internet to connect remote sites together securely. This yields Virtual Private Networks that link to geographically distributed sites. In a VPN, traffic from one site destined for another must traverse through an untrusted public network like the Internet. The site-to-site traffic is protected from outsiders.
5.5.2 Security Objectives of VPN

The security objectives of the VPN implementation are as follows:

- Isolate a distributed network from outsiders.
- Protect the privacy and integrity of messages traversing untrusted networks.
- Handle the whole range of Internet protocols currently in use.
- Public Internet access is available and cheaper.

5.5.3 Role of OpenVPN

In order to ensure security over the Internet environment, the OpenVPN client certificate based security is developed and implemented successfully in the experimental pilot plant system. A point-to-point connection is programmed in M2M and routed configurations are made which help to make remote access facilities. It uses SSL/TLS security for encryption and is capable of traversing network address translators (NATs) and firewalls.

OpenVPN allows peers to authenticate each other using certificates or username/password. It allows the server to release an authentication certificate for every client using signature and Certificate authority. It uses the OpenSSL encryption library extensively as well as the SSLv3/TLSv1 protocol.

5.5.4 Encryption

OpenVPN uses OpenSSL library to provide encryption of both data and control channels. It lets OpenSSL to do all the encryption and authentication work, allowing OpenVPN to use all the ciphers available in the OpenSSL package. It can also use the HMAC packet authentication feature to
add an additional layer of security to the connection (referred to as an "HMAC Firewall" by the creator). It uses hardware acceleration to get better encryption performance.

5.5.5 Authentication

The implementation of web-based remote supervisory control information system for the experimental pilot plant is authenticated at two different levels.

- The Open VPN certificate based authentication at the end remote user terminal.
- SCADA is programmed with multiple user access level and is password protected to ensure the authorized user to view plant status and provides further assistance to the plant / site engineers.

During the implementation of M2M, it is programmed with OpenVPN certificate which has more features and robust. The username/password is a new feature that can be used with or without a client certificate. The source tarball includes a sample Perl script to verify the username/password with PAM and a C auth-pam plug-in.

5.6 RESULTS AND DISCUSSION

5.6.1 GPRS / Internet latency and Data loss from the Network View

The possible solution for reducing GPRS/Internet data transmission delay is presented in this section. Unpredictable time delay and data loss are difficult to design at any period of time.
The pilot plant’s local control unit i.e., PLC is connected to the gateway device which is 2G/3G enabled. The GPRS/Internet is a public and shared resource in which various users transmit data via the GPRS/Internet simultaneously. So the VPN is implemented between experimental pilot plant and remote end user which ensures a channel for data transmission. This prevents collision of data when two or more remote users receive the data via the same route simultaneously.

The real-time implementation of web based remote supervisory control and information system is carried out initially with 2G GPRS environment. The observation is carried out at the remote sites with different time duration i.e. 3 hrs, 6 hrs, 12 hrs and 24 hrs during different days. Figure 5.6 to Figure 5.9 show the remote expert user interface process and web-client trend for online analysis of the pilot plant operation. The trend observations show that the data loss at the remote site occurs in many intervals of time and are presented as circular regions in the Figures 5.6, 5.7, 5.8 and 5.9.

A minimum of 25 seconds to maximum of 240 seconds interval is observed during different hours of continuous remote monitoring. The real-time on-line examination is also carried out with the 3G –EDGE in the remote pilot plant gateway device. In 3G environment, the data transfer rate is above 356Kbps - 2Mbps compared to maximum of 56kbps in 2G. Figures 5.10, 5.11, 5.12 and 5.13 show the process parameters on-line trend of the pilot experimental process in the 3G environment.

The same procedure was carried as mentioned in the 2G environment for remote observations i.e. 3 hrs, 6 hrs, 12 hrs and 24 hrs testing were carried out in the experimental setup. The trend observations show that the data loss at the remote site occurs in a few intervals of time and are presented as circular regions in the Figures 5.10, 5.11, 5.12 and 5.13. The data loss interval that lies between 10 seconds to 30 seconds maximum is
observed, which clearly indicates the promising performance of the 3G network environment for remote monitoring applications.

Figure 5.6  Process trend of Pilot plant operation in 2G –GPRS network environment – Duration: 3 hrs

Figure 5.7  Process trend of pilot plant operation in 2G-network environment – Duration: 6 hrs
Figure 5.8  Process trend of pilot plant operation in 2G-network environment – Duration: 12 hrs
Figure 5.9: Process trend of pilot plant operation in 2G-network environment – Duration: 24 hrs
Figure 5.10  Process trend of pilot plant operation in 3G-network environment – Duration: 3 hrs

Figure 5.11  Process trend of pilot plant operation in 3G-network environment – Duration: 6 hrs
Figure 5.12 Process trend of pilot plant operation in 3G network environment – Duration: 12 hrs
Figure 5.13  Process trend of pilot plant operation in 3G-network environment – Duration: 24 hrs
Table 5.1 Summary of Experimental observation in 2G/3G - GPRS/Internet Environment

<table>
<thead>
<tr>
<th>Experiment order number</th>
<th>Conditions</th>
<th>Feedback transmission time (ms)</th>
<th>Data package loss number / Total package number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Maximum time (ms)</td>
<td>Minimum time (ms)</td>
</tr>
<tr>
<td>Experiments carried out locally</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Local Network Communication</td>
<td>21</td>
<td>11</td>
</tr>
<tr>
<td>Experiments carried out from a 50 Km distance</td>
<td>2 2G – communication</td>
<td>4862</td>
<td>640</td>
</tr>
<tr>
<td></td>
<td>3G - communication</td>
<td>1265</td>
<td>132</td>
</tr>
<tr>
<td>Experiments carried out from a 285 Km distance</td>
<td>3 2G – communication</td>
<td>8819</td>
<td>2320</td>
</tr>
<tr>
<td></td>
<td>3G - communication</td>
<td>2649</td>
<td>529</td>
</tr>
</tbody>
</table>

GPRS - 2G / 3G environment – Internet latency and packet Loss analysis are presented in the Table 5.1. Based on the feedback transmission time and packet loss, it is observed that 3G –GPRS network for Web-based remote monitoring performs better than 2G GPRS/ Internet.
5.6.2 Remote Monitoring Over WWW Environment

The web-based remote supervisory control and information implemented with leading edge technology enables remote end user to easily obtain secured data, information and knowledge to support decision-making at all the levels of the process plant.

A number of positive and successful initiatives are investigated to improve the operations and utilization of process control system, information system and infrastructures used by the plant engineers and remote expert support team. In this section, the experimental result is presented and further suggestions are discussed.

In order to ensure security over the Internet environment, VPN is implemented. Further a password control is also programmed in the SCADA to stop unauthorized access to the local control system over Internet. Figure 5.14 shows that only an authorized user can view the remote control user interface and have access to web based remote supervisory control and information system.

- The actual SCADA Screen for experimental setup over the Internet looks similar to the one shown in Figure 5.15.
- This graphical screen helps to easily understand the overall process.
- The set point temperature and actual process variable are shown in the display.
- The controller output is also displayed on the screen.

The process or PID parameters can be tuned and controlled over the Internet remotely. The parameters tuning window appears as shown in Figure 5.15. The simple experimental setup over the Internet looks like the one shown in Figure 5.17. Here, the remote SCADA acts as a client.
Figure 5.14 Remote user access login requests over web browser environment – security check

Figure 5.15 Remote monitoring of experimental setup viewed in web browser environment
Figure 5.16 Controller tuning screen viewed in web browser environment

Figure 5.17 Structure of the experimental setup viewed in the web browser environment
Various critical alarms and their status can be monitored over the Internet. The sample alarm window screen appears as shown in Figure 5.18.

**Figure 5.18**  Process alarm viewed in web browser

**Figure 5.19**  Live process trend viewed in web browser
The actual trend window over the Internet is pictured in Figure 5.19. Description of various parameters over a time period can be monitored. The report on different process information can be viewed periodically. This option is made available by using a SCADA screen and it can be viewed over the Internet from any place. Figure 5.20 shows such a screen over the Internet.

Figure 5.20  Web-based on-line report option for experimental setup viewed in the web browser

The web-based online report of process station appears as in the web-browser environment shown in Figure 5.21. The web based information system uses the stored data to determine the performance of the pilot plant, which makes intelligent discussion regarding the periodical monitoring of the entire process variables. The detail of VBA program is available in the Appendix 1. Online monitoring of set point value is done and it is noted that when the process variable reaches the set point value, the controller output reaches zero. Any process parameter can be verified successfully and monitored through Internet using the same.
5.7 SUMMARY

In this chapter, design and real-time implementation of Web-based remote supervisory control and information system is presented. This novel architecture is secured and decreases the Internet latency with the support of 3G network. This system prevents unplanned downtime making optimal control operation and maximizes the operational life of plant assets.

The operational cost of the proposed system using GPRS is cheaper when compared to the conventional remote monitoring methods which use the Internet. Also, this system is beneficial over the traditional system in terms of remote monitoring, control and maintenance. The proposed system further reduces the technical requirement for monitoring and diagnosing in enterprises. It communicates information among the administration
department, running field staff and the experts allowing them to acquire broad information, thereby integrates experience and knowledge from different aspects. The system has been successfully tested at the pilot plant in Kongu Engineering College, Perundurai.