The Islamic University of Gaza

Deanery of Graduate Studies

Faculty of Engineering

Electrical Engineering Department

A SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) FOR WATER DISTRIBUTION SYSTEM OF GAZA CITY

By

Ayman M. Alihussein

Supervisor

Prof. Dr. Mohammed Abdelati

“A Thesis Submitted in Partial Fulfillment of Requirements for the Degree of Master in Electrical Engineering”

1431-2010

Abstract

Gaza has scarce water resources. At present, there are 40 wells that are supposed to supply adequate water from the aquifer to the public through the water distribution network. However, the pumping stations at these wells along with the distribution network are managed manually by operators in a primitive manner. During peak consumption periods, which may last for weeks, water is not delivered to wide areas and resources are not distributed evenly to public. Operators try hardly to achieve fairness by manually controlling gate valves along with pumping stations. The aim of this research is to design a Supervisory Control and Data Acquisition (SCADA) system for managing the water pumping stations in Gaza. This system is expected to increase customer satisfaction, reduce water distribution cost and provide an accurate overview of the plants' operations. Moreover, SCADA stores valuable information about the water system performance. This data is necessary for efficient development of the existent distribution system in a way that meets population growth.

عنوان البحث:

تحكم إشرافي و اكتساب بيانات لنظام توزيع المياه في مدينة غزة

ملخص البحث:

تعتبر مدينة غزة من المناطق الفقيرة في مصادر المياه، فهي تعتمد على استخراج المياه من باطن الأرض لتلبية احتياجات السكان. في الوقت الحالي يوجد تقريبا 40 بئرا جوفيا تغذي المدينة بالمياه الخاصة بالشرب و الاستخدام المنزلي. يتم ضخ المياه المستخرجة من هذه الآبار مباشرة في شبكة توزيع المياه. تدار و تنظم هذه العملية عن طريق المشغلين بطريقة يدوية و بدائية تعتمد على خبرة و نظر المشغل. خلال فترات الذروة التي قد تستمر لأسابيع، تنقطع المياه و لا تصل مناطق واسعة و كذلك عملية توزيع المياه لا تكون منتظمة و عادلة بالرغم من اجتهاد و كفاءة المشغلين و محاولاتهم توزيع المياه بطريقة عادلة على جميع السكان في جميع المناطق.

الهدف من هذا البحث هو تصميم نظام تحكم إشرافي و اكتساب بيانات لإدارة محطات أبار المياه في مدينة غزة. المتوقع من هذا النظام العمل على تقليل تكلفة توزيع المياه و تزويد المختصين بمعلومات دقيقة عن عمل الآبار للمساعدة في وضع الخطط اللازمة لإدارة و تنظيم عملية استخراج و توزيع المياه و الوصول إلى إرضاء و ارتياح المواطنين. كذلك يقوم هذا النظام بتخزين المعلومات المهمة عن كفاءة و فعالية عمل محطات أبار المياه، و تعتبر هذه المعلومات ضرورية عند وضع خطط تطوير فعالة تواجه الزيادة المستمرة في احتياجات المياه نظرا للزيادة المستمرة في الكثافة السكانية.

اعتمدت عملية التصميم على الحفاظ على الوضع الحالي في التحكم بأجهزة المحطة مع إضافة ما يلزم لتتوافق عملية التحكم و مع نظام التحكم الإشرافي و اكتساب البيانات. كما تم التوصية استخدام نظام اللاسلكي في ربط محطات الآبار مع غرفة التحكم الرئيسية التي يفضل بأن تكون في بلدية غزة نظرا لموقعها المتوسط و المرتفع.

Dedication

To all my family members who have been constant source of motivation, inspiration and support

Acknowledgment

I would like to express my sincere thanks to the many people who have contributed to the success of this research, in particular my thesis supervisor, Prof. Dr. Mohammed Abdelati, for his support, encouragement and professional assistance throughout the work of this research.

Special thanks to all other Islamic University staff members that I may have called upon for assistance especially Dr. Mohammed T. Hussein and Dr. Fadi El-Nahal , as their suggestions have helped with the development of this thesis. And extend my thanks to water department staff at municipality of Gaza and Coastal Municipalities Water Utility for their encouragement, support and assistance. Great thanks to EL WAFA Charitable Society for their financing support and grateful to the undergraduate students S. Sadeq, G. Shaweesh, R. kuhail, E. Ayad, Kh. Abualkhaer, H. Ekraim, N. Lolo, E. Mostafa, B. Salibi, A. Alsarraj, and O. Abdallateef for their help in building the experimental toolkits of the SCADA laboratory

I would like to also extend my gratitude to my family for the support they have given me.

Finally, I would like to thank the Islamic University of Gaza for accepting me in its graduate program and motivated me to do this work.

Contents

List of Tables

List of Figures

Nomenclature

ACK	Acknowledgment
ADSS	All-Dielectric Self-Supporting
AGC	Automatic Generation Control
ASCII	American Standard Code for Information Interchange
CANbus	Controller Area Network bus
CAS	Control and Status
CHAR	Character
CL.L	Chlorine low level
COM	Component Object Model
CPU	Central Processing Unit
CR/LF	Carriage Return/Line Feed
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTS	Clear-To-Send
dBi	Decibel isotropic
DCE	Data Communication Equipment
DIN	Deutsches Institut für Normung
DMS	Distribution Management Systems
DP	Decentralized Periphery
DTE	Data Terminal Equipment
ED	Economic Dispatch
EHF	Extremely High Frequency
EIA	Electronics Industry Alliance
ELF	Extremely Low Frequency
EMS	Energy Management Systems
EMT6	Overload Protection Relay
EPA	Enhanced Protocol Architecture
ERP	Enterprise Resource Planning
FCC	Federal Communications Commission
FIX	Financial Information eXchange
F.L.L	Fuel Low level
FMS	Fieldbus Message Specification
FTP	File Transfer Protocol
GCS	Grid Coordinates
GEDCO	Gaza Electricity Distribution Corporation
GSM	Global System for Mobile

H.M	Hour Meter
H.P	High Pressure
HF	High Frequency
HMI	Human Machine Interface
IEC	International Electrical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IT	Information Technology
ITU	International Telecommunications Union
Kbps	kilo bit per second
KVA	kilo Volt Ampair
L	Liter
L.L.	Low level
L.P	Low Pressure
LAN	Local Area network
LF	Low Frequency
LRC	Longitudinal Redundancy Check
MAN	Metropolitan Area Network
Mbps	Mega bit per second
MCR	Main Control Room
MES	Manufacturing Execution Systems
MF	Medium Frequency
MHz	Mega hertz
Mm	Millimeter
MMI	Man Machine Interface
Moist.	Moisture
MTU	Master Terminal Unit
NGEST	Northern Gaza Emergency Sewage Treatment
NI	National Instruments
NRV	Non Return Valve
NZM	Circuit-Breakers
OLI	Object Linking and Embedding
OPC	OLE for Process Control
OPGW	Optical Power Ground Wire
OSI	Open System Interconnection
PA	Process Automation
PBX	Private Branch Exchange
PC	Personal Computer
PES	Power and Energy Society
PLC	Programmable Logic Controller

PROFIBUS	Process Field BUS
PSTN	Public Switch Telephone Network
RAPLC	Remote Access PLC
RMU	Remote Monitoring Unit
RS485	Recommended Standard 485
RTS	Request-To-Send
RTU	Remote Terminal Unit
RxD	Receive Data
SCADA	Supervisory Control and Data Acquisition
SHF	Super High Frequency
SLF	Super Low Frequency
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
STP	Shielded Twisted Pair
SW.	Switch
T0	Timer 0 for low level water
T1	Timer 1 for High pressure
T2	Timer 2 for None Return Valve
T3	Timer 3 for Low pressure
T4	Timer to Reset High Pressure
T5	Timer 5 Timer for run
TCP/IP	Transmission Control Protocol and Internet Protocol
Temp.	Temperature.
TxD	Transmission Data
UHF	Ultra High frequency
ULF	Ultra Low Frequency
USB	Universal Serial Bus
UVR	Under Voltage Relay
VHF	Very High Frequency
VLF	Very Low Frequency
Wi-Fi	Wireless Fidelity
WOC	Wrapped Optical Cable
WWTP	Waste Water Treatment Plant

Chapter 1

Introduction and Literature Review

Gaza city is considered one of highest overpopulation regions in the word, there are 1.6 million people in 360 km^2. Also it is considered one of the poorest regions of water resources. The existing supply of potable water in Gaza is generally dependents upon well sources abstracted from the aquifer [1]. The water utility supply system in Gaza city consists of 40 water wells located in different regions in Gaza strip as illustrated in Figure (1.1) and summarized in Table (1.1) using Palestinian Grid Coordinates (GCS_Palestine_1923). Part of these wells has been constructed with submersible [2] water pumps and others having vertical turbine [3] pumps with a production rate varies between 50 and 220 m^3/hr. The pumping set is protected against low level water in the aquifer by means of dedicated sensors. Every year, Gaza municipality installs new well pumping stations to compensate the increase consumption of water due to the overpopulation , so through two or three years, the number of well stations may reach 60 well stations or more. The water wells are conventionally comprises of a pump, a chlorine dosing unit, a water manifold, an electrical switchboard, a sand trap and a standby diesel generating set.

The distribution system depends mainly on direct pumping from the wells to the distribution network. These pumping stations are managed manually through operators who are located as three consecutive 8-hour shifts along the day. Decisions are made according to observations and feedback which is delivered through phone calls between humans. An operator is allocated for each pumping station and he is in charge of running the station according to phone call orders coming from the responsible department in Gaza municipality, or according to a predefined time schedule. There is no automated centralized management and there is no computerized alarm logging and handling.

In this research we will design a Supervisory Control and Data Acquisition (SCADA) system for managing , monitoring and controlling the pumping stations in Gaza [4].

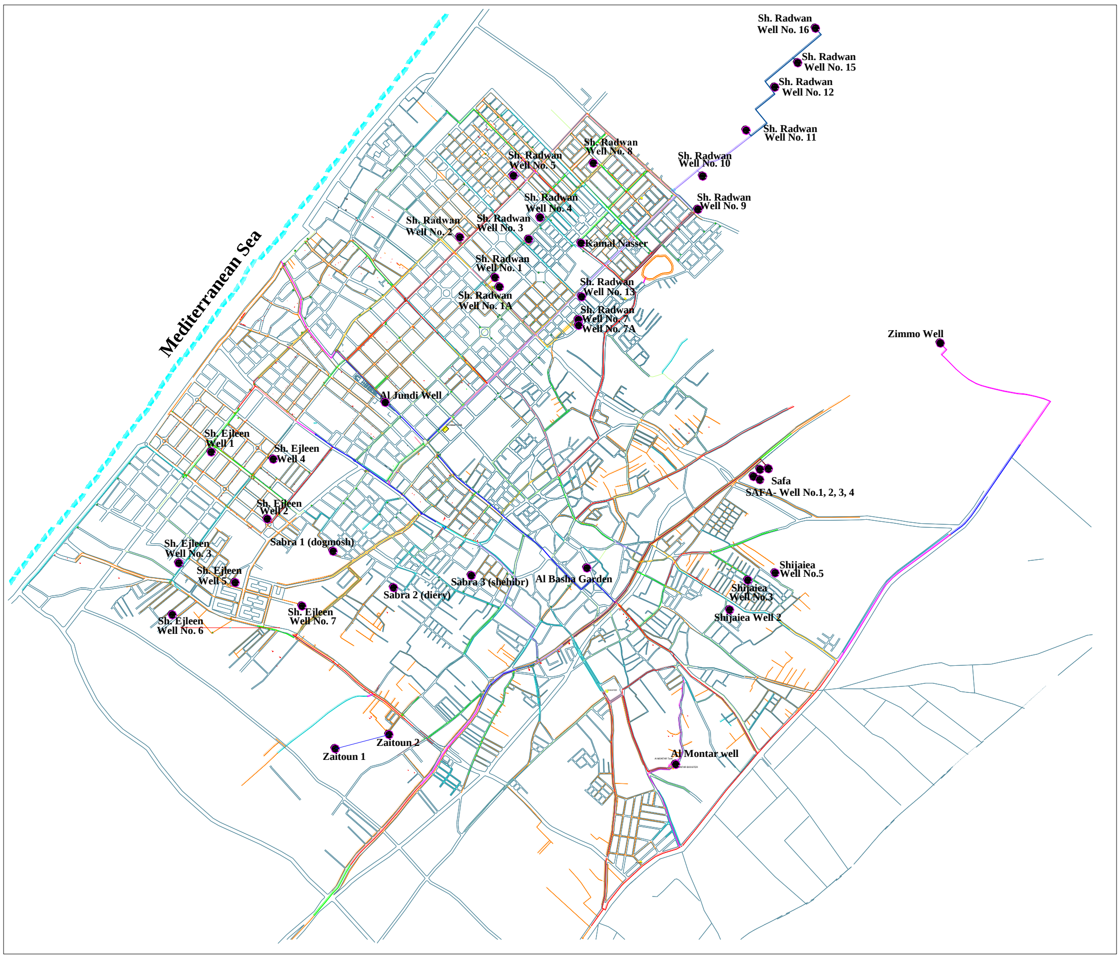


Figure (1.1): Gaza well pumping stations location

1.1 Literature Review

There are main generic parts to the operational automation system: The Master Station (central/host location), the Remote Interface Devices – commonly referred to as Remote Terminal Units (RTUs).

Master Station: Some of the earliest Supervisory Control and Data Acquisition (SCADA) systems were installed in the 1920s. At the time, some high voltage substations adjacent to power plants (aka generating stations) could be monitored and controlled from the power plant’s control room. [5].

In the 1930s, individual utilities started interconnecting to interchange electricity to reduce operating costs. With this came the need to control generation much more closely, so analog computers were developed to monitor and control generator output, tie-line power flows and frequency.

Table (1.1): Gaza well pumping stations coordinates

No.	Well Name	Coordinates		No.	Well name	Coordinates	
		X	Y			X	Y
1	Sh. Radwan 1	98457	104108	21	Safa 1	100779	102497
2	Sh. Radwan 1A	98480	104049	22	Safa 2	100702	102494
3	Sh. Radwan 2	98168	104435	23	Safa 3	100647	102436
4	Sh. Radwan 3	98739	104413	24	Safa 4	100701	102410
5	Sh. Radwan 4	98846	104605	25	Shijaiea 2	100444	101316
6	Sh. Radwan 5	98611	104965	26	Shijaiea 3	100598	101566
7	Sh. Radwan 7	99158	103710	27	Shijaiea 5	100829	101626
8	Sh. Radwan 7A	99155	103751	28	Almontar	099987	100017
9	Sh. Radwan 8	099303	105059	29	Zaitoun 1	97100	100149
10	Sh. Radwan 9	100175	104681	30	Zaitoun 2	97552	100272
11	Sh. Radwan 10	100202	104975	31	Sabra 1 (Dogmosh)	97076	101802
12	Sh. Radwan 11	100596	105332	32	Sabra 2 (diery)	97607	101504
13	Sh. Radwan 12	100825	105709	33	Sabra 3 (shehibr)	98263	101596
14	Sh. Radwan 13	99179	103956	34	Sh. Ejleen 1	96054	102650
15	Sh. Radwan 15	101010	105926	35	Sh. Ejleen 2	96524	102080
16	Sh. Radwan 16	101186	106191	36	Sh. Ejleen 3	95774	101709
17	Remal 1 AlJundi	97524	103059	37	Sh. Ejleen 4	96560	102585
18	Remal 2 kamal naser	99176	104395	38	Sh. Ejleen 5	96253	101546
19	AL Daraj (AlBasha)	99242	101666	39	Sh. Ejleen 6	95719	101275
20	Zimmo	102233	103555	40	Sh. Ejleen 7	96819	101348

By the 1950s the analog computers were enhanced to schedule generation to each generator to provide the lowest cost of generation. These functions were called Economic Dispatch (ED) and Automatic Generation Control (AGC), and the systems were labeled Energy Management Systems (EMS).

In the late 1960s, digital computers and software were developed to replace the analog EMS systems. Software applications were developed to include the off-line analysis functions along with transmission system analysis models. Vendors modified the computer supplier's operating system to meet their design and each set of application software was usually unique for each customer. Thus, when the computers needed to be upgraded or more functions were required the entire Master System had to be replaced. This trend continued into the 1980s and 1990s until open standard operating systems were developed that supported real-time applications. Figure (1.2) illustrates samples of modern SCADA control systems [5].

Figure (1.2): Samples of modern SCADA control system

More recently, some utilities have deployed distributed control systems with area transmission and distribution control centers. Other utilities have installed regional DMS (Distribution Management Systems) which communicate with distribution substations as well as with feeder devices (i.e., reclosers, capacitor bank controllers, sectionalizers and feeder voltage monitors). Today, communications to feeder devices is usually wireless. These systems provide closer control of feeder voltage profiles and faster determination of faulted feeder sections to improve service restoration times.

Remote Terminal Units: In the early application of monitoring and control systems, the interface between the power system and the control system was in a remote location. This interface was designated a Remote Terminal Unit – or RTU. An RTU consisted of a cabinet or panel of terminals for the instrumentation and control wires, which connected it to the power system. The position of the power system switches and circuit breakers were monitored by auxiliary relays. When the relay was closed, the power system switch was closed and a current was present resulting in a binary "1" signal. When the relay and the switch were open the binary count was a "0". Analog values were obtained from potential transformers and current transformers connected to the power system buses and circuits.

The transformer output was 120 Volts AC and nominal 5 Amperes AC; these values were converted by transducers to +/- 1 milliampere DC. The RTU had analog devices to convert the analog values into binary values (usually 8 to 12 bits) [5].

Thus, the digital and analog input values from the power system could be sent as a series of binary values to the master station for display and analysis purposes. The auxiliary relays in the RTU used for controlling power system devices were addressable so the operator could select the address for a specific power system device and function, (open or close) and send the command to the RTU [5].

The RTU remained basically the same until the mid-1970s when rugged microprocessors that could withstand the substation environment became available. The application of microprocessors reduced the hardware complexity of the RTU, but the interface wiring remained unchanged, or even increased as the external milliamp transducers were replaced by internal analog to digital converters. The use of these analog-to digital (A/D) converters required that the AC secondary amperes and voltages be brought to the RTU [5].

The use of microprocessors provided the opportunity to greatly increase the capabilities of the RTU. These capabilities included time keeping, more complex and powerful protocols, individual point numbering, local logging and time tagging of events, higher communication speeds, multiple communication ports and numerous other functions. But the complex and costly interface wiring continued to exist and kept costs relatively high.

In the 1980s, microprocessors began to be applied to protective relays, meters, various controllers and other devices, which usually were equipped with a communications port. As these more powerful devices were deployed, the utilities and system vendors both realized the substation design and complexity could be greatly simplified by interfacing these devices directly into the RTU. As the application of these devices grew, the IEEE Power and Energy Society (PES) Substations Committee determined that a need existed for a unique name to identify them. It was at that point that the term Intelligent Electronic Device (IED) was coined and defined. Soon, almost any device with a microprocessor and a communications port was deemed an IED [5].

In the 1990s, utilities began installing IEDs on their distribution feeders with some communicating to the substation RTU while others communicated directly to the network operations center. In both cases, this extended the reach of their control systems down to the distribution feeder level.

Currently there are tens of thousands, if not hundreds of thousands, of these feeder IEDs in operation that are regularly polled by the SCADA master for updated analog and status data. While these remote IEDs provide monitoring and control capabilities to the system operator, there is little or no automation [5].

1.2 Beit Lahia Wastewater Pumping Station

Palestinian Water Authority conducted a “Northern Gaza Emergency Sewage Treatment” (NGEST) project. It targets to drain the existing effluent lake and convey its partly treated effluent to the new wastewater treatment plant site (WWTP). This project controlled and monitored by SCADA system implemented by Prof. Mohammed Abdelati. This system is considered the first SCADA system applied in Gaza strip [6].

1.3 Thesis Structure

There are seven chapters in this thesis. Chapter1 provides introduction and literature review. Chapter 2 includes description of the SCADA system and its components and architectures. Chapter 3 presents description, analysis and upgrade to Gaza water well station. Chapter 4 discuses communication scenarios that can be used in the designing the SCADA system. Chapter 5 presents the communication system design for remote stations. Chapter 6 include many experiments that are designed to evaluate and demonstrate the communication scenarios described in the previous chapters. Finally, in chapter 7 , conclusions and suggestions for future work are given.

Chapter 2

SCADA System

SCADA stands for Supervisory Control and Data Acquisition [7, 8]. As the name indicates, it is not a full control system, but rather focuses on the supervisory level. It is a software package installed on networked computing platforms, like personal computers (PCs) or small dedicated devices which are hardened for industrial environments [9]. SCADA provides a high level layer on top of the Programmable Logic Controllers (PLCs) [6, 10] layer which is positioned over the plant hardware devices. Thus, we have a functionally modular platform in which there are three layers interacting with each other in a hierarchical manner as sketched in Figure (2.1)

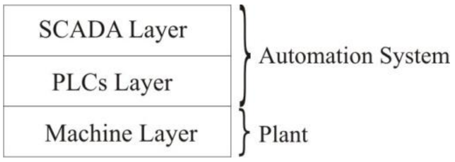


Figure (2.1): Functional decomposition of an automation system

SCADA and OSI: The International Electrical Commission (IEC) has been developing standards or establishing recommendations using one of the two following hierarchical reference models [11]:

EPA (Enhanced Protocol Architecture): Mainly used as communication network architecture among centers and the RTUs (Remote Terminal Unit) [12]. Assuming that these have been multipoint broadcasting networks, the EPA model includes only levels 1, 2 and 7 (Physical, Data link and application levels) of OSI model as illustrated in Figure (2.2). In this model, information integrity and coherence are functions of the data link level, while typical SCADA systems services are carried out by application levels.

OSI (Open System Interconnection): The protocols based in this architectural model have normally, a wider application area than those of previous model, handling the communication among control centers of equal or different hierarchy, the integration of management systems or the use of security mechanisms avoiding access to unauthorized users. These new services, together with the use of commutated telecommunication networks, endows with identity to the intermediate levels of the OSI model (Network, Transport, Session and Presentation) and make impracticable the use of the EPA architecture.

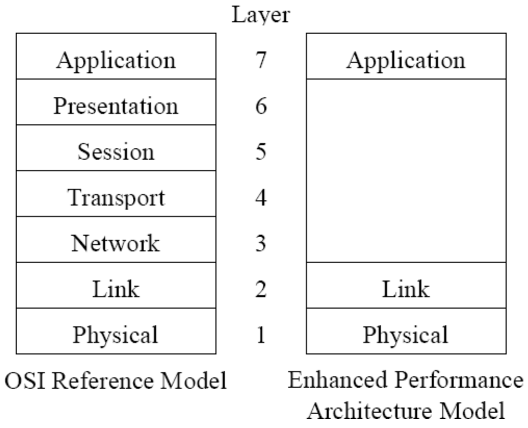


Figure (2.2) OSI and EPA models

Benefits SCADA Systems provide: ASCADA system provides several benefits such as:

1. Reduces operational costs.
2. Provides immediate knowledge of system performance.
3. Improves system efficiency and performance.
4. Increases equipment life.
5. Reduces costly repairs.
6. Reduces number of man-hours (labor costs) required for troubleshooting or service.
7. Frees up personnel for other important tasks.
8. Facilitates compliance with regulatory agencies through automated report generating.

2.1 SCADA System Parts

SCADA systems can be defined by its main parts that are:

1. One or more field data interface devices, usually RTUs, or PLCs, which interface to field sensing devices and local control switchboxes and valve actuators.
2. A communications system used to transfer data between field data interface devices and control units and the computers in the SCADA central host. The system can be radio, telephone, cable, satellite, etc., or any combination of these.

3. A central host computer server or servers (sometimes called a SCADA Center, master station, Master Terminal Unit (MTU) or Main Control Room (MCR)).
4. A collection of standard and/or custom software (sometimes called Human Machine Interface (HMI) software or Man Machine Interface (MMI) software) systems used to provide the SCADA central host and operator terminal application, support the communications system, and monitor and control remotely located field data interface devices.

2.1.1 Master Terminal Unit (MTU)

At the heart of the system is the master terminal unit. The master terminal unit initiates all communication, gathers data, stores information, sends information to other systems, and interfaces with operators. The major difference between the MTU and RTU is that the MTU initiates virtually all communications between the two. The MTU also communicates with other peripheral devices in the facility like monitors, printers, and other information systems. The primary interface to the operator is the monitor or CRT that portrays a representation of valves, pumps, etc. As incoming data changes, the screen is updated.

2.1.2 Remote Terminal Unit

Remote terminal units gather information from their remote site from various input devices, like valves, pumps, alarms, meters, etc. Essentially, data is either analog (real numbers), digital (on/off), or pulse data (e.g., counting the revolutions of a meter). Many remote terminal units hold the information gathered in their memory and wait for a request from the MTU to transmit the data. Other more sophisticated remote terminal units have microcomputers and programmable logic controllers (PLC) that can perform direct control over a remote site without the direction of the MTU. In addition, PLCs can be modular and expandable for the purpose of monitoring and controlling additional field devices. Within the RTU is the central processing unit (CPU) that receives a data stream from the protocol that the communication equipment uses. The protocol can be open like Modbus, Transmission Control Protocol and Internet Protocol (TCP/IP) or a proprietary closed protocol. When the RTU sees its node address embedded in the protocol, data is interpreted and the CPU directs the specified action to take.

During the sixties, many manufacturers developed RTUs with communicative functions that performed a few specific tasks such as monitor and control digital and analog field devices. These “all-in-one” RTUs needed constant communication with the MTU in order to operate. A wide variety of programming languages were used that were not well known or supported. In the eighties the first “micro” PLCs were introduced as the first “Open Architecture” technology which has evolved and gained acceptance.

Some manufacturers now make Remote Access PLCs (RAPLC) specifically designed for SCADA and Data Acquisition applications. These PLCs can:

1. Perform control
2. Check site conditions
3. Re-program anytime from anywhere
4. Have any alarm or event trigger a call to your personal computer.

Today, there are many and different manufacturer types and versions of RTUs and PLCs. Each manufacturer develops his products to accept the market needs. From these products:

1. SOLCON RMU – Remote Monitoring Unit [13]. It enables real time remote supervision, monitoring and parameter modification of the HRVS-DN, RVS-DN or RVS-DX soft starters [14] (or the motor connected to it), installed anywhere around the globe and communicate to remote locations using LAN, GSM (GPRS) or satellite. SOLCON RMU is illustrated in Figure (2.3).

Figure (2.3): SOLCON RMU

2. Remote TRAK RTU and RemoteLog RTU and Datalogger from SIXNET manufacture [15] are illustrated in Figure (2.4).

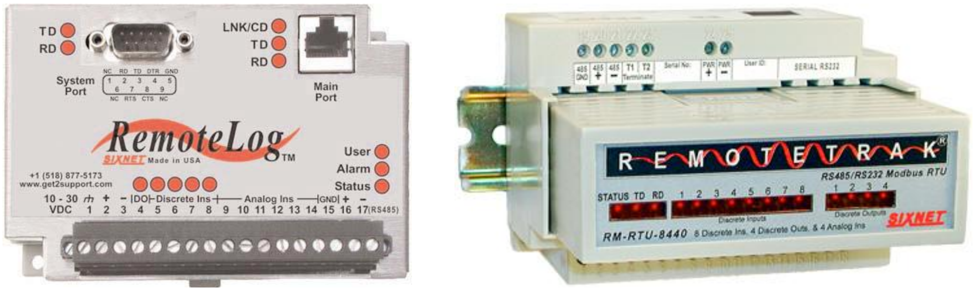


Figure (2.4): SIXNET RTU

3. AutoLog SCADA RTU - Complete system for remote monitoring and control from FF- AUTOMATION, Finland [16], this company sells the product with the solution. Figure (2.5) illustrates the AutoLog RTU.

Figure (2.5): AutoLog SCADA RTU

4. ACE3600 Remote Terminal Unit from Motorola [15]. The ACE3600 RTU combines the local processing of a PLC with the superior communications of an RTU for an all-in-one high-performance unit. It allows seamless integration with multiple PLCs, RTUs and Intelligent Electronic Devices. A powerful processor combined with versatile input/output modules allows this RTU to be used for the most demanding SCADA applications.

Figure (2.6): Motorola RTU

5. Delta PLCs: Delta manufacturer has DVP series of PLCs [18] that are high-speed, stable and highly reliable and applied in various automation machines. Besides its

fast logic operations, abundant instructions, various extension cards and cost-effectiveness, DVP series PLC’s support many communication protocols, seamlessly integrating the industrial automation control system as a whole. Figure (2.7) illustrates samples of Delta PLCs.

Figure (2.7): Delta PLCs

6. SIEMENS PLCs: SIMATIC controllers [19] as illustrated in Figure (2.8) can be expanded flexibly at any time via pluggable I/O, functional and communications modules, providing tailored solutions for all requirements. A wide range of performance, scope and interface options depending on the application.

Figure (2.8): SIEMENS PLC

7. Modicon PLCs: considered one of intelligent and more convoluted used in complicated control system [20], but rarely used in Gaza. Figure (2.9) illustrates one type of these PLCs.   Convoluted

Figure (2.9): Modicon PLC

2.1.3 Communications Equipment

Communication equipment is required for bi-directional communications between an RTU and the MTU. This can be done through public transmission media or atmospheric means. Note that it is quite possible that systems employ more than one means to communicate to remote sites. SCADA systems are capable of communicating using a wide variety of media such as fiber optics, dial-up, or dedicated voice grade telephone lines, or radio. Chapter 4 will illustrate all SCADA communication systems and their relation with our research.

2.1.4 SCADA Software’s

There are many software packages in today’s Information Technology (IT) market which enables engineers with moderate programming experience to build SCADA applications [21]. SCADA server applications handle data archiving, alarm processing and events logging. Main parts of the SCADA system are the device driver (PLC/RTU drivers) and the database [22] servers. OLE[1] for Process Control (OPC) [23] is an open standard designed to bridge process control hardware and software applications. An OPC server is simply a PLC device driver which enables programmers to communicate with the PLC through a standard interface. SQL server from Microsoft Company is widely used for data archiving, alarm processing and events logging. SMTP server from Microsoft Company may be used to build email and SMS alarm messages to alert the operators about unacknowledged alarm events happened for longer time than adjustable set delay time. SCADA systems include a HMI which uses graphical interface to visualize the state system variables, change set points, alerts operators of critical condition and generate data trends.

As we mentioned before, SCADA software is one of the main parts of the SCADA system. There are several software packages used for designing HMI and SCADA. WINCC from SIEMENS, Cimplicity HMI from General Electric, and Lookout from National Instruments are well known examples for efficient commercial SCADA packages. However, professional computer programmers are biased to standard programming languages and tools in building SCADA applications. This lower level programming approach offers them more freedom to configure their project with highly

[1] OLE stands for Object Linking and Embedding which is a technology that allows embedding and linking to documents and other objects developed by Microsoft.

reduced restrictions which are associated to these higher level packages. Moreover, while using standard programming languages allows SCADA developer to put their own character in the final product, the cost of extra programming efforts is fairly compensated by savings in software packages expenditure.

2.1.4.1 Human Machine Interface (HMI)

SCADA system includes a user interface, usually called Human machine Interface (HMI). The HMI of a SCADA system is where data is processed and presented to be viewed and monitored by human operator. This interface usually includes controls where the individual can interface with the SCADA system.

HMI’s are an easy way to standardize the facilitation of monitoring multiple RTUs or PLCs. RTUs or PLCs runs a pre programmed process, and spread out over the system so monitoring each of them individually may be difficult. Also, RTUs and PLCs have no standardized method to display or present data to the operator, the SCADA system communicate with the PLCs through the system network and processes information that is easily disseminated by the HMI. HMI’s can also be linked to database, which can use data gathered from PLC’s or RTU’s to provide graphs of trends, logistic information, schematics for specific sensor or machine or even make troubleshooting guides accessible . In the last decade, practically all SCADA systems include an integrated HMI and PLC device making it extremely easy to run and monitor a SCADA system.

2.1.4.2 OPC Server

OPC stands for OLE for Process Controls and the industrial applications of Microsoft’s OLE technology that comes with every Windows operating system. The OPC designers put forth the goal of developing a single client/server specification that would allow any vendor to develop software and applications that could share data in a fast, robust fashion, and do it in a way that would eliminate the proprietary schemes that forced these same vendors to duplicate development efforts. The OPC designers developed the first specification called Data Access Specification 1.0a that was released in early 1996. Using this specification, vendors were able to quickly develop client server software. A major goal of the OPC designers and the Data Access specification was to eliminate the need of client application vendor's to develop their own proprietary set of communications drivers. For many vendors, the effort required to develop numerous communications drivers outweighed the development effort involved in the client application itself. With the adoption of OPC technology a vendor could now focus their efforts almost exclusively on the development of the client application. The Data Access specification defines how both the client and the server application interface must be constructed. If the specification is followed properly, a client vendor knows that any OPC server that exists for an industrial device can provide the connectivity needed for data access. Issues like time to market or reliability no longer restrict applications to which any OPC compatible application can address. OPC has given the end user the additional benefit of being able to select the best of breed software to solve application problems. Historically, if the application software did not have the desired communication driver or if the available driver didn't perform adequately, the only solution was to try to persuade the application vendor to either develop the desired driver or repair an existing driver. The time required in either of these cases was usually never short. With OPC, the end user is no longer tied to the resource limitations of the client application vendor. The user can now choose from a variety of OPC server vendors to address a new driver requirement or remedy a performance issue. Equally, the client application vendor can now focus on the continued improvement of their core product without the disruptive effort required to address communication issues and needs. Our goal within the OPC environment is to be a leading provider of the server component of the OPC equation and to do so by providing a product that is reliable and easy to use. This server is built upon years of development efforts in communications driver development and OPC technology [24].

In the SCADA, OPC allows multiple applications to simultaneously access the SCADA communications system. The OPC specification is maintained by an independent interested body called the OPC foundation. It is made up of over 200 manufacturers and other interested organizations.

For the SCADA, there are two parts to an OPC system. The first is the OPC server. There are number of Modbus OPC servers available depending on the functionality required. It is the OPC server’s responsibility to send/receive data from the SCADA system. The second part is the clients. Typical clients are host systems such as wondeware, FIX or Factory Link, as well as spreadsheets, database, or applications running Visual Basic C++. Also manufacturers can add additional clients which allow for remote firmware changes and program editors.

In this manner, OPC allows a manufacturer’s programming tools to simultaneously communicate through the OPC server with an RTU that is being programmed while a host is also communicating with the balance of the RTUs in the field. It should be noted that the OPC server manages the communications network, and as such, while it appears simultaneous, only one message goes at a time. The more correct description would be multiplexing messages. However, considering most municipal systems react in terms of minutes or hours, a small slowdown in the system performance to maintain a system in quite justified.

KEPServerEX: KEPServerEx is a 32-bit windows application that provides a means of bringing data and information from a wide range of industrial devices and systems into client applications on your windows PC. KEPServerEx falls under the category of a "Server" application. It is very common to hear the term "client/server application" in use across many software disciplines and business segments. In the industrial market, it has usually come to mean the sharing of manufacturing or production data between a variety of applications ranging from human machine interface software and data historians, to large MES and ERP applications [25].

2.1.4.3 Database Server

SCADA Database servers are one of most important software’s used by SCADA system. Any of the database servers used to store and implement data as SQL server, SQL Server Desktop, Access and Oracle. The traditional database servers used in SCADA systems is SQL server from Microsoft Company. OPC servers deal with database servers in managing SCADA system data which includes Data Logging archiving, paging, alarm and authentication. All system data is stored in the database server. Then it is managed by the SCADA system designer to display the data to the operator simply and quickly using different ways of data management as alarms, SMS messages and reports.

2.2 SCADA Protocols

The important part of any complex SCADA system design is involved in matching the protocol and communication parameters between connecting devices. There are about 200 such real time user layer and application protocols. These include proprietary and non- proprietary protocols, some of which are listed below [26]:

- Modbus RTU / ASCII
- PROFIBUS Omron
- CANbus

Siemens Sinuate

- Mitsubishi
- Other Vendor Protocols

The industry is now moving away from many of the old and proprietary protocols. The following RTU/PLC protocols are emerging as virtual standards in modern SCADA systems.

2.2.1 Modbus

Modbus is one of most important protocols used by SCADA system; it has its roots in the late seventies of the previous century by Modicon PLC manufacturer. It is an open standard that described the messaging structure. The physical layer of the Modbus interface was free to choose. The original Modbus interface ran on RS232, but later Modbus implementations used RS485 because it allowed longer distances, higher speeds and the possibility of a true multi-drop network. In a short time hundreds of vendors implemented the Modbus messaging system in their devices and Modbus became the de facto standard for industrial communication networks [27].

The nice thing of the Modbus standard is the flexibility, but at the same time the easy implementation of it. Not only intelligent devices like microcontrollers, PLCs etc. are able to communicate with Modbus, also many intelligent sensors are equipped with a Modbus interface to send their data to host systems.

Modbus message structure: The Modbus communication interface is built around messages. The format of these Modbus messages is independent of the type of physical interface used. The same protocol can be used regardless of the connection type. Because of this, Modbus gives the possibility to easily upgrade the hardware structure of an industrial network, without the need for large changes in the software. A device can also communicate with several Modbus nodes at once, even if they are connected with different interface types, without the need to use a different protocol for every connection. On simple interfaces like RS485 or RS232, the Modbus messages are sent in plain form over the network. In this case the network is dedicated to Modbus. Although the main Modbus message structure is peer-to-peer, Modbus is able to function on both point-to-point and multi drop networks.

Each Modbus message has the same structure. Four basic elements are present in each message as shown in Table (2.1). The sequence of these elements is the same for all messages, to make it easy to parse the content of the Modbus message. A conversation is always started by a master in the Modbus network. A Modbus master sends a message and—depending of the contents of the message—a slave takes action and responds to it. There can be more masters in a Modbus network. Addressing in the message header is used to define which device should respond to a message. All other nodes on the Modbus network ignore the message if the address field doesn’t match their own address.

Table (2.1): Modbus Message Structure

Device address	Address of the receiver
Function code	Code defining message type
Data	Data block with additional information
Error check	Numeric check value to test for communication errors

Modbus serial transmission modes: *Modbus/ASCII and Modbus/RTU:* Serial Modbus connections can use two basic transmission modes, ASCII or RTU, remote terminal unit. The transmission mode in serial communications defines the way the Modbus messages are coded. With Modbus/ASCII, the messages are in a readable ASCII format. The Modbus/RTU format uses binary coding which makes the message unreadable when monitoring, but reduces the size of each message which allows for more data exchange in the same time span. All nodes on one Modbus network segment must use the same serial transmission mode. A device configured to use Modbus/ASCII cannot understand messages in Modbus/RTU and vice versa.

When using Modbus/ASCII, all messages are coded in hexadecimal values, represented with readable ASCII characters. Only the characters 0…9 and A…F are used for coding. For every byte of information, two communication-bytes are needed, because every communication-byte can only define 4 bits in the hexadecimal system. With Modbus/RTU the data is exchanged in a binary format, where each byte of information is coded in one communication-byte.

Modbus messages on serial connections are not sent in a plain format. They are framed to give receivers an easy way to detect the beginning and end of a message. When using Modbus/ASCII, characters are used to start and end a frame. The colon ':' is used to flag the start of a message and each message is ended with a CR/LF combination. Modbus/RTU on the other hand uses time gaps of silence on the communication line for the framing. Each message must be preceded by a time gap with a minimum length of 3.5 characters. If a receiver detects a gap of at least 1.5 characters, it assumes that a new message is coming and the receive buffer is cleared. The main advantage of Modbus/ASCII is that it allows gaps between the bytes of a message with a maximum length of 1 second. With Modbus/RTU it is necessary to send each message as a continuous stream. Table (2.2) illustrates the message frame of ASCCII and RTU modes, and Table (2.3) [27] illustrates the properties of Modbus/ASCII and Modbus/RTU.

Table (2.2): Modbus Message Frame

Message Frame	**Start**	**Address**	**Function**	**Data**	**LRC Check**	**End**
ASCII	I CHAR	2 CHARS	2 CHARS	n CHARS	2 CHARS	2 CHARS CRLF
RTU	T1-T2-T3-T4	8 BITS	8 BITS	n x 8 BITS	16 BITS	T1-T2-T3-T4

Table (2.3): Properties of Modbus/ASCII and Modbus/RTU

	Modbus/ASCII	**Modbus/RTU**
Characters	ASCII 0…9 and A..F	Binary 0…255

Error check	LRC Longitudinal Redundancy Check		CRC Cyclic Redundancy Check	
Frame start	character ‘:’		3.5 chars silence	
Frame end	characters CR/LF		3.5 chars silence	
Gaps in message	1 sec		1.5 times char length	
Start bit	1		1	
Data bits	7		8	
Parity	even/odd	none	even/odd	none
Stop bits	1	2	1	2

Modbus addressing: The first information in each Modbus message is the address of the receiver. This parameter contains one byte of information. In Modbus/ASCII it is coded with two hexadecimal characters, in Modbus/RTU one byte is used. Valid addresses are in the range 0..247. The values 1..247 are assigned to individual Modbus devices and 0 is used as a broadcast address. Messages sent to the latter address will be accepted by all slaves. A slave always responds to a Modbus message. When responding it uses the same address as the master in the request. In this way the master can see that the device is actually responding to the request [27].

2.2.2 PROFIBUS

ROFIBUS (*PROcess Field BUS*) [28] is a well-proven, widely accepted open fieldbus standard, which is supported by an industry supplying a wide range of equipment, tools and support. PROFIBUS was introduced in 1989 as German standard DIN 19245, later adopted as International Standard EN 50170. The PROFIBUS standard is now incorporated into IEC 61158, the international fieldbus standard.

The PROFIBUS Family: The PROFIBUS family consists of three compatible version offering very high integrity and a capability appropriate to the need.

- PROFIBUS DP – *Decentralised Periphery*
- PROFIBUS FMS – *Fieldbus Message Specification*
- PROFIBUS PA – Process Automation

All three systems can operate together; DP and FMS share the same electrical transmission system (RS485), PA uses a different electrical transmission system (IEC 1158-2) but shares the same protocol as DP and FMS. PROFIBUS DP extensions and the integration of PROFIBUS with Ethernet technology (PROFINet) mean that FMS is less important than in the past. FMS is no longer supported by PROFIBUS International, however there are still FMS installations successfully operating.

Areas of applicability: Because of the compatible versions, PROFIBUS is applicable to a wide range of applications:

- Simple low-cost distributed control and automation.
- High-speed, time-critical applications.
- Expensive/complex communication tasks.
- Operation in hazardous environments.

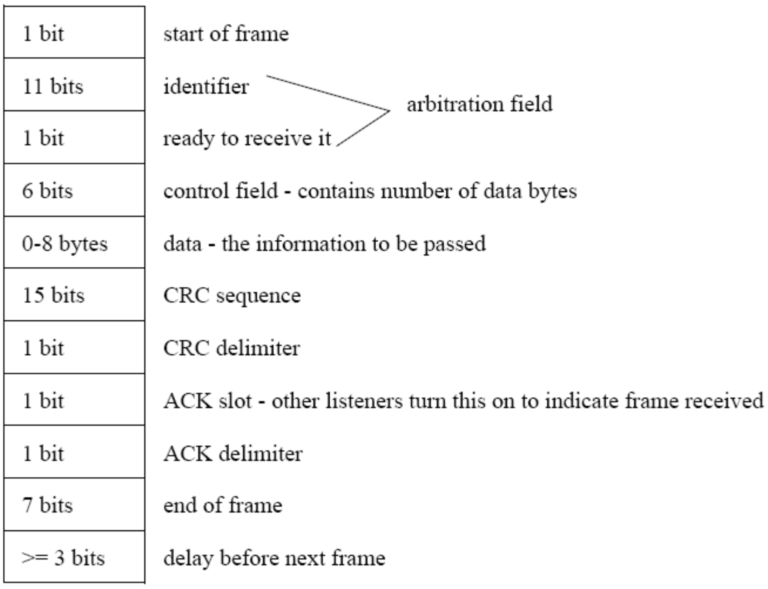
Recent developments mean that PROFIBUS is also applicable to:

- High reliability, safety critical systems (PROFISafe).
- Integration with management IT systems (PROFINet).

2.2.3 CANbus

The CANbus (Controller Area Network bus) standard is part of the Device net standard. Integrated circuits are now sold by many of the major vendors (Motorola, Intel, etc.) that support some, or all, of the standard on a single chip. This section will discuss many of the technical details of the standard. CANbus covers the first two layers of the OSI model. The network has a bus topology and uses bit wise resolution for collisions on the network (i.e., the lower the network identifier, the higher the priority for sending). A data frame is shown in Figure (2.10) [29]. The frame is like a long serial byte. It begins with a start bit. This is then followed with a message identifier. For Device net this is a 5 bit address code (for up to 64 nodes) and a 6 bit command code. The “Ready to receive it” bit will be set by the receiving machine. (Note: both the sender and listener share the same wire.) If the receiving machine does not set this bit the remainder of the message is aborted, and the message is resent later. While sending the first few bits, the sender monitors the bits to ensure that the bits send are heard the same way. If the bits do not agree, then another node on the network has tried to write a message at the same time - there was a collision. The two devices then wait a period of time, based on their identifier and then start to resend. The second node will then detect the message, and wait until it is done. The next 6 bits indicate the number of bytes to be sent, from 0 to 8. This is followed by two sets of bits for CRC (Cyclic Redundancy

Check) error checking, this is a checksum of earlier bits. The next bit ACK slot is set by the receiving node if the data was received correctly. If there was a CRC error this bit would not be set, and the message would be resent. The remaining bits end the transmission. The end of frame bits are equivalent to stop bits. There must be a delay of at least 3 bits before the next message begins.



1 bit	start of frame
11 bits	identifier
1 bit	ready to receive it
6 bits	control field - contains number of data bytes
0-8 bytes	data - the information to be passed
15 bits	CRC sequence
1 bit	CRC delimiter
1 bit	ACK slot - other listeners turn this on to indicate frame received
1 bit	ACK delimiter
7 bits	end of frame
>= 3 bits	delay before next frame

arbitration field

Figure (2.10): CANbus Frame

2.3 Hardware Architecture

Well stations are the remote sites that should be connected to the main control room which is proposed to be at Gaza Municipality. The main reason of selecting this location is the fact that it is located in the middle of the city and characterized by a high altitude. This feature is preferable for possible wireless communications.

Well stations contain field instruments and equipments connected to devices being controlled and monitored. They convert physical parameters to electrical signals, which are the lower layer of the automation system. Then these devices are connected to process controllers, PLCs and RTU. Process controllers control the field devices, operate the station automatically, gathering data from the field devices and provide data to the main control room. Main control room contains SCADA servers that store data from PLCs and RTUs, regulate the control system, provide HMI for the operators and send SMS messages (Alarms) to the operator. The connection between the process controllers and the SCADA servers may be established using different techniques. It is our main objective in this research to highlight these techniques along with their features and limitations. Figure (2.11) illustrate most common communication scenarios, nearby well stations may be connected using direct cables (RS232, RS485 or Ethernet) while faraway stations may be connected through the Public Switch Telephone Network (PSTN), cellular system or wireless private connection.

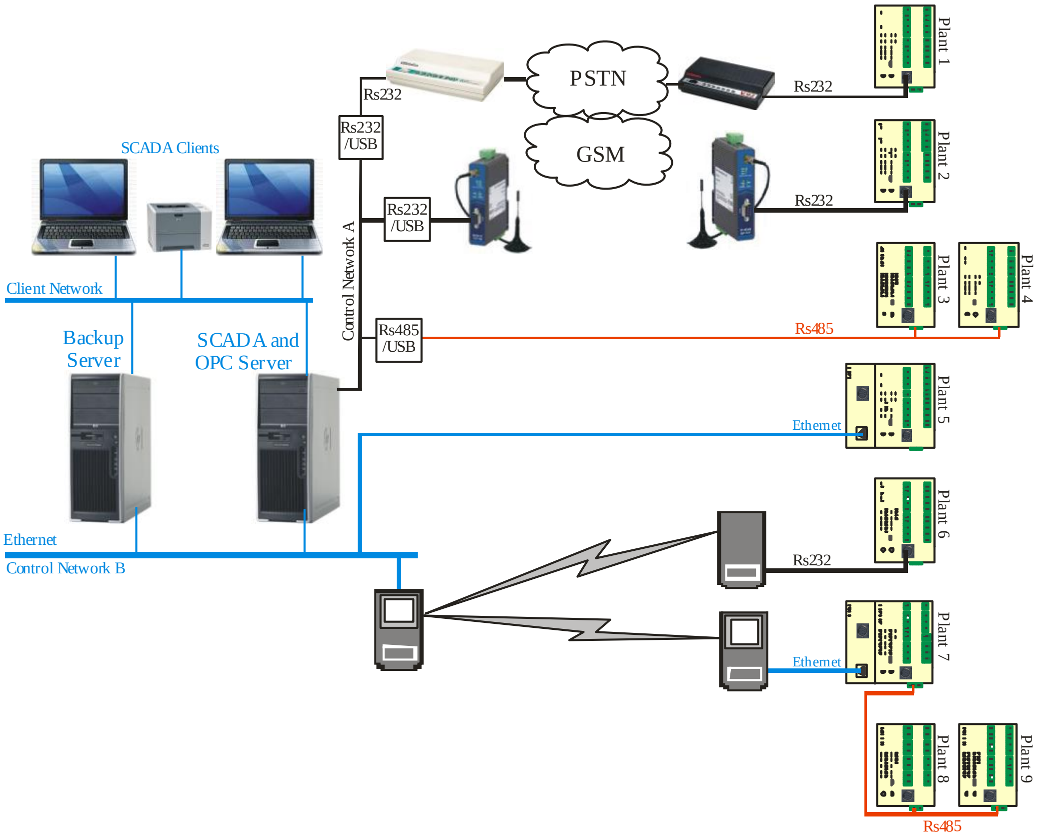


Figure (2.11): Hardware architecture

2.4 Software Architecture

Figure (2.12) illustrates the traditional relational connection between the plants and SCADA server along with the software relations between the SCADA server components. GSM and dialup plants connect to OPC server through the USB port by using RS232/USB converter, but they are defined as modems, and OPC server use dialing to connect to the PLCs to read and write data. RS485 direct connection bus connected to the OPC server through USB port by using RS485/USB converter [30]. The OPC server uses Modbus protocol [31, 32] in communication between the RS485 PLCs bus. Wireless plants connect to the SCADA server through Ethernet network and has software package used as communication driver between the wireless remote sites and the SCADA server. Direct Ethernet connection connects to the OPC driver through Ethernet port. Plants 8 and 9 use the same communication driver that is used with plant 7 which has the main communication with the OPC, plants 8 and 9 communicate with plant 7 only, and has no direct connection with the SCADA server.

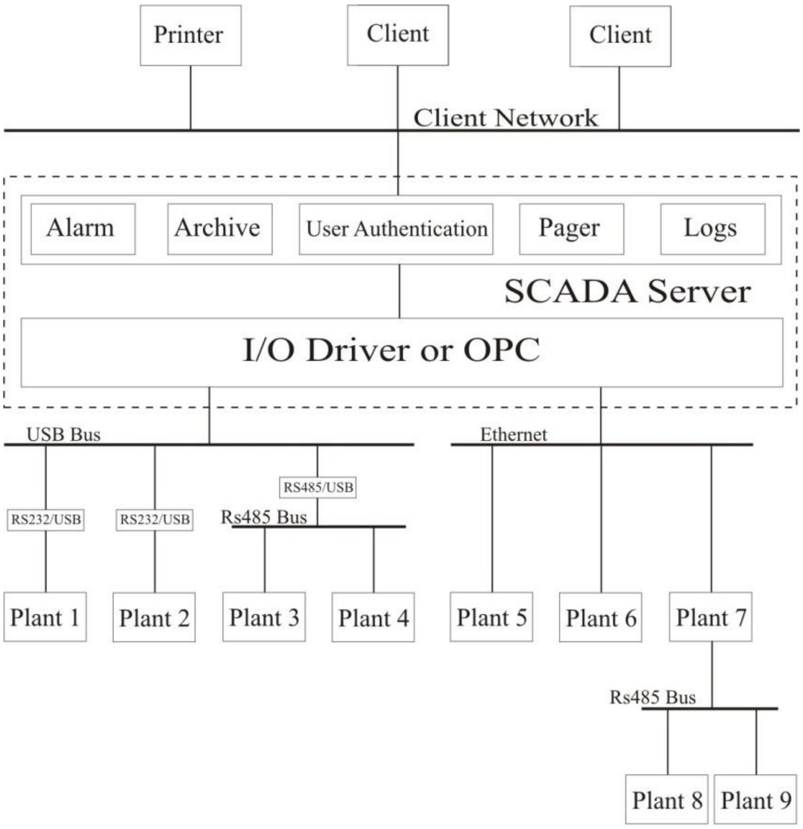


Figure (2.12): Software Architecture

Chapter 3

System Analysis

Gaza water well stations vary between new and old stations. All stations have almost the same components and instruments. Old stations components need maintenance and replacement, while new stations components are good.

3.1 System Components

Atypical station consists of a pumping station, a dosing chlorine pump, a chlorine tank, a pressure meter, a non return valve, a sand trap, an electrical generator, a soft starter and a main electrical distribution board. Figure (3.1) illustrates two types of pumping stations, pumping stations that differ in the pumping type. Now we will illustrate these types and classify the pumping station components:

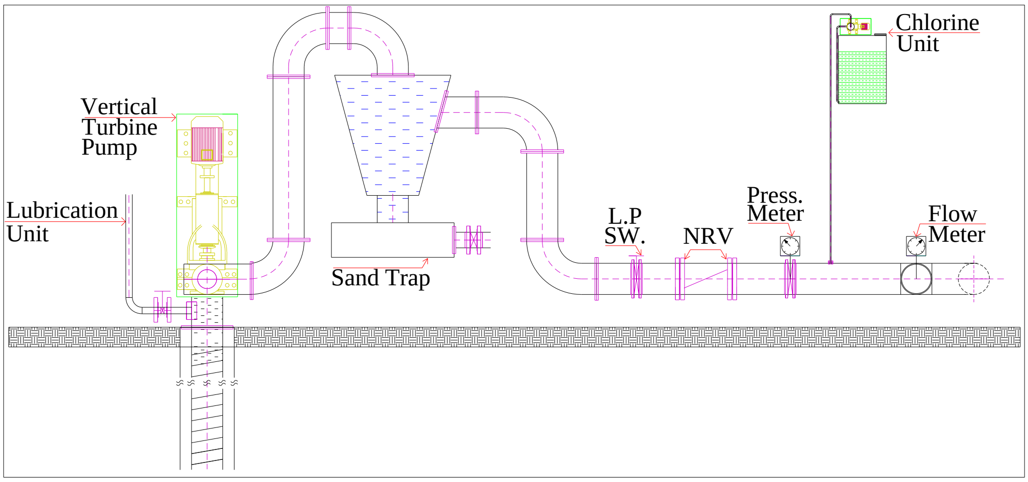
***Water Pump*:** There are two types of pumps vertical turbine (overhead) pumps and submersible pumps. Vertical turbine pumps have high capacity as it pumps for 100-200 m^3 per hour, where submersible pumps used for 40-60 m^3 per hour. Vertical turbine pumps need lubrication unit.

Lubrication Unit: Used only with vertical turbine pumps to prevent friction. This unit consists of water tank (500 L) used to splash water before the pump operation.

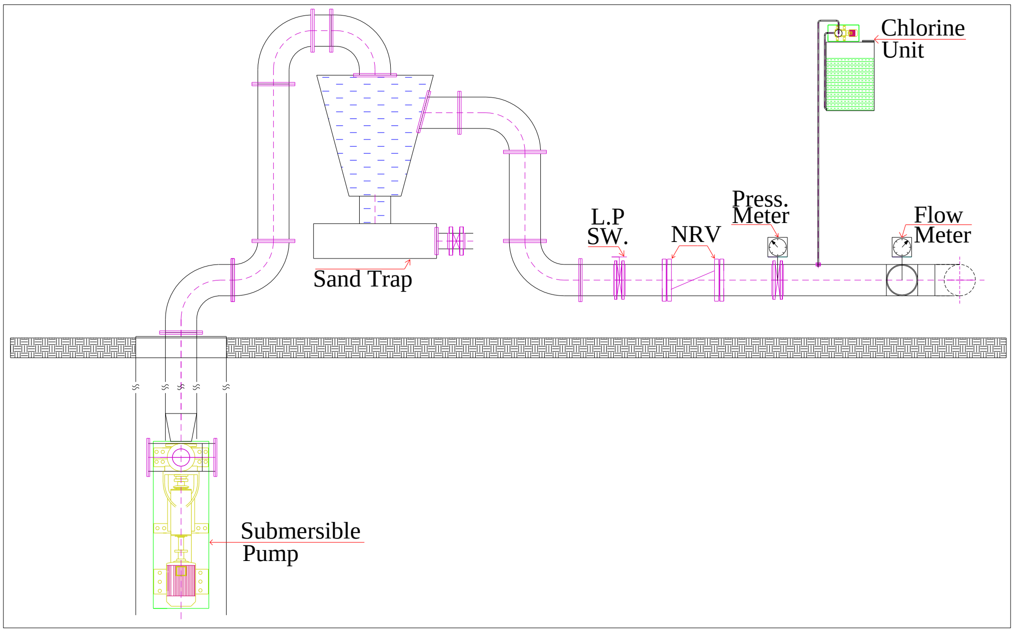
Soft starter: Soft starter used at start operation to limit the high starting current of the water pump motor. After adjustable period around (20 sec), By-pass contactor connects the pump station motor directly with the power supply and disconnects the soft starting. Although water pump motor by-pass connection, soft starter remain monitoring and measuring the electrical parameters of the pump station motor.

Chlorine dosing Unit: Chlorine dosing unit is small pump doses chlorine in the pumped water before connection to the main distribution network. This chlorine is important to sterilize water.

Non Return Valve (NVR): There is a Non Return Valve (NRV) on the water distribution line in station. NRV used to let the water move in one direction from the well to the water distribution line and prevent the opposite. This valve closed when water pumped from the station to the main water distribution network and used as indication the pump is pumping water and the system working is okay.



(a): Well station with vertical turbine pump



(b): Well station with submersible pump

Figure (3.1): Well station with vertical turbine and submersible pump

Electrical Generator: Nearly all the stations have stand by electrical generator used as a source of electricity when the main electricity cut off. Some of these generators have spare fuel tank and others has its main fuel tank only. Electrical generator capacity ranges from 60 KVA to 200 KVA depending on the station capacity.

Main Electrical Distribution Board: Main electrical distribution board contains the main electrical power supply from Gaza Electricity Distribution Corporation (GEDCO) and from the stand by electrical generator; also this board contains the station electrical control system.

Control system: Control system used to control the station operation; this system depends on relays, timers, switches, contactors on controlling the pump station system, and doesn't depend on process controllers PLCs or RTUs. Recently we will classify this system in details.

3.2 Control System Operation

In this section we will classify the present control system of well station pumps which is based on hardwiring using relays and timers. Then update and upgrade this system to be compatible with the SCADA systems. Submersible pump control is simpler than vertical turbine pump control since it has no lubrication unit.

Present control system: The present process control of vertical turbine pumping station is shown in Figures (3.2, 3.3, and 3.4) that include 24V DC control circuit diagram, 220 V AC control circuit diagram and the Main Distribution Board (M.D.B) diagram. These diagrams may be described as follows:

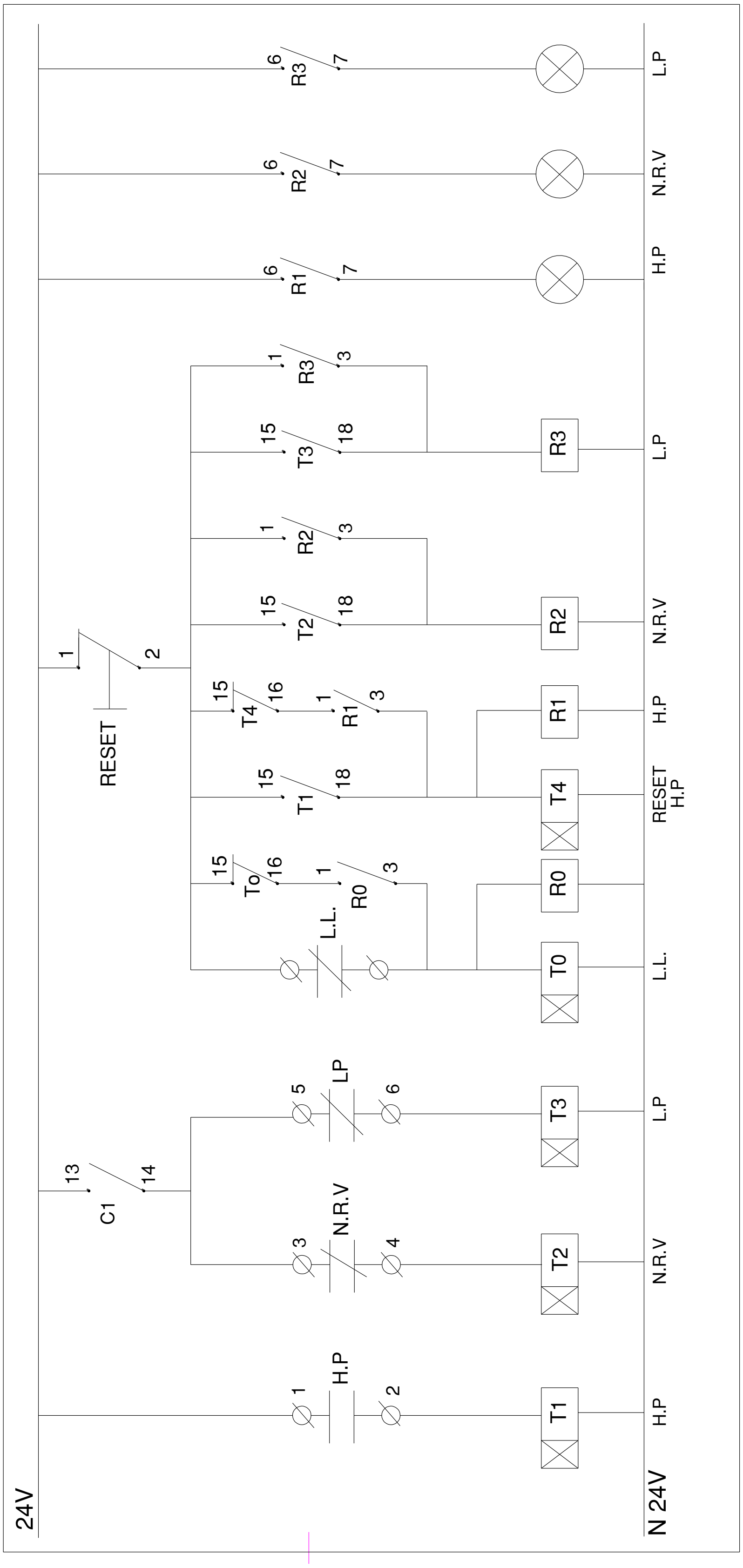


Figure (3.2): Control circuit diagram 24V DC

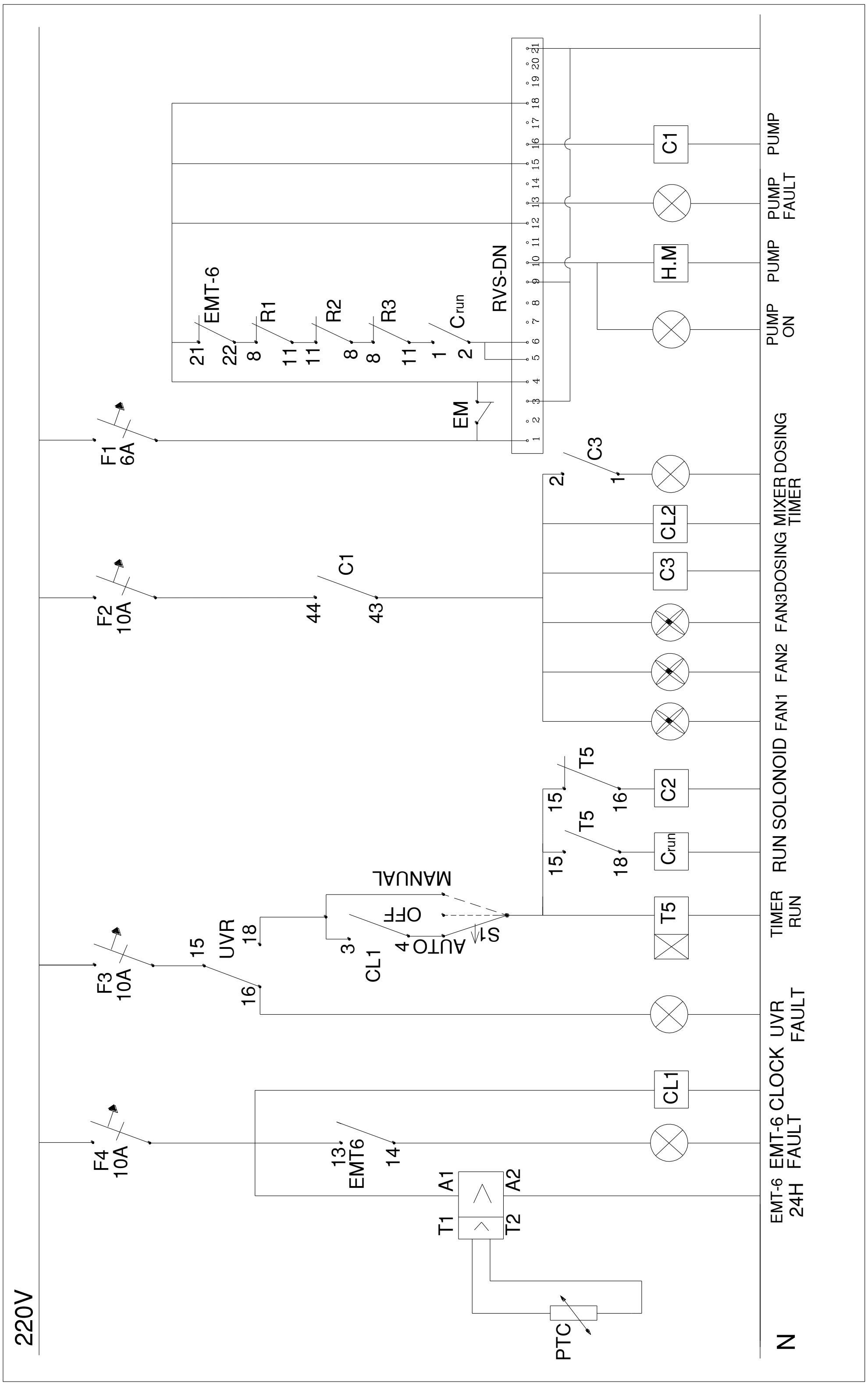


Figure (3.3): Control circuit diagram 220V AC

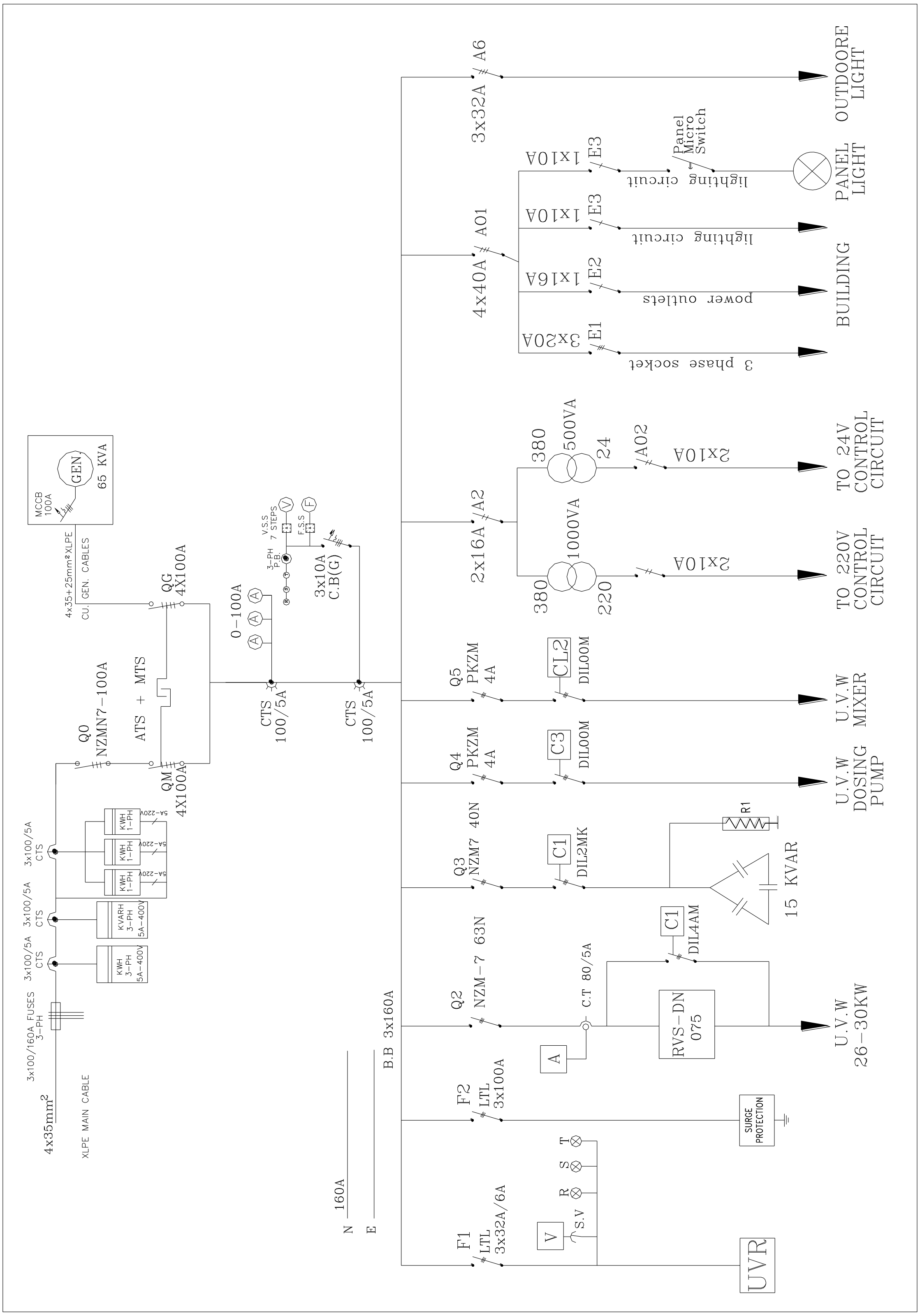


Figure (3.4): Main Distribution Board (M.D.B.) details

24V DC Control Circuit Diagram: Consist of devices operate using 24V DC which are: high pressure (HP) switch, low pressure switch (LP), NRV switch (NRV) and 4 timers. Every switch connected to timer that is preset with specific period of time. When the switch reached its preset threshold value its timer relay will be connected after the preset period of time of its timer.

220V AC Control Circuit Diagram: Consists of devices operate using 220V AC which are: Manual switch with 3 steps, EMT6 (Overload monitoring system for machines operating in increased safety area) [33], Under Voltage Relay (UVR), Clock timer, Hour meter and the soft starter circuit.

The two diagrams shared in controlling the water pump station as follows:

1. There are two options to operate the station, *Automatic* run that depends on preprogrammed clock timer and *Manual* run that depends on the operator.
2. Starting the system runs Timer 5 (T5) for 60 sec, during this time lubrication unit splash water on the rubber shaft of vertical turbine pumps.
3. After the set time of T5, and if there is not any fault in the control system, soft starter [15] runs the motor pump in acceleration speed for 20 sec.
4. Then, by-pass contactor (C1) runs the motor pump station through by-pass.
5. Pumped water opens the NRV and its timer (T2). T2 is NRV timer and preset for 20 sec. if the NRV remain close.T2 will stop the system after this preset time.
6. T1 and T3 timers for high and low pressure switches respectively. If pressure reached the preset threshold value (high /low) for 60 sec, these timers will stop the system.
7. T4 timer used to reset T1 timer after specific period to prevent hysteresis.

Upgrade Control System: A remote terminal unit should be installed to integrate the plant with the SCADA system. Therefore, a simple upgrade is required to allow handling the I/O signals summarized in Table (3.1).

Table (3.1): I/O system signals

NO.	Signal	Type	NO.	Signal	Type
1.	Is Remote	Digital input	9.	Fuel low level	Digital input
2.	Is Manual	Digital input	10.	Generator Fault	Digital input
3.	Soft starter fault	Digital input	11.	Flow meter	Analog input
4.	Pump in operation	Digital input	12.	Pressure meter	Analog input
5.	NRV	Digital input	13.	Pump operation	Digital output
6.	Chlorine level	Digital input	14.	Lubrication valve	Digital output
7.	Moist. /Over temp.	Digital input	15.	RS-VDN (RS485 bus)	Data bus (I/O)
8.	Power Fall	Digital input			

Upgrade of the system depends on adding new components that are needed for the SCADA system while keeping the previous control system components. New components will robust and upgrade the protection system and increase the benefits from the SCADA system in monitoring water well station and archiving its data. The components ought to be added are:

1. Delta PLC, recommended being of DVP28SV model.
2. Switch sensors for chlorine tank and fuel tank.
3. RS485 card for SOLCON soft starts may be added to connect the soft starter with the PLC through RS485 port, to reed soft starter parameters.
4. Electrical pressure meter, to send signals to the PLC to calculate the pressure in the water distribution network and adjust its threshold to be ad high pressure switch.
5. Flow meter, to calculate the quantity of the water pumped from the station. This data is important and archived in the SCADA system. This data is one important factor in Development and upgrading to water distribution system.
6. UPSs are added to operate the PLC and the communication unit for nearly 1 hour, when the main electrical current cut off.
7. Control and Status (CAS) [34] used as low level water switch installed in the well and used to protect the system if the water level in the well is low.

The new upgraded system will have the ability to run the new control system with all its original options along with the additional supervisory and data acquisition features. Figures (3.5, 3.6 and 3.7) illustrate the upgrade control circuit diagrams and the PLC control circuit diagram. The new control system will depend on:

1. PLC input signals will be from the present control system devices (switches, valves, NZM [35], EMT6, soft starter, and generator).
2. Output signal will used to run the soft starter.
3. The PLC will be programmed to control the pump using previous signals.
4. New control system will has three operation methods: local manual depending on the operator and monitored with the PLC, local automatic depending on clock timer, relays and timers and also monitored with PLC, the third method of operation is automatic remote and supervisory control depending on the PLC and supervisory by the SCADA system.
5. Any fault signal will be implemented in the PLC, and a reaction response will be activated.
6. PLC will be responsible on controlling the station operation as run/stop the pump through the soft starter, run lubrication solenoid valve and send alarms when the fault happen.

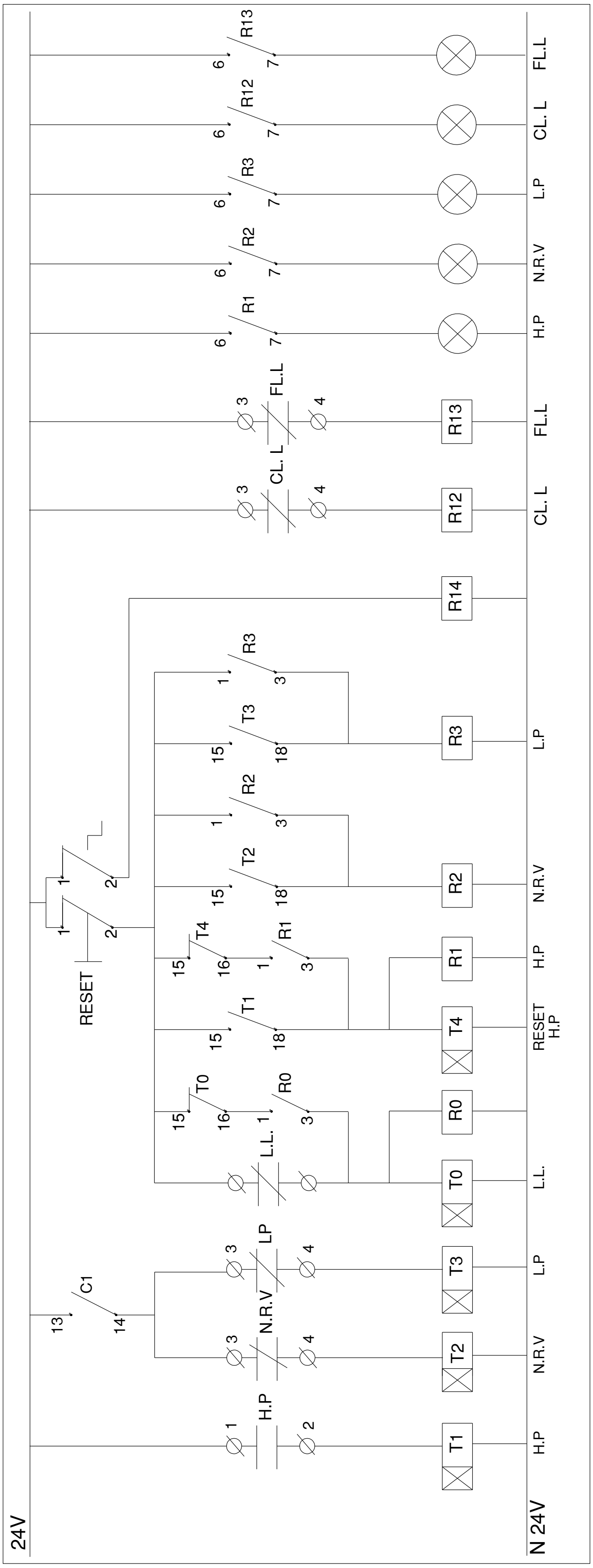


Figure (3.5): Upgrade control circuit diagram 24V DC

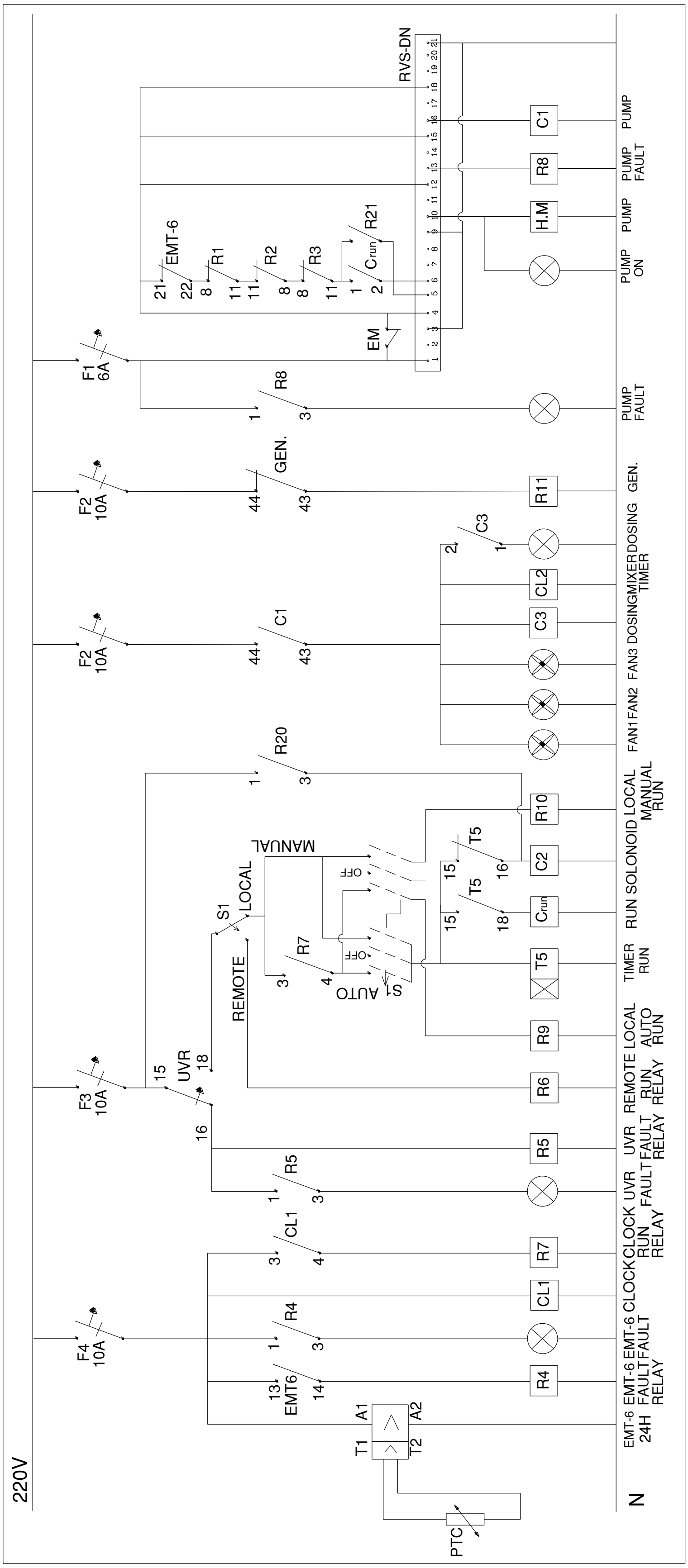


Figure (3.6): Upgrade control circuit diagram 220V AC

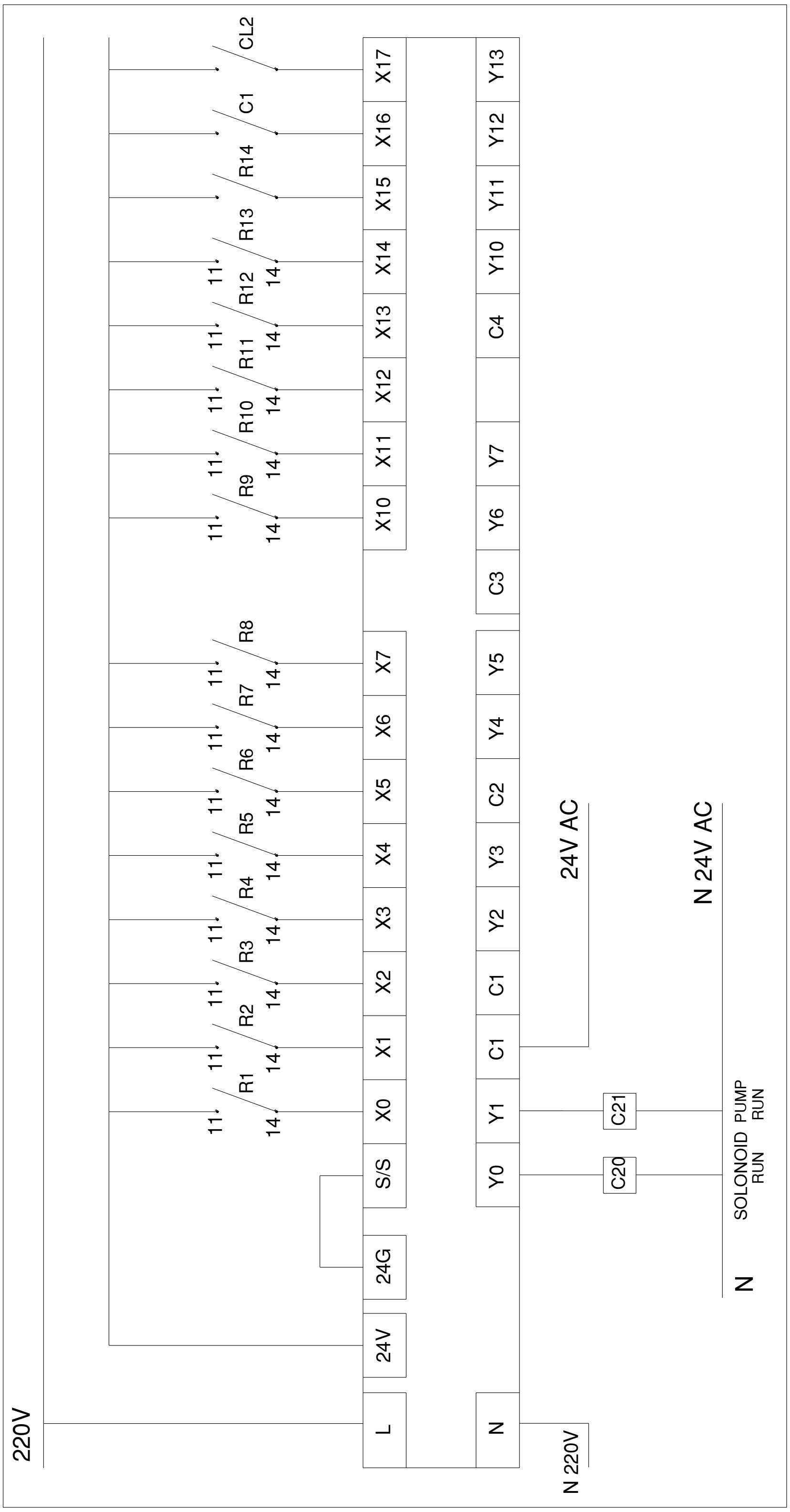


Figure (3.7): PLC control circuit diagram

3.3 Alarms, Reports and Trend Displays

Alarms and reports are main parts of the SCADA system functions [36]. The control system generates several alarms that are used to alarm the controller if the system interred in danger state and these alarms are archived in the SCADA system. These alarms are:

1. Pump faller (Pressure, EMT6 and NRV),
2. Soft starter faller (NZM),
3. Chlorine level switch,
4. Fuel level switch,
5. Generator fault.

Other data as the flow meter, pressure meter and soft starter RS485 data bus are also archived in the SCADA system and used for analyzing and developing the systems. Reports are one of the main functions and benefits of the SCADA system, recommended reports that may be generated for the system are:

1. Time of pumps operation.
2. Current of the motor pump.
3. Pressure level of the distribution line.
4. The flow rate of the water from the pump station.

3.4 Supervisory Control

Control system of the well station recommended divide the station control to remote and local. Remote control will be through the SCADA system using the PLC instructions and soft programs. Local control will be two parts, local automatic using preset clock timer and local manual control using the operator. Local control will be monitored through the SCADA system using the PLC input signals. Remote control using the SCADA will help in blocking and deblocking pumps and generators remotely in addition in monitoring and archiving the system processes.

Chapter 4

Communication System

In this chapter we will illustrate components and the technologies of the communication systems available with the SCADA. Communication system depends on port type, media and technology. These depend on equipments used in the SCADA system. PLCs/RTUs, servers and workstations are the main equipments of the SCADA and the aim is to connect and communicate these devices with each others.

4.1. Networking Standards

RS232, RS485, and Ethernet are the main network standards in PLCs and industrial devices. In this section we will illustrate specifications, advantages and disadvantages for these ports.

4.1.1 RS232

RS232 is a network technology that supports asynchronous, full-duplex data exchange between exactly two peers. RS232 supports for speeds of up to 20 Kbps with a maximum cable length of 15 m. An RS232 bus uses a minimum of two pins where software handshaking is used, with additional pins for hardware handshaking.

RS232 connects two transmitter/receiver pairs, the Data Communication Equipment (DCE) and the Data Terminal Equipment (DTE) [37]. For a two-wire configuration, each device has a transmit data (TxD) and a receive data (RxD) line; the TxD from one device connects to the RxD of the other device and vice versa Figure (4.1). For hardware handshaking, two lines (request-to-send (RTS), and clear-to-send (CTS)) are added. Data transmission begins with a start bit, followed by the data bits, a parity bit and a number of stop bits. Where hardware handshaking is used for flow control then, prior to transmission, the DTE sends the RTS line low and waits for an acknowledgement to be signaled over CTS.

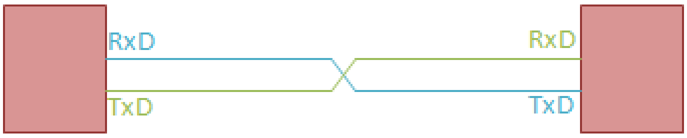


Figure (4.1): The two-wire RS-232 configuration

Whilst RS-232 is a peer technology with advantages for point-to-point communication, its support for only very limited topologies makes it inappropriate for scenarios in which numerous devices must all engage in communication with each other.

4.1.2 RS485 Port

RS485 (Recommended Standard 485), also known as TIA/EIA-485-A, is a standard maintained by the Electronics Industry Alliance (EIA). The RS485 standard was developed to meet the needs of electronic component designers for longer cable lengths, increased throughput and control of multiple devices.

One of the main problems with RS232 is the lack of immunity for noise on the signal lines. The transmitter and receiver compare the voltages of the data- and handshake lines with one common zero line. Shifts in the ground level can have disastrous effects. Therefore the trigger level of the RS232 interface is set relatively high at ±3 Volt. Noise is easily picked up and limits both the maximum distance and communication speed. With RS485 on the contrary there is no such thing as a common zero as a signal reference. Several volts difference in the ground level of the RS485 transmitter and receiver does not cause any problems. The RS485 signals are floating and each signal is transmitted over a Sig+ line and a Sig- line. The RS485 receiver compares the voltage difference between both lines, instead of the absolute voltage level on a signal line. This works well and prevents the existence of ground loops, a common source of communication problems. The best results are achieved if the Sig+ and Sig- lines are twisted as shown in Figure (4.2) [38].

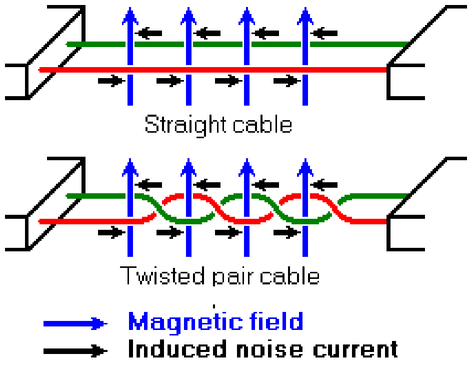


Figure (4.2): Noise in straight and twisted pair cables

The noise is generated by magnetic fields from the environment. The figure shows the magnetic field lines and the noise current in the RS485 data lines that is the result of that magnetic field. In the straight cable, all noise current is flowing in the same direction, practically generating a looping current just like in an ordinary transformer. When the cable is twisted, we see that in some parts of the signal lines the direction of the noise current is the opposite from the current in other parts of the cable. Because of this, the resulting noise current is many factors lower than with an ordinary straight cable. Shielding—which is a common method to prevent noise in RS232 lines—tries to keep hostile magnetic fields away from the signal lines. Twisted pairs in RS485 communication however adds immunity which is a much better way to fight noise. The magnetic fields are allowed to pass, but do no harm. If high noise immunity is needed, often a combination of twisting and shielding is used as for example in STP, shielded twisted pair and FTP, foiled twisted pair networking cables. Differential signals and twisting allows RS485 to communicate over much longer communication distances than achievable with RS232. With RS485 communication distances of 1200 m are possible [38].

Differential signal lines also allow higher bit rates than possible with non-differential connections. Therefore RS485 can overcome the practical communication speed limit of RS232. Currently RS485 drivers are produced that can achieve a bit rate of 35 mbps.

Characteristics of RS485 compared to RS232, RS422 and RS423: Table (4.1) illustrates that: First of all we see that the speed of the differential interfaces RS422 and RS485 is far superior to the single ended versions RS232 and RS423. We also see that there is a maximum slew rate defined for both RS232 and RS423. This has been done to avoid reflections of signals. The maximum slew rate also limits the maximum communication speed on the line. For both other interfaces RS422 and RS485 the slew rate is indefinite. To avoid reflections on longer cables it is necessary to use appropriate termination resistors [38].

Table (4.1): Characteristics of RS232, RS422, RS423 and RS485

	RS232	RS423	RS422	RS485
Differential	No	no	Yes	yes
Max number of drivers Max number of receivers	1 1	1 10	1 10	32 32
Modes of operation	half duplex full duplex	half duplex	half duplex	half duplex
Network topology	point-to-point	multidrop	multidrop	multipoint
Max distance (acc. Standard)	15 m	1200 m	1200 m	1200 m
Max speed at 12 m Max speed at 1200 m	20 kbs (1 kbs)	100 kbs 1 kbs	10 Mbs 100 kbs	35 Mbs 100 kbs
Max slew rate	30 V/µs	adjustable	n/a	n/a
Receiver input resistance	3..7 kΩ	≧ 4 kΩ	≧ 4 kΩ	≧ 12 kΩ
Driver load impedance	3..7 kΩ	≧ 450 Ω	100 Ω	54 Ω
Receiver input sensitivity	±3 V	±200 mV	±200 mV	±200 mV
Receiver input range	±15 V	±12 V	±10 V	–7..12 V
Max driver output voltage	±25 V	±6 V	±6 V	–7..12 V
Min driver output voltage (with load)	±5 V	±3.6 V	±2.0 V	±1.5 V

We also see that the maximum allowed voltage levels for all interfaces are in the same range, but that the signal level is lower for the faster interfaces. Because of this RS485 and the others can be used in situations with a severe ground level shift of several volts, where at the same time high bit rates are possible because the transition between logical 0 and logical 1 is only a few hundred millivolts.

Interesting is, that RS232 is the only interface capable of full duplex communication. This is, because on the other interfaces the communication channel is shared by multiple receivers and—in the case of RS485—by multiple senders. RS232 has a separate communication line for transmitting and receiving which—with a well written protocol—allows higher effective data rates at the same bit rate than the other interfaces. The request and acknowledge data needed in most protocols does not consume bandwidth on the primary data channel of RS232.

Network Topology with RS485: Network topology is probably the reason why RS485 is now the favorite of the four mentioned interfaces in data acquisition and control applications. RS485 is the only of the interfaces capable of internetworking multiple transmitters and receivers in the same network. When using the default RS485 receivers with an input resistance of 12 kΩ it is possible to connect 32 devices to the network. Currently available high-resistance RS485 inputs allow this number to be expanded to 256. RS485 repeaters are also available which make it possible to increase the number of nodes to several thousands, spanning multiple kilometers. And that with an interface which does not require intelligent network hardware: the implementation on the software side is not much more difficult than with RS232. It is the reason why RS485 is so popular with computers, PLCs, micro controllers and intelligent sensors in scientific and technical applications.

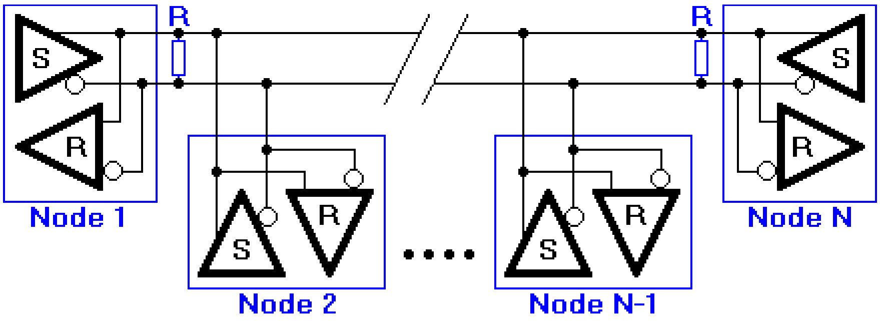


Figure (4.3): RS485 network topology

Figure (4.3) [38] shows the general network topology of RS485. N nodes are connected in a multipoint RS485 network. For higher speeds and longer lines, the termination resistances are necessary on both ends of the line to eliminate reflections. Use 100 Ω resistors on both ends. The RS485 network must be designed as one line with multiple drops, not as a star. Although total cable length maybe shorter in a star configuration, adequate termination is not possible anymore and signal quality may degrade significantly.

RS485 Functionality: All the senders on the RS485 bus are in tri-state with high impedance. In higher level protocols, one of the nodes is defined as a master who sends queries or commands over the RS485 bus [38]. All other nodes receive these data. Depending of the information in the sent data, zero or more nodes on the line respond to the master. In this situation, bandwidth can be used for almost 100%. There are other implementations of RS485 networks where every node can start a data session on its own. This is comparable with the way Ethernet networks function. Because there is a chance of data collision with this implementation, theory tells us that in this case only 37% of the bandwidth will be effectively used. With such an implementation of a RS485 network it is necessary that there is error detection implemented in the higher level protocol to detect the data corruption and resend the information at a later time.

There is no need for the senders to explicity turn the RS485 driver on or off. RS485 drivers automatically return to their high impedance tri-state within a few microseconds after the data has been sent. Therefore it is not needed to have delays between the data packets on the RS485 bus.

RS485 is used as the electrical layer for many well known interface standards, including Profibus and Modbus. Therefore RS485 will be in use for many years in the future.

4.1.3 Ethernet

Today Ethernet is the predominant and most widely and popular networking technology specified in standard IEEE802.3 and used in office and home environments. An Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires. Ethernet is also used in wireless LANs. The most commonly installed Ethernet systems are called 10BASE-T and provide transmission speeds up to 10 Mbps to nearly 120 m distance. Devices are connected to the cable and compete for access using a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol [39].

Fast Ethernet or 100BASE-T provides transmission speeds up to 100 megabits per second and is typically used for LAN backbone systems, supporting workstations with 10BASE-T cards. Gigabit Ethernet provides an even higher level of backbone support at 1000 megabits per second (1 gigabit or 1 billion bits per second). 10-Gigabit Ethernet provides up to 10 billion bits per second.

Since Ethernet networks are inexpensive and fairly well understood, they have quickly becoming popular in industrial and utility data communication networks, despite the fact that they were not originally developed to operate in hostile environments.

Ethernet infrastructure is usually available, or can be easily implemented. Buildings tend to have existing Ethernet networks. PLC and RTU manufacturers are starting to develop Ethernet add-ons to network their products, at a premium cost for this functionality. Both industrial and utility networking experts are moving forward accepting the limitations of Ethernet networks and solving the problems associated with its application. Now days, new Ethernet equipment has becoming available designed to operate reliably under extreme harsh environment typically found in utility applications for SCADA, substation and distribution automation.

4.1.4 Universal Serial Bus (USB)

A USB port is a standard cable connection interface on personal computers and consumer electronics. USB ports allow stand-alone electronic devices to be connected via cables to a computer (or to each other).

More recent computers have USB ports instead of serial ports. This converter will plug into your USB port and provide a COM port for the PC. Use with a USB hub to get multiple COM ports.

4.2 Converters

Converters are good tools used to convert network connection type especially for serial port devices. New computers and servers may have not any serial port, although, they may have several USB ports and the USB port may be connected to HUB USB to expand the USB port to other USB ports. Serial ports (RS232, RS422, RS485) are mainly used with industrial devices. So USB/Serial converters are important in implementing industrial networks. When the serial device connects to the computer through USB port, it gets specific virtual COM port number. This COM port is the device software address used by the operating system to communicate with.

4.2.1 RS232/USB Converter

This converter used to convert the serial port to USB port. So it can be used to connect any serial RS232 device to the computer directly. In our application it may be used to connect pool of external modems (dialup, GSM or Radio) with the computer through the computer USB port. Figure (4.4) illustrates one of these industrial USB/RS232 devices.

Figure (4.4): RS232/USB Converter

4.2.2 USB/RS485 Converter

This device used to connect RS485 devices to the computer through USB port. RS485 is a serial port setting that is most commonly used in industrial machines and devices especially PLCs. Also several RS485 devices can be connected through RS485 bus. So USB/RS485 converter used to connect the RS485 bus to the computer through the computer USB port. The computer communicates with the USB/RS485 converter through its virtual COM port number then the converter communicates with the RS485 device through its address.

There are many industrial USB/RS485 converters can be used. VFD-USB01 USB/RS485 [40] Communication Interface from Delta Company can be used in the industrial network of the communication control system.

Figure (4.5): RS485/USB Converter

4.3 Deploying SCADA System

Designing the communication network of the SCADA system is one of the main parts of our research. That will specify the way of connecting the water well stations with the main control room. There are several scenarios that depend on communication technology exist in Gaza strip [26]. It includes direct connection through (RS232, RS485 and Ethernet), dial up connection using Public Switching Telephone Network (PSTN), Global System for Mobile (GSM) cellular system, and wireless LAN. Every connection has advantages and disadvantages. We can use mix of these techniques to reach to the optimum connection.

There are many different ways in which SCADA systems can be implemented. Before a SCADA or any other system is rolled out, you need to determine what function the system will perform. Depending on whether you are a utility company or a telecommunications provider, you have a number of options in creating your systems. There may be a need to employ different methods that are complimentary to each other. The way in which SCADA systems are connected can range from fiber optic cable to the use of satellite systems. The following sections will present some of the common ways in which SCADA systems are deployed.

4.3.1 Direct Connection

Direct connection usually uses RS232, RS485 or Ethernet port to connect a process controller (PLC) with SCADA servers. This technology uses twisted pair media wires. This is the cheapest and most preferable connection method. But this is suitable for small distances that are less than 20 m for RS232, less than 100 m for Ethernet and less than 1200 m for RS485. So this connection is used when the well station near the main control room as shown in plants 3, 4 and 5 in Figure (2.11); or when there are several well stations near each other and connected with master PLC controller as the case of plants 8 and 9 in the same figure.

Fiber Optic: Fiber optic technology [7, 39] has improved considerably since its inception in 1970. The technology has improved to the point where commercially available fibers have losses less than 0.3 dB/km. Losses of this magnitude, as well as the development of suitable lasers and optical detectors, allow designers to consider fiber optic technologies for systems of 140 km or more without repeaters.

Optical fibers consist of an inner core and cladding of silica glass and a plastic jacket that physically protects the fiber. Two types of fibers are usually considered: multi-mode graded index and single-mode step index fiber. Single-mode fiber supports higher signaling speeds than the multi-mode fiber due to its smaller diameter and mode of light propagation. Communication services usually supported by optical fiber include voice, data (low speed), SCADA, protective relaying, telemetering, video conferencing, high speed data, and telephone switched tie trunks. Optical fiber cables have similar characteristics to twisted-pair communications cables in that aluminum tape or steel-wire armors and polyethylene outer jackets can protect them. However, the inner core is constructed to accommodate the mechanical characteristics of the fibers. Typically, the fibers are placed loosely in semi-rigid tubes, which take the mechanical stress. Special types of fiber optic cables have been developed for the power industry. One type of fiber cable is the Optical Power Ground Wire (OPGW) that is an optical fiber core within the ground or shield wire suspended above transmission lines. Another type of optical fiber cable is the All-Dielectric Self-Supporting (ADSS) cable that is a long-span of all dielectric cables designed to be fastened to high voltage transmission line towers underneath the power conductors. A Wrapped Optical Cable (WOC) is also available that is usually wrapped around the phase conductor or existing ground/earth wire of the transmission or distribution line. In the Utility’s case, aerial fiber optic cable can be fastened to the distribution poles under the power lines.

Single mode fiber optic cables is now less than multimode fiber optic cable because of the increasing demand for single mode fiber. Conversely, the multimode fiber optic has limited distance and bandwidth characteristics. The fiber optic terminal equipment is simpler and generally less expensive than microwave equipment. Optical transmitters can be either light emitting diodes (LEDs) or laser diodes. They operate at 850, 1310, or 1550 nm wavelengths, depending on the application. Many optical terminals have been developed for the telephone industry for large numbers of channels. There are now a number of products specifically designed for power utilities. These are low capacity terminals that feature surge withstand capabilities and special channel units for tele-protection signaling. Parameters that influence the choice of the type of optical cable to be used are:

- Overhead cable can be OPGW, ADSS, or WOC

- Underground cable can be duct cable (light, medium, or heavy duty), ADSS for use in a duct, or direct burial cable with armor jacket

4.3.2 Dialup Connection

Connecting far process controller (PLC) with the SCADA servers using PSTN [7] needs external dial up modem with serial port at each well station. At the other side, at the main control room, the SCADA server connects to the PSTN through dial up modem as illustrated in the case of planet 1 in Figure (2.11). This scenario implies a relatively low cost running cost that composed of the monthly fixed charges and the dial up calls. There is no online data connections, data will be collected several times through the station work period, and collecting data through dialup takes a time, as every call need 1 minute. On line connection will be expensive. Also, getting data at urgent actions will take time until dialing the modem and connecting to PLC. Well stations that have already dialed up phone line can use this scenario for connecting with the main control room.

4.3.3 Cellular Phone System

Connecting the PLC with the SCADA server through the cellular phone system need GSM modem with serial port at each well station to connect to at the process controller PLC with the RS232 serial port. At the other site, pool of GSM or dial up modem used to connect the control system with the cellular system as shown in plant 2 of Figure (2.11). Gaza cellular phone system, JAWWAL, has good service that is called GPRS; this service is used for internet connection. The user is assigned an IP number which allows him to connect online with internet. Charging depends on the size of download packets not on the calling time. When using this service the PLC is connected online with the SCADA server. The problem of this service is assigning dynamic IPs to clients. This forces us to program the PLC to send data to the SCADA server but this is not a professional solution. On the other hand, requesting static IPs is much expensive.

One promising advantage of cellular phone system is the availability of using RTUs from SOLCON Company. Resent well stations soft starters are from SOLCON so, using SOLCON RTUs reduces the required upgrade equipments and cost.

Cost of using cellular phone system is more expensive than PSTN although there are no monthly fixed charges. Calling charges of cellular system are more expensive. It is good to benefit from the prepaid system by using it at well stations modem and use it for alarms and emergency cases only. At main control room, it is recommended to buy a big package of calling to benefit from the discount on big packages. Cellular system used in stations that has good GSM signals. Cellular system has some problems in calling as network busy, lack of the signal in some locations and change of the signal strength.

4.3.4 Wireless Private Network

Since the invention of the Wireless Telegraph in 1896 communication system is, by any measure, the fastest growing segment of the communications industry. As such, it has captured the attention of the media and the imagination of the public. Wireless local area networks currently supplement or replace wired networks in many homes, businesses, and campuses. Many new applications – including wireless sensor networks, automated hiways and factories, smart homes and appliances, and remote telemedicine- are emerging from research ideas to concrete systems. The explosive growth of wireless systems coupled with the proliferation of laptop and palmtop computers suggests a bright future for wireless networks, both as stand-alone systems and as part of the larger networking infrastructure. However, many technical challenges remain in designing robust wireless networks that deliver the performance necessary to support emerging applications. Designers have sought to use wireless because of the reduced infrastructure cost and complexity, when compared to wire line communication systems. There is no need to construct miles of line poles or cable trenches. Simply put in a few strategically positioned radio towers and transmit around the world. Today, wireless systems are significantly more complex because we want to allow millions of users receive feature length movies via wireless systems. There are four general types of wireless (radio) communication systems:

- Cellular Telephone
- Basic 2-Way Radio
- Microwave
- Wi-Fi (Wireless Fidelity), and Wi-Max

These systems depend on frequency band that has ranges from 3MHz to 300GHz. each rang of frequency band has its special use that depends on the transmission distance, the data transmission and the system cost. Table (4.2) illustrates the designations and the nomenclature of the International Telecommunication Union (ITU) frequency bands [41].

Table (4.2): ITU Frequency Band Nomenclature

ITU Band	Designation	Frequency	Wavelength
1	Extremely Low Frequency (ELF)	3 - 30 Hz	100,000 km - 10,000 km
2	Super Low Frequency (SLF)	30 - 300 Hz	10,000 km - 1000 km
3	Ultra Low Frequency (ULF)	300 - 3000 Hz	1000 km - 100 km
4	Very Low Frequency (VLF)	3 - 30 kHz	100 km - 10 km
5	Low Frequency (LF)	30 - 300 kHz	10 km - 1 km
6	Medium Frequency (MF)	300 - 3000 kHz	1 km - 100 m
7	High Frequency (HF)	3 - 30 MHz	100 m - 10 m
8	Very High Frequency (VHF)	30 - 300 MHz	10 m - 1 m
9	Ultra High frequency (UHF)	300 - 3000 MHz	1 m - 10 cm
10	Super High Frequency (SHF)	3 - 30 GHz	10 cm - 1 cm
11	Extremely High Frequency (EHF)	30 - 300 GHz	1 cm - 1 mm

4.3.4.1 Microwave Technology

Microwave communication is the transmission of signals of frequencies (300 MHz – 300 GHz) [7] for distances of tens of kilometers with relatively huge power requirement. This transmission is via radio using parabolic dishes mounted on a series of towers or on top of buildings. Microwave communication is known as a form of “line of sight” communication, because there must be nothing obstructing the transmission of data between these towers for signals to be properly sent and received. Microwave communication one of the most commonly used data transmission method for telecommunications service providers and takes place both analog and digital formats.

Digital microwave communication utilizes more advanced, more reliable technology. It is much easier to find equipment to support this transmission method because it is the newer form of microwave communication. Because it has a higher bandwidth, it also allows transition more data using more verbose protocols. The increased speeds will also decrease the time it takes to poll microwave site equipment.

Microwave can be used as communication system for SCADA or other monitoring systems. But SCADA data needed to be transmit is relatively small and distances between stations is also relatively small not exceed on 5Km. So using microwave communication system able to transmit huge of data for tens of kilometers for our SCADA system is not acceptable. So SCADA systems and most environmental monitoring data communications requirements can be addressed through other more cost effective and equally robust wireless solutions.

4.3.4.2 Wi-Fi Technology

Wi-Fi Systems is a term that is applied to a generic point-to-multipoint data communication service. The Federal Communications Commission (FCC) has set aside radio spectrum in the 900 MHz, 2GHz and 5 GHz frequency range [7, 39 and 42]. The frequencies are available for use by the general population and commercial enterprise. No licenses are required, and the only restrictions are that systems not exceed power or antenna height requirements. Complete rules governing the use of Wi-Fi systems are listed under FCC rules, the Commission established new general emission limits in order to create more flexible opportunities for the development of new unlicensed. Wi-Fi systems are Ethernet based and allow for a seamless transition from wireless to wire line. So this technology is suitable and applicable with SCADA systems. Wi-Fi standard outdoor distance transmission is small reaches to 100 m only. There are several industrial wireless systems that use Wi-Fi transmission technology. These systems have outdoor access point units connect with directional antennas of 12-20 dBi. This enables these systems to transmit data for large distances reaches to 10-20 kilometers as the device catalog. From these systems:

1- MOXA AWK-6222- EU-T with antenna MOXA ANT-WSBPNF-12 [43].

2- 3Com 54 Mbps Wireless LAN Building to-Building Bridge and Access Point [44].

Another problem with Wi-Fi technology is its transmission on free license frequency band 2.4GHz. All local internet wireless devices use this free license. So this may make overlap and interference between the SCADA system data and the local wireless internet systems.

4.3.4.3 Wi-Max Technology

Based on the IEEE 802.16 series of standards, Wi-MAX is a wide area wireless system with a coverage area stated in terms of miles rather than feet [7]. The standard was developed to provide for fixed point-to-multipoint coverage with broadband capabilities. For the latest information on the evolving 802.16 standards “802.16 is a group of broadband wireless communications standards for Metropolitan Area Networks (MANs) developed by a working group of the IEEE. The original 802.16 Standard, published in December 2001, specified fixed point-to-multipoint broadband wireless systems operating in the 10-66 GHz licensed spectrum [45]. An amendment, 802.16a, approved in January 2003, specified non-line-of–sight extensions in the 2-11GHz spectrum, delivering up to 70 Mbps at distances up to 31 miles. Officially called the Wireless MAN specification, 802.16 standards are expected to enable multimedia applications with wireless connection and, with a range of up to 40 Kilometers [39].

Wi-MAX systems are Ethernet based and allow for a seamless transition from wireless to wire line as Wi-Fi systems. This is suitable and applicable with SCADA systems. There are several industrial systems uses Wi-MAX technology. One of these systems is BreezeNET®B from ALVARION Company. This product used in local market.

4.3.4.4 VHF/UHF Technology

Environmental monitoring data are typically transmitted in packets through radio signals using VHF and UHF frequencies [7]. VHF/UHF transmission ranges from 30MHz to 3000MHz through special antennas (good for up to 40Km). A license from the ministry of telecommunications must be obtained and coverage is limited to special geographical boundaries. Commonly used VHF/UHF frequencies in radio modems for environmental monitoring or SCADA includes frequencies of the range from 66MHz to 960 MHz. These ranges locate in the ISM (Industrial Scientific and Medical) band frequencies that are unlicensed [45].

Also, there are many companies manufacture industrial devices compatible with SCADA system and use UHF/VHF technology, samples of these systems are listed below and illustrated in Figure (4.6):

1. TS4000 Radio modem from TELEDESIGN SYSTEM Company.

2. SATELLAR system [46], which is wireless communication system in unlicensed frequency range 380-520 MHz, and has point to point link communication range reach to 10 KM in urban area.

Figure (4.6): UHF/VHF Systems

4.4 Communication Cost

Table (4.3) illustrates the cost of the previous communication scenarios. We calculate the price of the hardware devices with its installation and the running cost for 5 years. For dialing systems we make our cost on making 10 calls per a day, with calling charges of 2cents for dialing and 20 cent for cellular.

Table (4.3): Communication scenarios cost for first 5 years

#	Communication Method	Method parts	Setup Cost		Running Cost /Year	Total cost for first 5 years
			Remote Unit Cost	Central Unit Cost		
1	Direct Connection	-	0	0	0	0
2	Dial Up Connection (PSTN)	Modem	70*31 =2170$	70*4=280$	10 calls per day 2 Cent per call 10*30*12*.02*31= 2232$ Fixed charges: 5$ 5*12*35= 2100$	26210$
		Phone Line	60 *31= 1860$	60*4=240$		
3	Cellular phone System (GSM)	Modem	300*31= 9300$	300*4= 1200$	10 calls per day 20 Cent per Call 10*30*12*0.20*31 = 22320$	123150$
		Phone Line	2*31= 62$	30*4= 120$		
4	Radio wireless connection	-	3000*31= 93000	5000*2= 10000	0	103000$
5	RTU (SOLCON)	Unit price	3500*31= 108500	1200$	10 calls per day 6 Cent per Call 10*30*12*0.06*35 = 7560$	147562$
		Phone Line	2*31= 62$	0		

Chapter 5

System Design

In this chapter we will design the SCADA system. This will include the communication system that is considered the main scope of our research. Main control room equipments, software needed and operator display structure.

5.1 Communication System Topology

According to the previous description of communication systems, and according to the well water stations distribution in Gaza, we recommend to design the network communication system using RS485 bus, wireless communication and dialup as a feedback system as illustrated below:

5.1.1 Connection Using RS485 Bus

We recommend using this connection for stations that have a distance less than 1200 m between each other and have low cost infrastructure implementation to expand RS485 cable underground. Also, stations in the same location will be connected using RS485. Stations which are recommended to be connected with RS485 are listed below:

1. Sh. Radwan wells 1 and 1A. Figure (5.1) shows the location of the wells. It is illustrated they are in the same location.

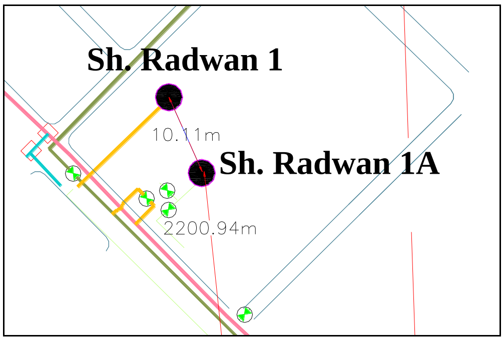


Figure (5.1): Sh. Radwan wells 1and 1A location

2. Sh. Radwan wells 7 and 7A. Figure (5.2) shows the location of the wells. It is illustrated they are in the same location.

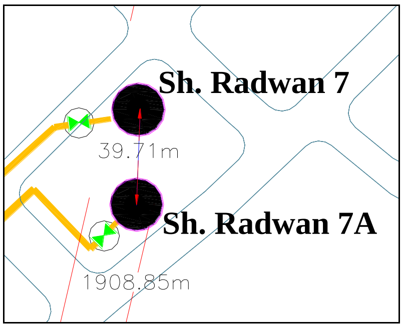


Figure (5.2): Sh. Radwan wells 7 and 7A location

3. Well stations Sh. Radwan wells 12, 15 and 16. The central PLC connection will be at Sh. Radwan well 15. Figure (5.3) shows the location of the wells. It is illustrated they are near to each other and can be connected with cables underground or up ground.
4. Well stations Sh. Radwan wells 10 and 11. The central PLC connection will be at Sh. Radwan well 10. The wells location is shown in Figure (5.3). It is illustrated they can be connected with cables underground or up ground.

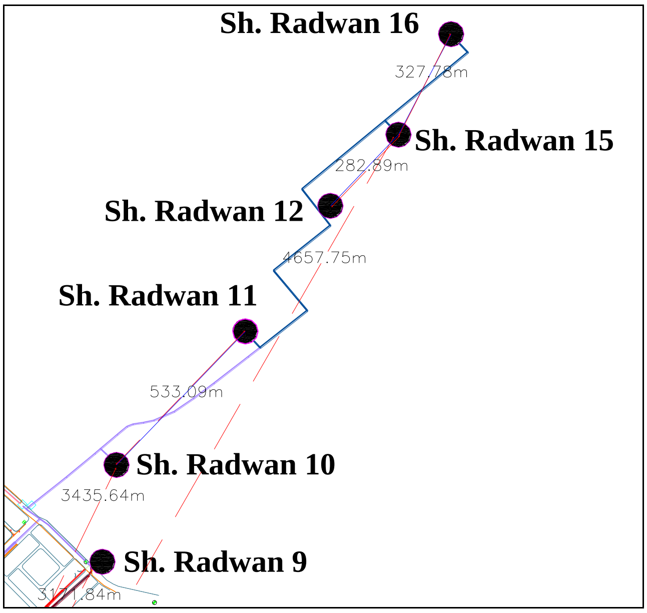


Figure (5.3): Sh. Radwan wells 10, 11. 12, 15 and 16 locations

5. SAFA-wells 1, 2, 3 and 4. Figure (5.4) illustrates SAFA wells are in the same location.

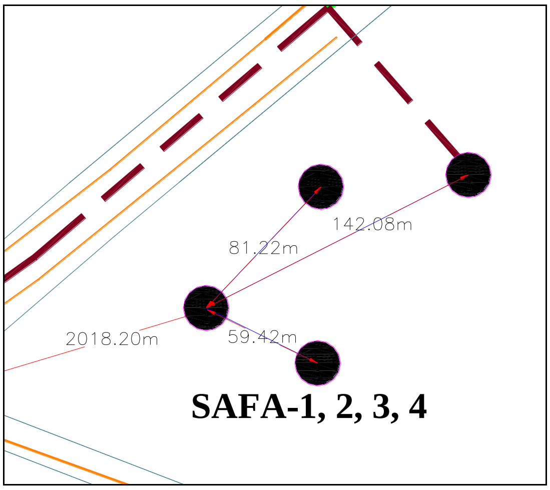


Figure (5.4): SAFA wells locations

6. Zaitoun wells 1 and 2. Figure (5.5) illustrates the wells are in near location and can be connected to other by underground cables.

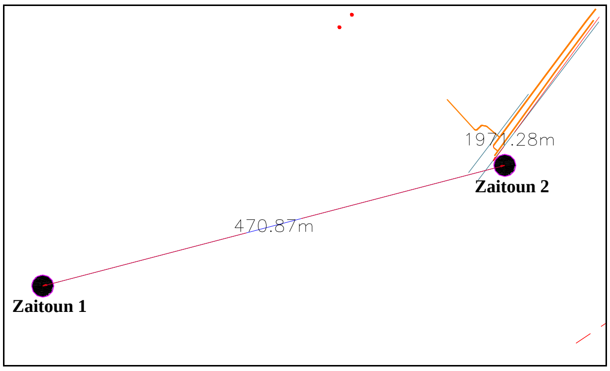


Figure (5.5): Zaitoun wells location

5.1.2 Connection Using Private Radio Channels (WIRELESS)

It is recommended to use wireless radio signals to connect far stations with the main control room. Table (5.1) and Figure (5.6) summarize the line-of-site distance between the proposed main control room and remote locations. It is remarkable that this distance is less than 5Km for all remote locations.

Table (5.1): Gaza well pumping stations groups and distance to main control room

No.	ID	Well Name	Distance to MCR	No.	ID	Well Name	Distance to MCR
1	WG1	Safa well 1	2026	12	WS6	Sh. Radwan 2	2667
		Safa well 2		13	WS7	Sh. Radwan 3	2568
		Safa well 3		14	WS8	Sh. Radwan 4	2753
		Safa well 4		15	WS9	Sh. Radwan 5	3111
2	WG2	Sh. Radwan 1	2176	16	WS10	Sh. Radwan 8	3262
		Sh. Radwan 1A		17	WS11	Sh. Radwan 9	3171
3	WG3	Sh. Radwan 7	1908	18	WS12	Sh. Radwan 13	2137
		Sh. Radwan 7A		19	WS13	Remal 1 Aljundi	1688
4	WG4	Sh. Radwan 10	3435	20	WS14	Remal 2 kamal naser	2581
		Sh. Radwan 11		21	WS15	AL Daraj - AlBasha	550
5	WG5	Sh. Radwan 12	4657	22	WS16	Sh. Ejleen 1	2791
		Sh. Radwan 15		23	WS17	Sh. Ejleen 2	2221
		Sh. Radwan 16		24	WS18	Sh. Ejleen 3	2949
6	WG6	Zaitoun 2	1971	25	WS19	Sh. Ejleen 4	2256
		Zaitoun 1		26	WS20	Sh. Ejleen 5	2496
7	WS1	Shijaiea 2	1811	27	WS21	Sh. Ejleen 6	3063
8	WS2	Shijaiea 3	1900	28	WS22	Sh. Ejleen 7	1965
9	WS3	Shijaiea 5	2135	29	WS23	Sabra 1 (Dogmosh)	1638
10	WS4	Almontar	2231	30	WS24	Sabra 2 (diery)	1170
11	WS5	Zimmo	3911	31	WS25	Sabra 3 (shehibr)	529

From the table and the figure we find all remote stations are at a distance of less than 5 km from the proposed main control room at the Gaza Municipality. If the signal is low at main control room far stations as Sh. radwan 16, we can install a repeater unit as shown in Figure (5.7). The repeater unit recommended to be installed at the high elevated water tank at Sh. Radwan well 1. Then make practical test to find this location covers the entire region specially zemmo well and Sh. Radwan 16. Other location for the repeater may be Sh. Radwan 7, this more near to Zemmo well and Sh. Radwan 16.

One of wireless systems suitable for this distance is SATELLAR system that is manufactured by from SATEL Company. SATELLAR system proposed to be the main connection between these stations (remote stations) and main control room. Some of important stations will have backup connection. Dialup connection is recommended to be used as a backup connection. Meanwhile, nearly all big and important well stations already have a dialup phone line.

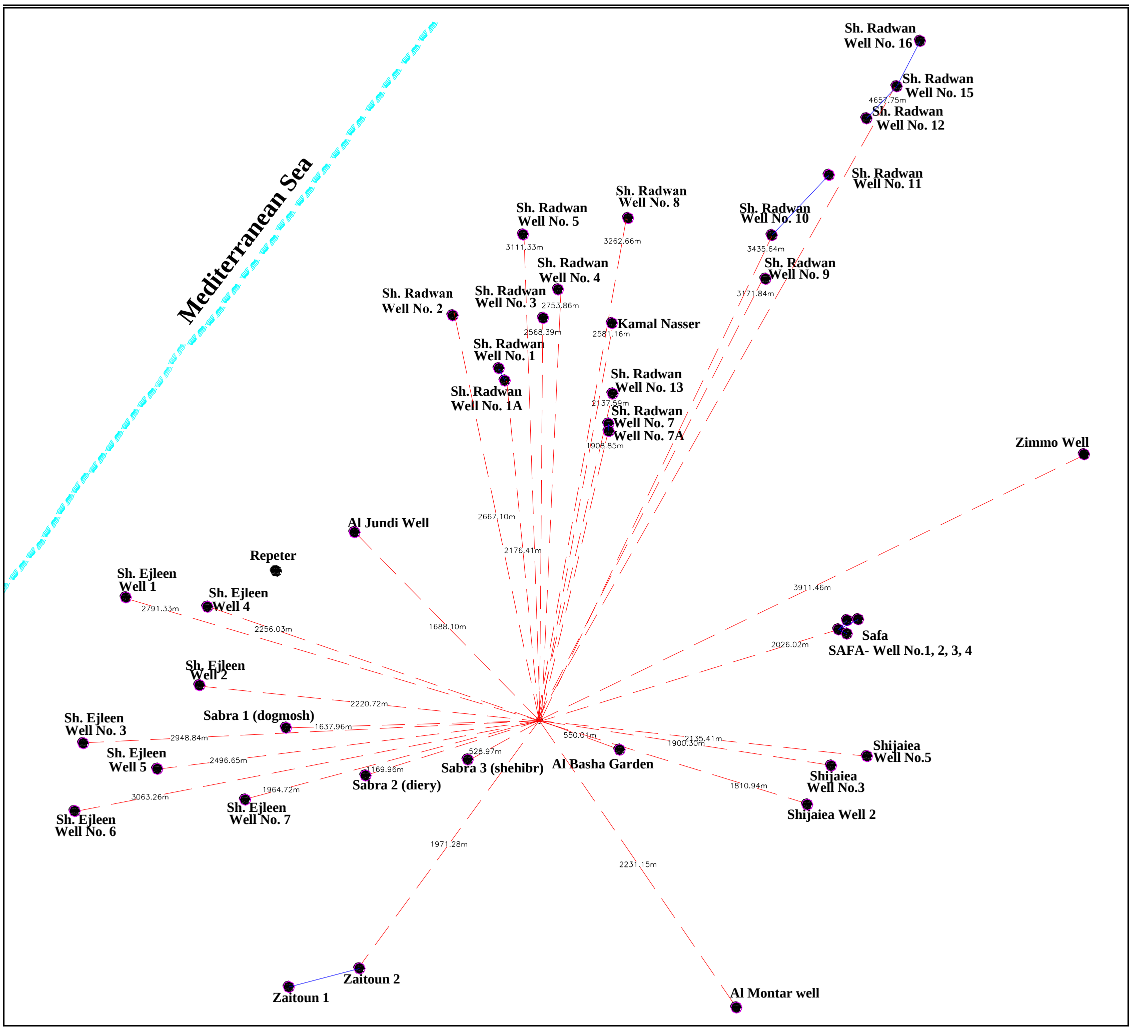


Figure (5.6): Gaza well stations distances from the main control room

SATELLAR is used as the wireless system in connecting remote stations with the main control room because it has several advantages compared with the other wireless systems listed before. Main advantages are:

1. **Rang:** SATELLAR radio communication range of a point-to- point link is typically over 10 km in urban conditions (some obstacles to line of sight) and over 20 km for ideal line of sight.
2. **Frequency:** SATELLAR work at frequency range of 380 - 520 MHz. This rang far away from free license ranges 2.4 GHz which is distributed by Wi-Fi- system. So this frequency range is low interference.
3. Each station can serve as a radio router to extend the radio coverage. Each station can serve either only one client or provide a wireless uplink to an entire IP network on a substation consisting of many units.

Any other wireless system has these main important advantage points can be used as wireless system to connect remote stations with the main control room.

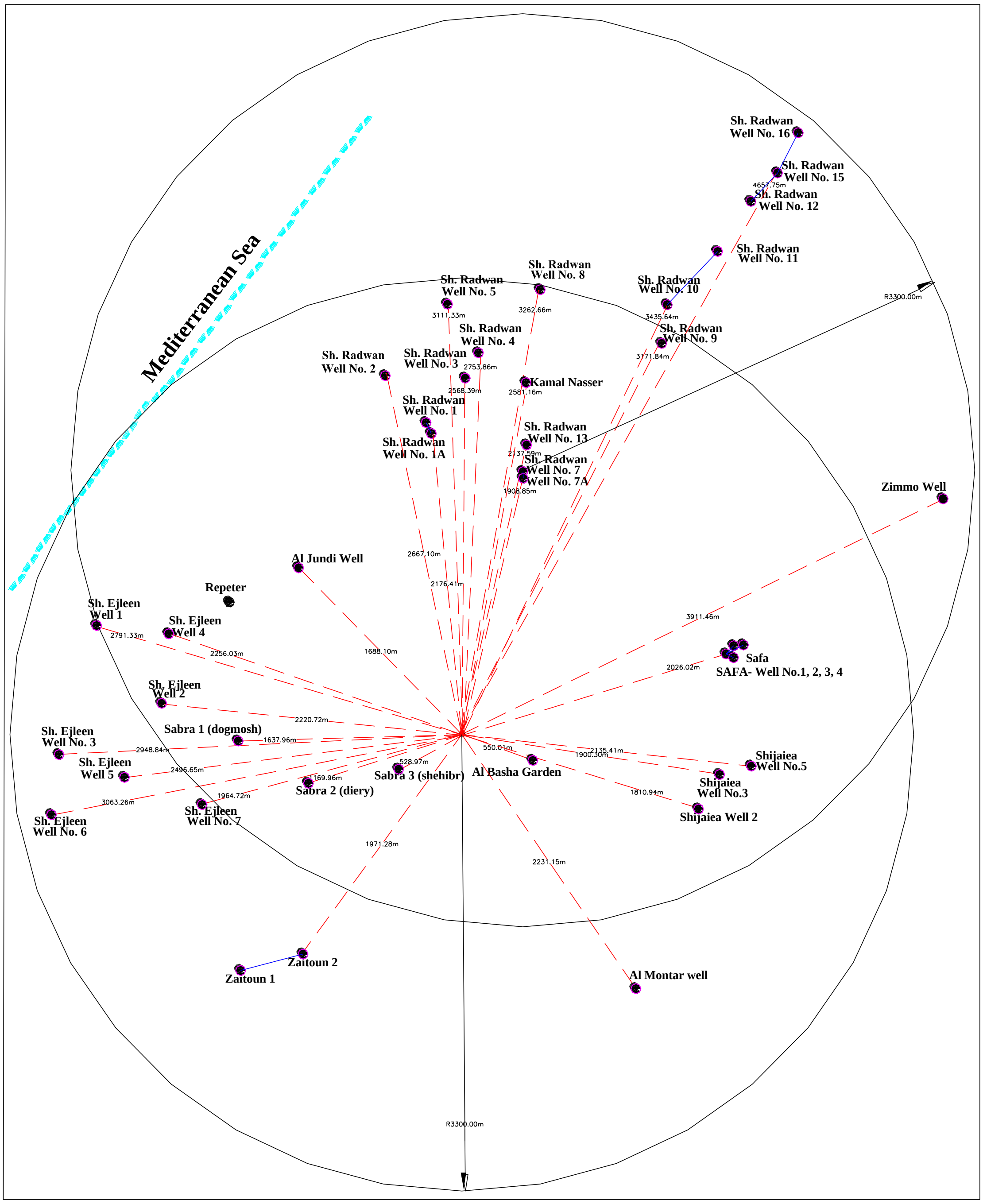


Figure (5.7): Regions covered by two wireless central units

5.2 Main Control Room

As mentioned before, main control room is proposed to be at the Gaza Municipality which located in the middle of the city and characterized by a high altitude. These features are preferable for the proposed wireless system.

At this room the computer system for the SCADA will be installed. This system consists of hardware and software.

5.2.1 Hardware Computer System

This includes all the hardware devices needed to implement the SCADA system that consists of:

1. SCADA server computer: this server needs to have very good specification. And will be used to install all the SCADA software packages that include software programs and tools.
2. Backup SCADA server, used as a backup of the main server and for redundancy.
3. Workstation: from 2 to 3 workstations for the supervisor and operators.
4. Laser printer.
5. Local Area Network: Ethernet LAN needed to connect the servers, printers and the client workstations with each others.

5.2.2 Software System

Software system will include all software packages needed to implement the SCADA system which are:

1. SCADA server package.
2. OPC server.
3. SQL Server.
4. HMI implementation program as Lookout from National Instruments (NI).

5.2.3 Operator Interface

HMI package is used to design the operator interface with SCADA system Lookout Program from National Instruments (NI) can be used. This display need to be simple structure, enable the operator to reach to his target fast and simply. It is recommended to build the system display on several levels with the ability to move from one level to other levels.

First level: Display all the wells “as in Figure (1.1).

Second level: Display Regions: Gaza can be divided to regions depending on the wells supply. Taking in coordination there is interference between the wells and regions they supply.

1. Sh. Radwan wells supply Sh Radwan and Remal
2. Remal wells supply Remal region.
3. Sh. Ijlleen wells supply Sh. Ejleen and Talelhwa region.
4. Sabra wells supply Sabra region.
5. Zimmo and SAFA wells supply Aldarj Region.
6. Shijaiea wells supply Shijaiea region.
7. Zaitoun wells supply zaitoun region.

Third level: Water well station with all its components and devices.

Fourth level: well station components status.

Chapter 6

Experimental Results

The experimental platform comprises four well plant modules which are equipped with Delta DVP28SV PLCs as shown in Figure (6.1). The SCADA server will communicate with these plants using different configurations to evaluate and demonstrate the communication scenarios described in chapter 4 . KEPServerEx [47] and OPC Quick client [23] (from Kepware product) is used to read and write PLC data.

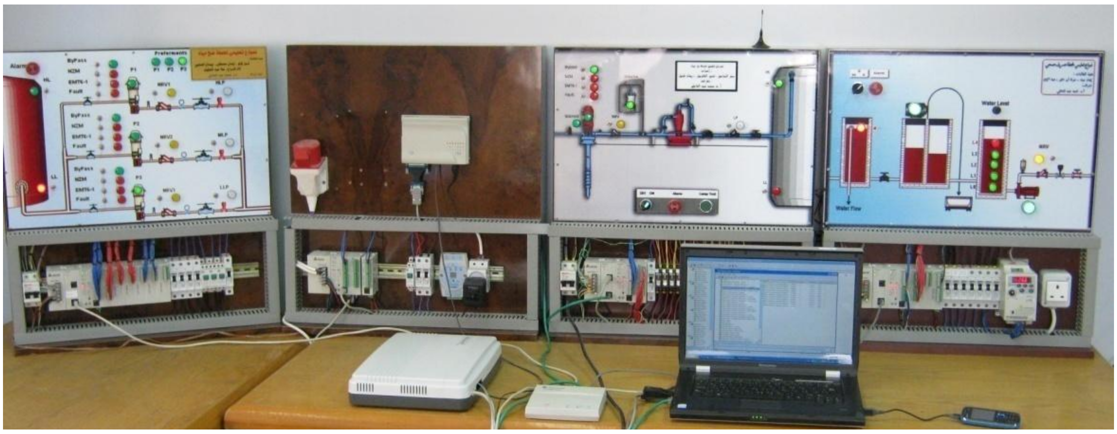


Figure (6.1): Four plants modules

6.1 Direct Connection Configuration

Direct connection experiment includes testing RS232, RS485 and Ethernet direct connection.

6.1.1 RS232 Connection

The simplest and cheapest way to connect the PLC with the computer is using the serial port RS232. But its maximum connection distance is limited to 15 m only. Therefore, this method is proper for connecting the PLC locally for programming and troubleshooting.

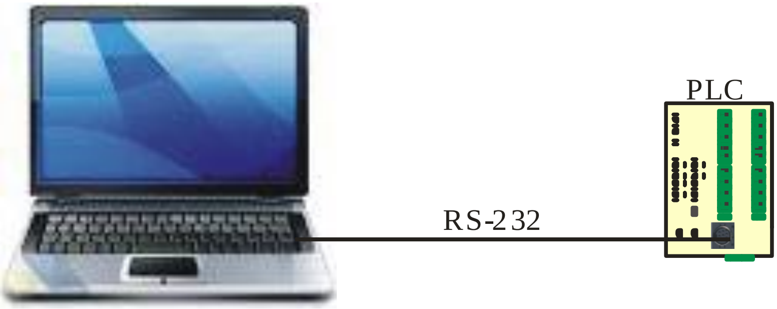
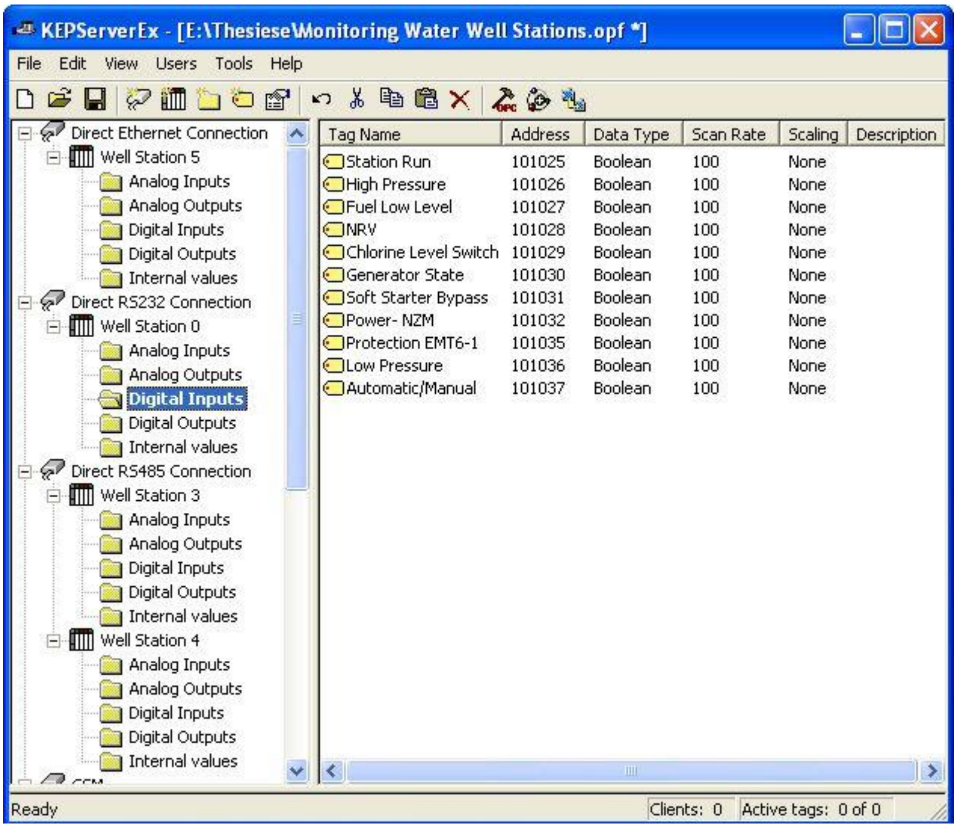


Figure (6.2): PLC RS232 connection

To demonstrate this method for a vertical turbine plant, its PLC is connected with the computer through RS232 port as illustrated in Figure (6.2). KEPServerEX OPC program is lunched and new project is started. In this project a new channel with “Modbus Ascii Serial” device driver and “9600, 7, e, n, 1” communication settings is created. A device with “Modbus Ascii” model is added to the channel. Finally, the system tags [48] are defined according to Table (3.1). The resulting OPC server interface is illustrated in Figure (6.3).


KEPServerEx - [E:\Thesiese\Monitoring Water Well Stations.opf *]
File
Edit
View
Users
Tools
Help

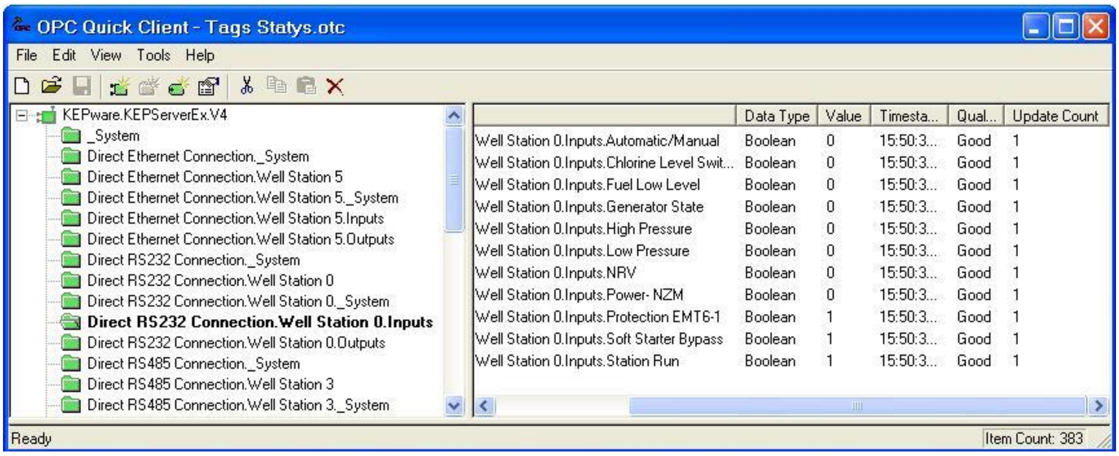
- Direct Ethernet Connection
  - Well Station 5
    - Analog Inputs
    - Analog Outputs
    - Digital Inputs
    - Digital Outputs
    - Internal values
- Direct RS232 Connection
  - Well Station 0
    - Analog Inputs
    - Analog Outputs
    - Digital Inputs
    - Digital Outputs
    - Internal values
- Direct RS485 Connection
  - Well Station 3
    - Analog Inputs
    - Analog Outputs
    - Digital Inputs
    - Digital Outputs
    - Internal values
  - Well Station 4
    - Analog Inputs
    - Analog Outputs
    - Digital Inputs
    - Digital Outputs
    - Internal values
- CCM

Tag Name	Address	Data Type	Scan Rate	Scaling	Description
Station Run	101025	Boolean	100	None	
High Pressure	101026	Boolean	100	None	
Fuel Low Level	101027	Boolean	100	None	
NRV	101028	Boolean	100	None	
Chlorine Level Switch	101029	Boolean	100	None	
Generator State	101030	Boolean	100	None	
Soft Starter Bypass	101031	Boolean	100	None	
Power- NZM	101032	Boolean	100	None	
Protection EMT6-1	101035	Boolean	100	None	
Low Pressure	101036	Boolean	100	None	
Automatic/Manual	101037	Boolean	100	None	

Ready | Clients: 0 | Active tags: 0 of 0

Figure (6.3): KEPseverEX tags view

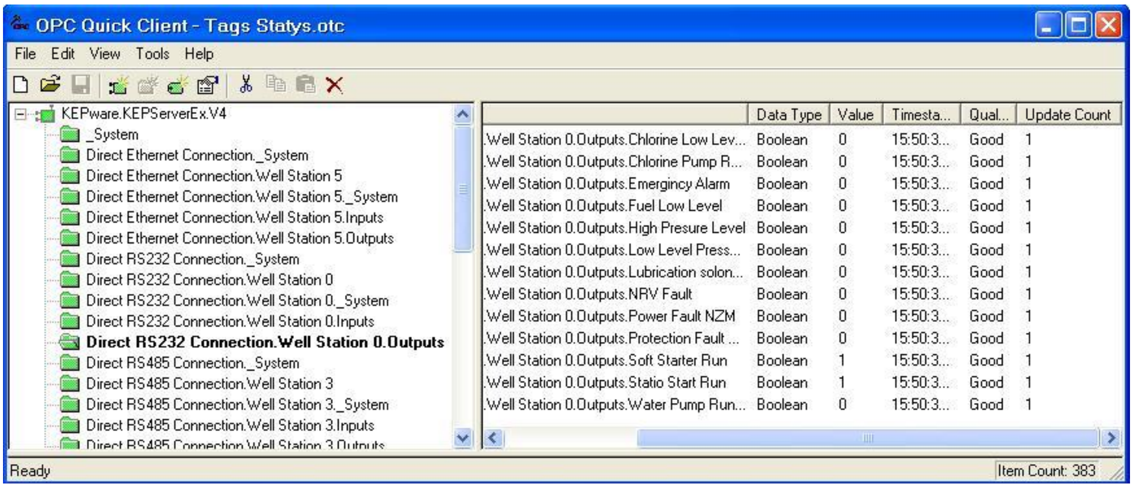
The OPC Quick Client tool from Kepware allows testing the OPC project easily. This tool establishes a connection with OPC server enabling monitoring the system tags on the fly as illustrated in Figure (6.4). In this experiment all system tags are updated and monitored rapidly as expected.



KEPware.KEPServerEx.V4
_System
Direct Ethernet Connection._System
Direct Ethernet Connection.Well Station 5
Direct Ethernet Connection.Well Station 5._System
Direct Ethernet Connection.Well Station 5.Inputs
Direct Ethernet Connection.Well Station 5.Outputs
Direct RS232 Connection._System
Direct RS232 Connection.Well Station 0
Direct RS232 Connection.Well Station 0._System
Direct RS232 Connection.Well Station 0.Inputs
Direct RS232 Connection.Well Station 0.Outputs
Direct RS485 Connection._System
Direct RS485 Connection.Well Station 3
Direct RS485 Connection.Well Station 3._System

	Data Type	Value	Timesta...	Qual...	Update Count
Well Station 0.Inputs.Automatic/Manual	Boolean	0	15:50:3...	Good	1
Well Station 0.Inputs.Chlorine Level Swit...	Boolean	0	15:50:3...	Good	1
Well Station 0.Inputs.Fuel Low Level	Boolean	0	15:50:3...	Good	1
Well Station 0.Inputs.Generator State	Boolean	0	15:50:3...	Good	1
Well Station 0.Inputs.High Pressure	Boolean	0	15:50:3...	Good	1
Well Station 0.Inputs.Low Pressure	Boolean	0	15:50:3...	Good	1
Well Station 0.Inputs.NRV	Boolean	0	15:50:3...	Good	1
Well Station 0.Inputs.Power- NZM	Boolean	0	15:50:3...	Good	1
Well Station 0.Inputs.Protection EMT6-1	Boolean	1	15:50:3...	Good	1
Well Station 0.Inputs.Soft Starter Bypass	Boolean	1	15:50:3...	Good	1
Well Station 0.Inputs.Station Run	Boolean	1	15:50:3...	Good	1

(a) Input tags view



KEPware.KEPServerEx.V4
_System
Direct Ethernet Connection._System
Direct Ethernet Connection.Well Station 5
Direct Ethernet Connection.Well Station 5._System
Direct Ethernet Connection.Well Station 5.Inputs
Direct Ethernet Connection.Well Station 5.Outputs
Direct RS232 Connection._System
Direct RS232 Connection.Well Station 0
Direct RS232 Connection.Well Station 0._System
Direct RS232 Connection.Well Station 0.Inputs
Direct RS232 Connection.Well Station 0.Outputs
Direct RS485 Connection._System
Direct RS485 Connection.Well Station 3
Direct RS485 Connection.Well Station 3._System
Direct RS485 Connection.Well Station 3.Inputs
Direct RS485 Connection.Well Station 3.Outputs

	Data Type	Value	Timesta...	Qual...	Update Count
.Well Station 0.Outputs.Chlorine Low Lev...	Boolean	0	15:50:3...	Good	1
.Well Station 0.Outputs.Chlorine Pump R...	Boolean	0	15:50:3...	Good	1
.Well Station 0.Outputs.Emergincy Alarm	Boolean	0	15:50:3...	Good	1
.Well Station 0.Outputs.Fuel Low Level	Boolean	0	15:50:3...	Good	1
.Well Station 0.Outputs.High Presure Level	Boolean	0	15:50:3...	Good	1
.Well Station 0.Outputs.Low Level Press...	Boolean	0	15:50:3...	Good	1
.Well Station 0.Outputs.Lubrication solon...	Boolean	0	15:50:3...	Good	1
.Well Station 0.Outputs.NRV Fault	Boolean	0	15:50:3...	Good	1
.Well Station 0.Outputs.Power Fault NZM	Boolean	0	15:50:3...	Good	1
.Well Station 0.Outputs.Protection Fault ...	Boolean	0	15:50:3...	Good	1
.Well Station 0.Outputs.Soft Starter Run	Boolean	1	15:50:3...	Good	1
.Well Station 0.Outputs.Statio Start Run	Boolean	1	15:50:3...	Good	1
.Well Station 0.Outputs.Water Pump Run...	Boolean	0	15:50:3...	Good	1

(b) Output tags view

Figure (6.4): OPC Quick client input/output tags

6.1.2 RS485 Connection

As RS232, RS485 is one of the simple connections of the PLC with the computer. This method has more advantages than RS232 as below:

1. RS485 use one pair of wires to connect up to 32 drivers (PLC or RS485 device) on the same bus. Every driver has its special address.
2. The distance between the RS485 devices may be as far as 1200 m.

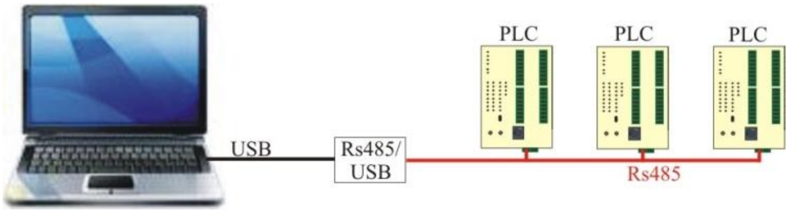


Figure (6.5): PLC RS485 connection

The same previous steps are applied on the vertical turbine plant module by using RS485 port connection. The computer used USB/RS485 converter to connect RS85 bus to the computer as shown in Figure (6.5). RS485 depends on the PLC address in its communication, so it is important to assign specific address numbers to the PLCs on the RS485 bus. This address number is assigned to "Modbus Ascii" device in the KEPserverEx OPC program. All system tags are updated and monitored rapidly as in previous experiment.

6.1.3 Ethernet Connection

Ethernet is one of simple and wide used standard communication connections. In this experiment PLCs are specified with their special IP address. Assigning IP address to the PLC will simple the connection between the PLC and the computer network. DVPEN01-SL [49] is an external Ethernet communication module from Delta is used to add Ethernet port to the Delta PLCs. Figure (6.6) illustrates PLC Ethernet connection.

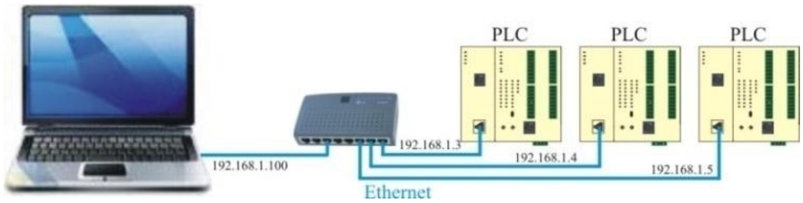


Figure (6.6): PLC Ethernet connection

The DVPEN1-SL modules are connected to the PLCs through the extension port and to the computer through the Ethernet port. DCISoft is used to search about the Ethernet modules. IP address and subnet mask are assigned to each module. WPLSoft program used to read the PLCs programs using their IP addresses. The previous KEPServerEX OPC file is lunched. New channel with "Modbus Ethernet" device driver is created. New "Modbus" device module with the previous IP address is added to the channel. Finally, previous tags are copied to the new devices. As before, The OPC Quick Client tool is used for monitoring the system tags and all system tags are updated and monitored rapidly as expected.

6.2 Connecting With Delta PLC Through Modems

In this part of the experiment external modems are used to connect the plants PLCs to the computer as shown in Figures (6.7) and (6.8). The two plants connections have the same idea, but they differ in the modem type and connection media. U.S. Robotics dial up modem is used to connect the first plant PLC to the computer using dialup and Panasonic Private Branch Exchange (PBX). MOXA OnCell_G2100 GSM/GPRS modem [43] is used to connect the other plant PLC to the computer using cellular phone system. Using modems with Dleta PLCs [50] of earlier models (before SV models) needs to enable and initialize the modem from the PLC. That is done by adding the instructions (Set on M1184 “Enable the modem”) [50] and (Set on M1185 “Enable initialization of modem from PLC”) [50] to the PLC program. Also, modem serial port settings must be as that of the PLC.

6.2.1 Dialup Modems

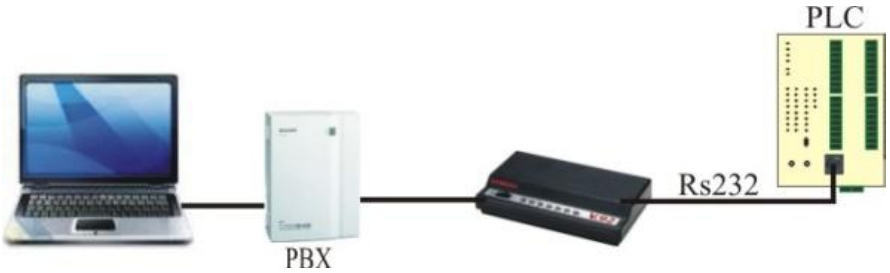


Figure (6.7): PLC dial up connection

In this experiment, the vertical turbine plant’s PLC is connected to the computer through a US Robotics external modem, Panasonic PBX as local dial up exchange, and the internal modem of the computer, this is illustrated Figure (6.7). Plant PLC is SV model so this PLC connects with modems directly without adding previous instructions to the PLC program. As before steps, KEPServerEX OPC program is lunched with same project, new channel with “Modbus ascii Serial” device driver and the internal modem is created. Then new device with “Modbus Ascii” is added to the channel. Also the previous tags are copied to the new device. Dialing up the modem is needed to allow the OPC Quick Client tool to monitor and update the system tags. First the phone number is added by selecting “device_name._Modem” [51] ; right clicking on “Device_name._Modem._PhoneNumber” then selecting “Synchronous Write” and writing the PLC phone number in “Write Value” column. Second, dialing the phone number by right clicking “Device_name._Modem._Dial”; selecting “Synchronous Write” and writing “1” in “Write Value” column to dial the first number in the phone number list. After dialing is succeeded the tags are updated and monitored rapidly as when the PLC was connected directly. To hang up the connection, “device_name._Modem._ Hangup” is right clicked, “Synchronous Write” is selected and 1 is written in “write Value” column.

6.2.2 Cellular Modem

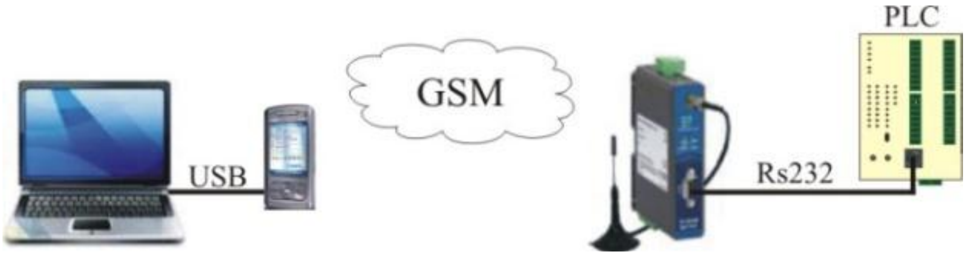
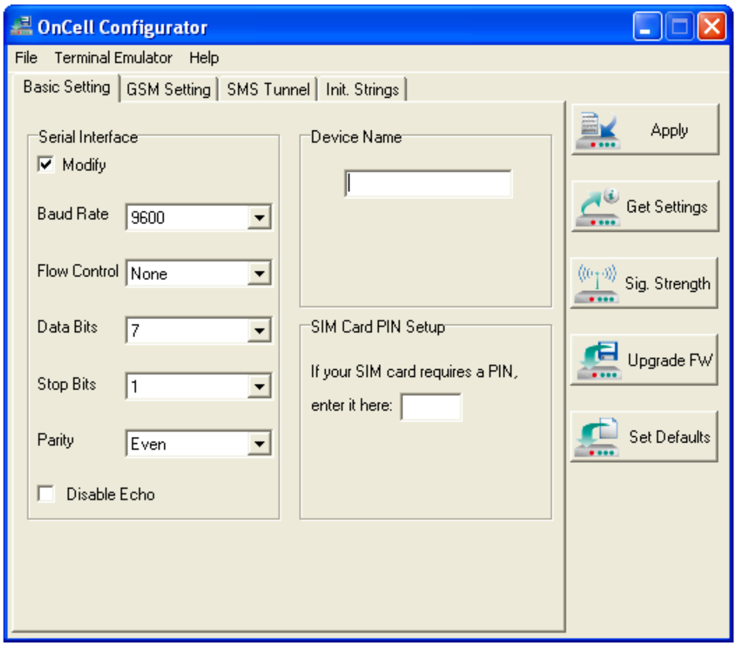


Figure (6.8): PLC cellular system connection

This experiment has the same steps of previous dial up experiment and has the same results. The tags are updated and monitored rapidly as they are connected directly. The difference is only in using the GSM modem “MOXA OnCell_G2100” with the PLC and using mobile phone with computer. The mobile phone is used as modem connected with the computer through the USB port. “OnCell configurator” [43] is program used to configure the GSM modem and modify its serial port settings to match that of the PLC as shown in Figure (6.9).

Through this experiment there was problem of selecting the connection cable between the PLC and the GSM modem. Figure (6.10) shows the serial cable pin settings of the PLC and the GSM modem. The PLC and the modem serial port pins are illustrated in Table (6.1). According to the table, a cross cable connection between the pins (2-3, 3-2) is needed to connect the PLC with the modem.



Serial Interface

☑ Modify

Baud Rate: 9600

Flow Control: None

Data Bits: 7

Stop Bits: 1

Parity: Even

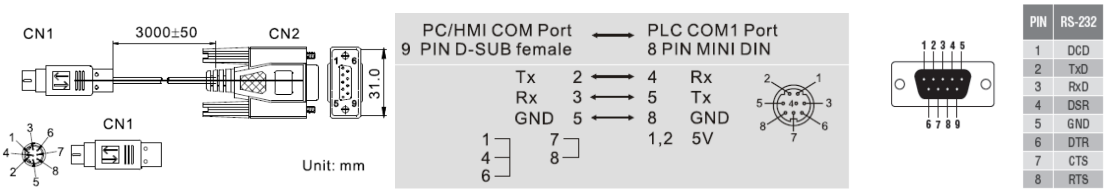
□ Disable Echo

Device Name

SIM Card PIN Setup

If your SIM card requires a PIN, enter it here:

Figure (6.9): OnCell Configurator modify settings window



PIN	RS-232
1	DCD
2	TxD
3	RxD
4	DSR
5	GND
6	DTR
7	CTS
8	RTS

(a) (b)

Figure (6.10): Delta PLC and GSM modem cables settings

Table (6.1): PLC and Modem RS232 pins settings

PLC 9 PIN D-SUB female	GSM Modem RS232 female
Pin 2: Tx	Pin 3: Rx
Pin 3: Rx	Pin 2: Tx
Pin 5: GND	Pin 5: GND

Another problem is generated during this experiment that is the GSM modem port settings are not modified to be as the settings of the PLC. So PLC port settings are modified to match the modified settings of modem. Figure (6.11) illustrates instructions that can be used to modify the PLC serial port settings (115200, e, n, 1). These settings are saved in the PLC register D1036.

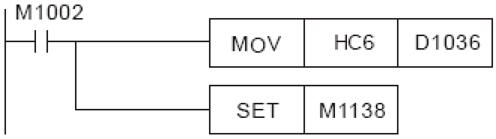


Figure (6.11): Modify PLC serial port settings

Finally, JAWWAL network did not support Circuit Switching Data (CSD), so ORANG cellular network is used. This network has low signal strength in the Lab.

6.3 Connecting With Slave Delta PLC through RS485 Port

This method is called EASY EASY PLC LINK [50], also called master slave connection. The idea depends on that: specific registers (D100-D115 and D200-D215) of the slave PLC are mapped in specific registers in the master PLC depending on the slave PLC address. First group of registers are used for read out and the other are used for write in. Master PLC can communicate with 32 slaves PLC using Modbus protocol.

To demonstrate this experiment the same vertical turbine plants is used as slave with address number 1. Another DVP28SV module is used as master PLC with address number 17. Figure (6.12) illustrates the instructions used to modify the PLC address number and COM2 communication protocol settings (H86: 9600,7,E,1). COM2 used for RS485 port [50].

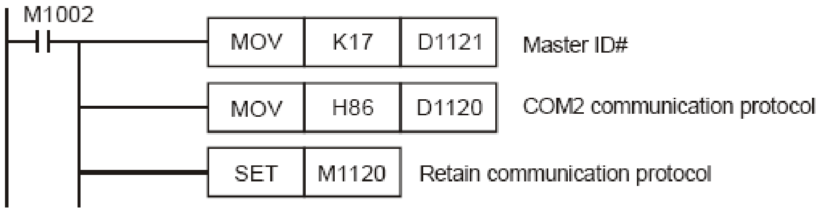


Figure (6.12): Setup the PLC ID and communication protocol

Monitoring data registers of the slave plant depends on monitoring its mapped data registers in the master PLC. In this experiment, it was connected to the master PLC using dialup modem. The previous KEPServerEX file is lunched with its previous file. New device is added to the PSTN dial up connection channel with the slave PLC address number “1”. Previous tags are added to the new device. Tag addresses are modified to match the address of registers in the master PLC which are used to map slave PLC registers. The OPC Quick Client tool is used for monitoring the system tags. All system tags are updated and monitored rapidly as if the PLC is connected directly.

Previous experiments demonstrated most communication scenarios of connecting with the PLC. All these experiments were succeeded in communicating and monitoring the PLC. Monitoring response was rapid. There was some delay in dialing system until making dial and connection. Selecting the communication type between well stations and the SCADA system will depend on cost, availability not on the technician.

Chapter 7

Conclusions and Recommendation

7.1 Conclusions

The importance of water in our region pushes us to try to use the new world technology in controlling our little resources of water supply. One of main parts of this research is an experimental platform comprises four well plant modules which are equipped with Delta DVP28SV PLCs. Several experiments were presented to test, evaluate and demonstrate several communication scenarios between the SCADA server and these plants using different configurations, all results were acceptable.

The other part of the research presents a framework for building a SCADA system to control Gaza water well stations. The final recommendations are upgrading of the present system depending on adding new components that are needed for the SCADA system with keeping the previous control system components, so the upgraded system will have the ability to run the new control system with all its original options.

Also, Wireless communication system is more suitable because it has no cost for infrastructure, no running cost charges and the connection and monitoring can be online for 24 hours. Near stations are connected with others through RS485 bus then connected with the main control room through wireless unit. SATTELLAR and TELEDESIGN wireless systems are recommended to be used for wireless system. It is good to use backing communication system for main well pumping stations using PSTN system for well stations that has dialup line, and cellular system may be used for stations that have problems with PSTN network.

7.2 Future Work and Suggestions

Water system depends on water resources and water distribution network. This research builds SCADA system for the water resources, to complete the automation of drinking water system in Gaza city, it is needed to extend the work to include the water distribution network to monitor the network pressure, water flow and automate the main valves in the network.

Also it is good to extend this SCADA system to include all cities in Gaza strip, especially all these cities nearly have the same water resources, stations components and the same control system stations.

References

[1] SHAKER, A.: “Prospects of Private Sector Participation for Sustainable Water and Sanitation Services in The Gaza Strip”, The Islamic University, Gaza 2007.

[2] Alberta Agriculture, Food and Rural Development, “Submersible Pumps”, January 2007.

[3] The Gouldspump web site, available: http://www.gouldspumps.com/pag_0027a%20.html.

[4] A. Alihussein, M.Abdelati, “A Supervisory Control and Data Acquisition (SCADA) for Water Pumping Stations Of Gaza”, International Engineering Conference 3, The Islamic University of Gaza, 2010.

[5] H. Lee Smith, “A Brief History of Electric Utility Automation Systems”, Electric Energy magazine, Copyright 2010.

[6] M.Abdelati, F. Rabah, “A framework For Building a SCADA System for Beit Lahia Wastwater Pumping Station” The Islamic University Journal, Vol.15, No. 2, pp 235-245, ISSN 1726-6807, 2007.

[7] Office of the Manager National Communications System, Communication Technologies, Inc. “Supervisory Control and Data Acquisition (SCADA) Systems”, October 2004.

[8] A. Creery, E. J. Byres, “Industrial Cybersecurity For Power System And Scada Networks”, IEEE Paper No. PCIC-2005-DV45.

[9] M. Abdelati, “Modern Automation Systems”, Laxmi Publications, 2009.

[10] M. Mahmud, M. R. Karim, M. M. Islam, K. M. Rahman, “Supervisory Control and Data Acquisition (SCADA) Through Internet”, Second International Conference on Electrical and Computer Engineering, ICECE 2002, Dhaka, Bangladesh, pp 56-59, ISBN 984-32-0328-3, 26-28 December 2002.

[11] F. Perez, I. Gomez, J. Luque, G. Sanchez “SCADA System Design Alternatives Based on TCP/IP”, Study Committee 35, POLAND, October 1999 .

[12] Douglas C. Osburn, “Remote Terminal Unit”, US2002/0147503A1, Oct. 10,2002.

[13] SOLCON website, “SMStransever”, available: http://www.solcon.com.

[14] SOLCON website, “RVS-DN Digital Soft Starter”, Instruction Manual, Available: http://www.solcon.com.

[15] Sixnet Company website, available: http://www.sixnet.com.

[16] FF-Automation company website, available: http:// www.ff-automation.com.

[17] Motorola company website, available: http://www.motorola.com.

[18] Delta Electronic INC., available: http://www.delta.com.tw.

[19] SIEMENS website, available: http://www.automation.siemens.com.

[20] Modicon sales website, available: http://www.squared.com.

[21] Mini S. Thomas, Parmod Kumar, Vinay K. Chandna, “Design, Development, and Commissioning of a Supervisory Control and Data Acquisition (SCADA) Laboratory for Research and Training”, IEEE Transactions On Power Systems, VOL. 19, NO. 3, August 2004.

[22] Zolotová, I., Flochová, J., Ocelíková, E. “Database Technology and Real Time Industrial Transaction Techniques In Control”, Journal of Cybernetics and Informatics pp 18-23, ISSN: 1336-4774**,** VOL. 5, 2005.

[23] OPC Foundation, “OLE for Process Control Data Access Automation Specification”, Ver 2.01, January 1999.

[24] Erion Allan, “Raising Expectations for SCADA/RTUs”, Alberta Operators Seminar, March 2001.

[25] KEPServerEx program help, “Introduction to KEPServerEx” , Help version 1.019

[26] Rao Kalapatapu, “SCADA Protocols and Communication Trends”, ISA, 2004.

[27] Modbus interface tutorial, available: http://www.lammertbies.nl.

[28] “PROFIBUS Technology and Application”, available: www.automation.siemens.com .

[29] “NETWORKING”, available: http://claymore.engineer.gvsu.edu/~jackh/books/plcs/chapters/plc_interface.pdf.

[30] DELTA web site, “VFD-USB01”, Available: http://www.delta.com.tw.

[31] Modbus IDA. “Modbus application protocol specification” , v1.1a, June 4, 2004.

[32] Modbus IDA. “Modbus messaging on TCP/IP implementation guide”, v1.0a, June 4, 2004.

[33] Moeller, “Overload Relay EMT6”, available: ftp://ftp.moeller.net/documentation/awb_manuals/h1446g.pdf .

[34] FLYGT, ITT industries, “Installation and service, CAS”,. Available: http://int.flygt.com/682787.pdf.

[35] Moeller, industrial automation, NZM Moulded Case Circuit-Breakers –NZM 1, 2, 3 & 4 available: http://www.moeller.co.uk/circbreak_swdis_nzm1-4.htm.

[36] NGEST project management unit, “Bidding Documents for the Construction of Terminal Pumping Station”, Palestinian Water Authority, December 2004.

[37] Technical Tutorial, “Introduction to Serial Communication” , Dec. 2002, available: http://www.sena.com/download/tutorial/tech_Serial_v1r0c0.pdf.

[38] “RS485 serial information”, available: http://www.lammertbies.nl.

[39] US department of Transportation, Federal Highway Administration, “Telecommunications Handbook for Transportation Professionals” Sep. 2004.

[40] Delta Electronic INC. website, “VFD-USB01”, Available: http://www.delta.com.tw.

[41] “International Telecommunication Union”, available: http://www.itu.int

[42] “Introduction to Wireless Networks” available: http://www.tinker.tv/download/wireless_sample.pdf.

[43] MOXA Technologies Co., Ltd, web site, “G2100 Series User’s Manual”, Fourth Edition, November 2007.

[44] 3COM website, “3COM 54 MBPS Wireless Lan Building To Building Bridge and Access Point” manual, available: http://www.3com.

[45] Ministry of Telecom and Information Technology, “Wire and Wireless Communication low - # 3 19996”, available: http://www.mtit.gov.ps.

[46] SATEL web site, “SATELLAR_Digital_System_052009”, available: http://www.satel.com.

[47] KEPware Inc., “KEPware Enhanced OPC/DDE Server Help Documents”, V4.201.359-U, 2006.

[48] Delta Electronic INC. website, “KEPServer EX with SV”, available: http://www.delta.com.tw.

[49] Delta Electronic INC., “PLCDVPEN01-SL_manual_en”, available: http://www.delta.com.tw.

[50] Delta Electronic INC. website, “PLC-Application-Manual_en”, available: http://www.delta.com.tw.

[51] Kepware website, “KEPServerEX_Modem_Use_Notes”, available: http://www.kepware.com.