"SCADA IMPLIMENTATION IN PIPELINE NETWORK"

By
Badgujar Mayur Ramkrishna
M.Tech (Gas Engineering)

College of Engineering

University of petroleum & energy studies

Dehradun

May, 2008

“SCADA IMPLIMENTATION IN PIPELINE NETWORK”

A thesis submitted in partial fulfillment of the requirement for the degree of
Master of technology
(Gas engineering)

By
Badgujar mayur ramkrishna

Under the guidance of

Gammon India ltd	University of Petroleum and Energy Studies
Mr.J.S.MORE	Prof.Kamal bansal

Approved

....

Dean

College of Engineering

University of petroleum & energy studies

Dehradun

May , 2008

UNIVERSITY OF PETROLEUM & ENERGY STUDIES
(ISO 9001:2000 Certified)

CERTIFICATE

This is to certify that the project work contained in this thesis titled **SCADA IMPLIMENTATION IN PIPELINE NETWORK** has been carried out by **Mr. Mayur Ramrishna Badgujar**, under my supervision and has not been submitted elsewhere for a degree.

Prof. Kamal Bansal
College of Engineering
University of Petroleum and Energy Studies
Dehradun, India

Date: 16 / 5 / 08

Report has been assessed for
34 marks out of 50
$\frac{34}{50}$

Corporate Office:
:ocarbons Education & Research Society
d Floor, PHD House.
4/2 Siri Institutional Area
ugust Kranti Marg, New Delhi - 110 016 India
h.: +91-11-41730151-53 Fax : +91-11-41730154

Main Campus:
Energy Acres,
PO Bidholi Via Prem Nagar,
Dehradun - 248 007 (Uttarakhand), India
Ph.: +91-135-2102690-91, 2694201/ 203/ 208
Fax: +91-135-2694204

Regional Centre (NCR):
SCO, 9-12, Sector-14,
Gurgaon 122 007
(Haryana), India.
Ph: +91-124-4540 300
Fax: +91-124-4540 330

Regional Centre (Rajahmundry):
GIET, NH 5, Velugubanda,
Rajahmundry - 533 294,
East Godavari Dist., (Andhra Pradesh), India
Tel: +91-883-2484811/ 855
Fax: +91-883-2484822

Email: info@upes.ac.in URL: www.upes.ac.in

GAMMON

Date – 10th May 2008

TO WHOMSOEVER IT MAY CONCERN

This is to certify that **Mr. Mayur Badgujar S/o Sri Ramkrishna Badgujar** has successfully completed his project work on **' SCADA Implementation in Pipeline Network'** in order to partial fulfillment of his **Master of Technology (M.Tech)** in Gas Engineering from 10th March 2008 to 10th May 2008 in our organization for our Dahej-Uran Pipeline project - Navi Mumbai

During his project period, we found him sincere, hard working, and having a good conduct.

We wish him for his bright future.

For **GAMMON INDIA LIMITED**

P.D.Prasad Rao
General Manager -Projects

Abstract

The goal of this 50 days project was to commission (SCADA) control system and Data management System for "Dahej Uran 30" Gas transportation pipeline".

The system measure, monitor and control flow and pressure of gas at supervisory level.

Working Gas pressure is 60 to 65 bars, the line follow path of rocky, rural area and crossed highway, railways and rivers with 24 control stations

Two controls system has been used at each station

1. PLC, which is used to control main line actuator Valves & pressure of line.
2. Flow computer, which collects, analyze the data from Gas chromatography, filtration, laid down skid and metering skid and give feedback signal for further controls.

Both control system has been terminated to RTU panel, which is interfaced with SCADA control system through 24 cores OFC. All stations has been provided with fire, smoke & gas detection system like point gas detector, open path gas detector for emergency preparedness.

Four level securities have been provided at station computers for data security of process parameters. It also provides all type Management Information System.

During this period commissioning has been completed for Uran MSEB, Deepak Fertilizer.

Finally, recommendations on what the organization should focus on with regards SCADA systems, Project Planning and Execution for smooth execution, to save cost.

ACKNOWLEDGEMENT

First of all I would like to thank Gammon India ltd for allowing me to undergo final year project at their esteemed organization. It was a wonderful learning experience to work with the organization.

I am greatly indebted to my guide **Prof. Kamal bansal ,UPES** , for providing me an opportunity to work under his guidance .His unflinching support,suggations and directions have helped in the smooth progress of the project work.

I would like express my deepest thanks to **Major Vikram Singh (AGM-HR)** who allowed us access to various departments.

I express my heartfelt gratitude to my mentor Mr. **P.D.Prasad Rao, GM (Project)** and **Mr.B.Surendra** under whose aegis the project could be completed. I would like to thank Mr. J.S.More (Dy.Mgr), Mr. Mayur Chitte, Mr.Jitendra, Mr.Prem, and Mr. Shadab.who was of immense help at every stage of my project work.

Mayur R. Badgujar
M.Tech (Gas Engg.)
Roll no –R030206007

INDEX

NOMENCLATURE

ANSI	American National Standards Institute
ARP	Address Resolution Protocol
CDMA	Code Division Multiple Access
CMS	Central Monitoring Station
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DNP	Distributed Network Protocol
ESD	Emergency Shut Down
HMI	Human Machine Interface
I/O	Input/output
IEC	International Electro technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
MMI	Man Machine Interface
NCS	National Communications System
NE/EP	National Security/Emergency Preparedness
PLC	Programmable Logic Controller
RTU	Remote terminal unit
SSV	Slam shut valve
SCADA	Supervisory Control and Data Acquisition
TCP/IP	Transmission Control Protocol/Internet Protocol
UHF	Ultra High Frequency

1.0 Introduction

SCADA (Supervisory Control And Data Acquisition) system refers to the combination of telemetry and data acquisition. It consists of collecting information, transferring it back to a central site, carrying out necessary analysis and control, and then displaying this data on a number of operator screens. The SCADA system is used to monitor and control a pipeline network, plant or equipment. Control may be automatic or can be initiated by operator commands.

It is a process control system that enables a site operator to monitor and control processes that are distributed among various remote sites.

A properly designed SCADA system saves time and money by eliminating the need for service personnel to visit each site for inspection, data collection/logging or make adjustments. Real-time monitoring, system modifications, troubleshooting, increased equipment life, automatic report generating these are just a few of the benefits that come with today's SCADA system. As technology continues to advance, SCADA systems will be the operating standard for any processing site. But from the hundreds of system providers available today, which one will you choose to partner with and why? Choosing a SCADA system provider that will design a system applicable to your needs can be an overwhelming, confusing task. With little or no knowledge of SCADA and telemetry systems and an incomplete pre-system assessment, decisions made can be costly mistakes.

The four major SCADA system components include the Master Terminal Unit (MTU), the Remote Terminal Unit (RTU), Communication Equipment and SCADA Software. The MTU is located at the operator's central control facility and enables two-way data communication and control of remote field devices. The RTU, located at the remote site, gathers data from field devices (pumps, valves, alarms, etc.) in memory until the MTU initiates a send command. The central processing unit (CPU) within the RTU receives a data stream via hardware equipment protocol. When the RTU sees its specific address embedded in the protocol, data is interpreted and the CPU directs the specified action to take. The protocol used can be open like Modbus, Transmission Control Protocol and Internet Protocol (TCP/IP) or a proprietary closed protocol. Some RTUs, called "smart PLCs" or Remote Access PLCs (RAPLC) provide remote programmable functionality while retaining the communications capability of an RTU. These devices are designed to perform control, check site conditions, re-program anytime from anywhere and have any alarm or event trigger a call to your personal computer without any direction from the MTU.

2.0 SCADA Overview

SCADA is an acronym for Supervisory Control and Data Acquisition. SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation. These systems encompass the transfer of data between a SCADA central host computer and a number of Remote Terminal Units (RTUs) and/or Programmable Logic Controllers (PLCs), and the central host and the operator terminals. A SCADA system gathers information (such as where a leak on a pipeline has occurred), transfers the information back to a central site, then alerts the home station that a leak has occurred, carrying out necessary analysis and control, such as determining if the leak is critical, and displaying the information in a logical and organized fashion. These systems can be relatively simple, such as one that monitors environmental conditions of a small office building, or very complex, such as a system that monitors all the activity in a nuclear power plant or the activity of a municipal water system. Traditionally, SCAD systems have made use of the Public Switched Network (PSN) for monitoring purposes. Today many systems are monitored using the infrastructure of the corporate Local Area Network (LAN)/Wide Area Network (WAN). Wireless technologies are now being widely deployed for purposes of monitoring.

SCADA systems consist of:

- One or more field data interface devices, usually RTUs, or PLCs, which interface to field sensing devices and local control switchboxes and valve actuators
- 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.
- A central host computer server or servers (sometimes called a SCADA Center, master station, or Master Terminal Unit (MTU)
- 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

Figure 2.1 shows a typical SCADA system. Each of the above system components will be discussed in detail in the next

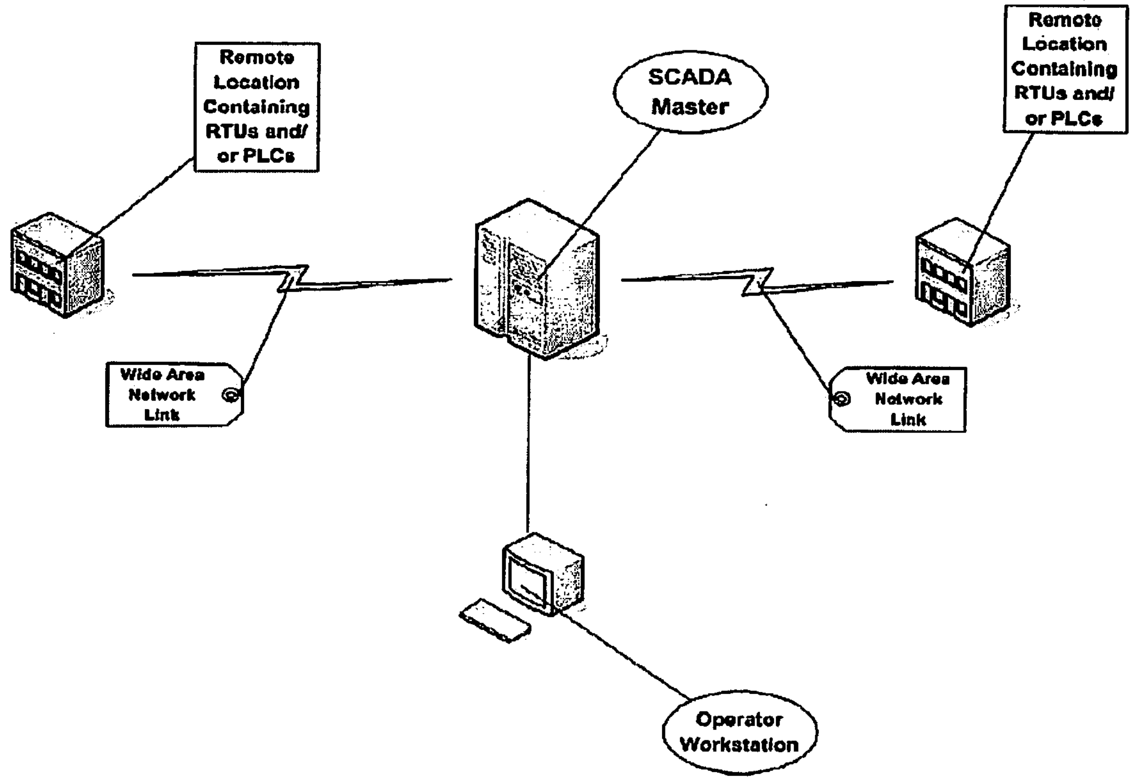

Remote Location Containing RTUs and/ or PLCs
SCADA Master
Remote Location Containing RTUs and/ or PLCs
Wide Area Network Link
Wide Area Network Link
Operator Workstation

Figure 2.1: Typical SCADA System

2.1 Field Data Interface Devices

Field data interface devices form the "eyes and ears" of a SCADA system. Devices such as reservoir level meters, water flow meters, valve position transmitters, temperature transmitters, power consumption meters, and pressure meters all provide information that can tell an experienced operator how well a water distribution system is performing. In addition, equipment such as electric valve actuators, motor control switchboards, and electronic chemical dosing facilities can be used to form the "hands" of the SCADA system and assist in automating the process of distributing water.

However, before any automation or remote monitoring can be achieved, the information that is passed to and from the field data interface devices must be converted to a form that is compatible with the language of the SCADA system. To achieve this, some form of electronic field data interface is required. RTUs, also known as Remote Telemetry Units, provide this interface. They are primarily used to convert electronic signals received from field interface devices into the language (known as the communication protocol) used to transmit the data over a communication channel. The instructions for the automation of field data interface devices, such as pump control logic, are usually stored locally. This is largely due to the limited bandwidth typical of communications links between the SCADA central host computer and the field data interface devices. Such instructions are traditionally held within the PLCs, which have in the past been physically separate from RTUs. A PLC is a device used to automate monitoring and control of industrial facilities. It can be used as a stand-alone or in conjunction with a SCADA or other system. PLCs connect directly to field data interface devices and incorporate programmed intelligence in the form of logical procedures that will be executed in the event of certain field conditions.

PLCs have their origins in the automation industry and therefore are often used in manufacturing and process plant applications. The need for PLCs to connect to communication channels was not great in these applications, as they often were only required to replace traditional relay logic systems or pneumatic controllers. SCADA systems, on the other hand, have origins in early telemetry applications, where it was only necessary to know basic information from a remote source. The RTUs connected to these systems had no need for control programming because the local control algorithm was held in the relay switching logic. As PLCs were used more often to replace relay switching logic control systems, telemetry was used more and more with PLCs at the remote sites. It became desirable to influence the program within the PLC through the use of a remote signal. This is in effect the "Supervisory Control" part of the acronym SCADA. Where only a simple local control program was required, it became possible to store this program within the RTU and perform the control within that device. At the same time, traditional PLCs included communications modules that would allow PLCs to report the state of the control program to a computer plugged into the PLC or to a remote computer via a telephone line. PLC and RTU manufacturers therefore compete for the same market. As a result of these developments, the line between PLCs and RTUs has blurred and the terminology is virtually interchangeable. For the sake of simplicity, the term RTU will be used to refer to a remote field data interface device; however, such a device could include automation programming that traditionally would have been classified as a PLC.

2.2 Communications Network

The communications network is intended to provide the means by which data can be transferred between the central host computer servers and the field-based RTUs. The

Communication Network refers to the equipment needed to transfer data to and from different sites. The medium used can either be cable, telephone or radio.

The use of cable is usually implemented in a factory. This is not practical for systems covering large geographical areas because of the high cost of the cables, conduits and the extensive labor in installing them. The use of telephone lines (i.e., leased or dial-up) is a more economical solution for systems with large coverage. The leased line is used for systems requiring on-line connection with the remote stations. This is expensive since one telephone line will be needed per site. Dial-up lines can be used on systems requiring updates at regular intervals (e.g., hourly updates). Here ordinary telephone lines can be used. The host can dial a particular number of a remote site to get the readings and send commands. Remote sites are usually not accessible by telephone lines. The use of radio offers an economical solution. Radio modems are used to connect the remote sites to the host. An on-line operation can also be implemented on the radio system. For locations where a direct radio link cannot be established, a radio repeater is used to link these sites.

Historically, SCADA networks have been dedicated networks; however, with the increased deployment of office LANs and WANs as a solution for interoffice computer networking, there exists the possibility to integrate SCADA LANs into everyday office computer networks. The foremost advantage of this arrangement is that there is no need to invest in a separate computer network for SCADA operator terminals. In addition, there is an easy path to integrating SCADA data with existing office applications, such as spreadsheets, work management systems, data history databases, Geographic Information System (GIS) systems, and water distribution modeling systems.

2.3 Central Host Computer

The central host computer or master station is most often a single computer or a network of computer servers that provide a man-machine operator interface to the SCADA system. The computers process the information received from and sent to the RTU sites and present it to human operators in a form that the operators can work with. Operator terminals are connected to the central host computer by a LAN/WAN so that the viewing screens and associated data can be displayed for the operators. Recent SCADA systems are able to offer high resolution computer graphics to display a graphical user interface or mimic screen of the site or water supply network in question. Historically, SCADA vendors offered proprietary hardware, operating systems, and software that was largely incompatible with other vendors' SCADA systems. Expanding the system required a further contract with the original SCADA vendor. Host computer platforms characteristically employed UNIX-based architecture, and the host computer network was physically removed from any office-computing domain. However, with the increased use of the personal computer, computer networking has become commonplace in the office and as a result, SCADA systems are now available that can network with office-based personal computers. Indeed, many of today's SCADA systems can reside on computer servers that are identical to those servers and computers used for traditional office applications. This has opened a range of possibilities for the linking of SCADA systems to office-based applications such as GIS systems, hydraulic modeling software, drawing management systems, work scheduling systems, and information databases.

2.4 Operator Workstations and Software Components

Operator workstations are most often computer terminals that are networked with the SCADA central host computer. The central host computer acts as a server for the

SCADA application and the operator terminals are clients that request and send information to the central host computer based on the request and action of the operators. An important aspect of every SCADA system is the computer software used within the system. The most obvious software component is the operator interface or Man Machine Interface/Human Machine

Interface (MMI/HMI) package; however, software of some form pervades all levels of a SCADA system. Depending on the size and nature of the SCADA application, software can be a significant cost item when developing, maintaining, and expanding a SCADA system. When software is well defined, designed, written, checked, and tested, a successful SCADA system will likely be produced. Poor performances in any of these project phases will very easily cause a SCADA project to fail. Many SCADA systems employ commercial proprietary software upon which the SCADA system is developed. The proprietary software often is configured for a specific hardware platform and may not interface with the software or hardware produced by competing vendors. A wide range of commercial off-the-shelf (COTS) software products also are available, some of which may suit the required application. COTS software usually is more flexible, and will interface with different types of hardware and software. Generally, the focus of proprietary software is on processes and control functionality, while COTS software emphasizes compatibility with a variety of equipment and instrumentation. It is therefore important to ensure that adequate planning is undertaken to select the software systems appropriate to any new SCADA system. Software products typically used within a SCADA system are as follows:

- Central host computer operating system: Software used to control the central host computer hardware. The software can be based on UNIX or other popular operating systems.
- Operator terminal operating system: Software used to control the central hostcomputer hardware. The software is usually the same as the central host computer operating system. This software, along with that for the central host computer, usually contributes to the networking of the central host and the operator terminals.
- Central host computer application: Software that handles the transmittal and reception of data to and from the RTUs and the central host. The software also provides the graphical user interface which offers site mimic screens, alarm pages, trend pages, and control functions.
- Operator terminal application: Application that enables users to access information available on the central host computer application. It is usually a subset of the software used on the central host computers.
- Communications network management software: Software required to control the communications network and to allow the communications networks themselves to be monitored for performance and failures.

- RTU automation software: Software that allows engineering staff to configure and maintain the application housed within the RTUs (or PLCs). Most often this includes the local automation application and any data processing tasks that are performed within the RTU.

The preceding software products provide the building blocks for the application-specific software, which must be defined, designed, written, tested, and deployed for each SCADA system.

3.0 SCADA Architectures

SCADA systems have evolved in parallel with the growth and sophistication of modern computing technology. The following sections will provide a description of the following three generations of SCADA systems:

- First Generation – Monolithic
- Second Generation – Distributed
- Third Generation – Networked

3.1 Monolithic SCADA Systems

When SCADA systems were first developed, the concept of computing in general centered on "mainframe" systems. Networks were generally non-existent, and each centralized system stood alone. As a result, SCADA systems were standalone systems with virtually no connectivity to other systems. The Wide Area Networks (WANs) that were implemented to communicate with remote terminal units (RTUs) were designed with a single purpose in mind–that of communicating with RTUs in the field and nothing else. In addition, WAN protocols in use today were largely unknown at the time.

The communication protocols in use on SCADA networks were developed by vendors of RTU equipment and were often proprietary. In addition, these protocols were generally very "lean", supporting virtually no functionality beyond that required scanning and controlling points within the remote device. Also, it was generally not feasible to intermingle other types of data traffic with RTU communications on the network.

Connectivity to the SCADA master station itself was very limited by the system vendor.

Connections to the master typically were done at the bus level via a proprietary adapter or controller plugged into the Central Processing Unit (CPU) backplane. Redundancy in these first generation systems was accomplished by the use of two identically equipped mainframe systems, a primary and a backup, connected at the bus level. The standby system's primary function was to monitor the primary and take over in the event of a detected failure. This type of standby operation meant that little or no processing was done on the standby system. Figure 3.1 shows a typical first generation SCADA architecture.

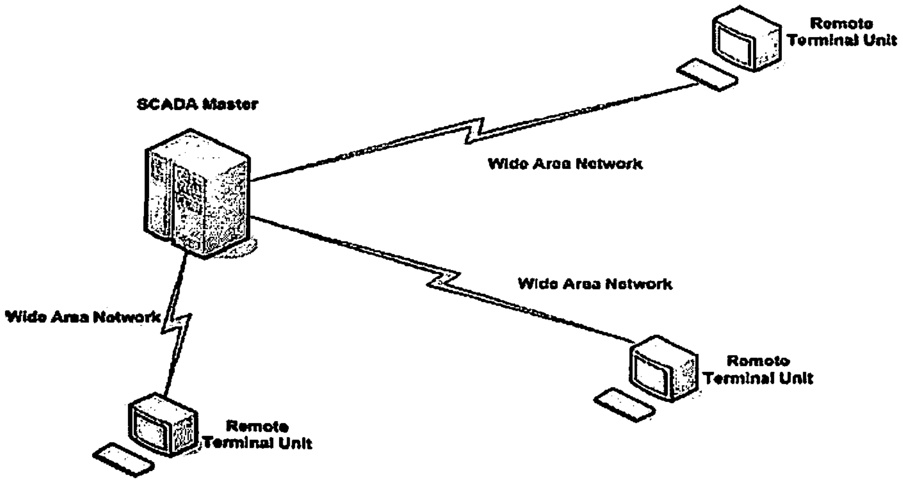


Figure 3.1: First Generation SCADA Architecture [5]

3.2 Distributed SCADA Systems

The next generation of SCADA systems took advantage of developments and improvement in system miniaturization and Local Area Networking (LAN) technology to

Distribute the processing across multiple systems. Multiple stations, each with a specific function, were connected to a LAN and shared information with each other in real-time. These stations were typically of the mini-computer class, smaller and less expensive than their first generation processors. Some of these distributed stations served as communications processors, primarily communicating with field devices such as RTUs. Some served as operator interfaces, providing the human-machine interface (HMI) for system operators. Still others served as calculation processors or database servers. The distribution of individual SCADA system functions across multiple systems provided more processing power for the system as a whole than would have been available in a single processor. The networks that connected these individual systems were generally based on LAN protocols and were not capable of reaching beyond the limits of the local environment

Some of the LAN protocols that were used were of a proprietary nature, where the vendor created its own network protocol or version thereof rather than pulling an existing one off the shelf. This allowed a vendor to optimize its LAN protocol for real-time traffic, but it limited (or effectively eliminated) the connection of network from other vendors to the SCADA LAN. Figure 3.2 depicts typical second generation SCADA architecture.

Distribution of system functionality across network-connected systems served not only to increase processing power, but also to improve the redundancy and reliability of the system as a whole. Rather than the simple primary/standby failover scheme that was utilized in many first generation systems, the distributed architecture often kept all stations on the LAN in an online state all of the time. For example, if an HMI station were to fail, another HMI station could be used to operate the system, without waiting for failover from the primary system to the secondary. The WAN used to communicate with devices in the field were largely unchanged by the development of LAN connectivity between local stations at the SCADA master. These external communications networks were still limited to RTU protocols and were not available for other types of network traffic.

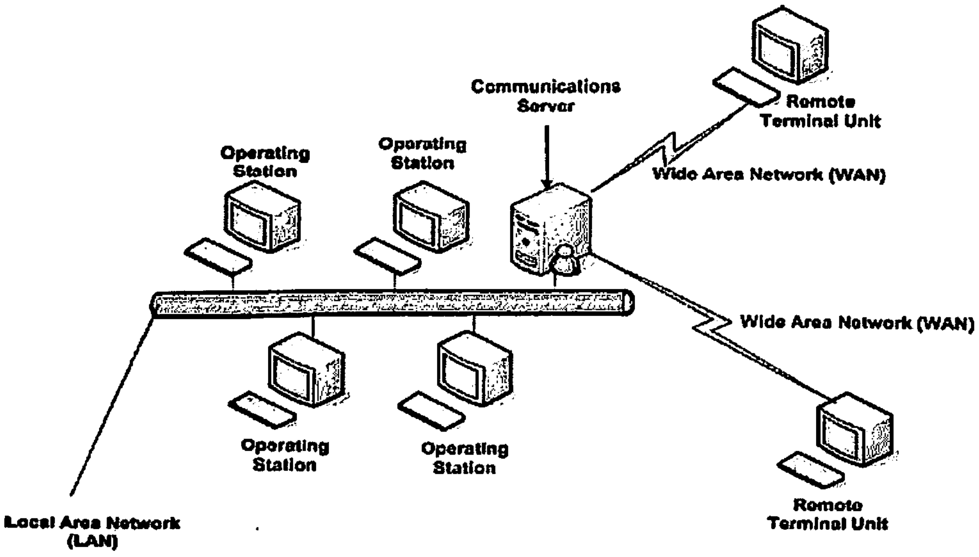


Figure 3.2: Second Generation SCADA Architecture [5]

As was the case with the first generation of systems, the second generation of SCADA systems was also limited to hardware, software, and peripheral devices that were provided or at least selected by the vendor

3.3 Networked SCADA Systems:-

We are commonly use this architecture because it will provided

- Open system architecture
- Utilizing open standard and protocol
- Making it possible to distribute SCADA functionality across WAN.
- System make easier for the user to third party periphery devices (such as monitor ,printer, disk drive etc .)

The current generation of SCADA master station architecture is closely related to that of the second generation, with the primary difference being that of open system architecture rather than a vendor controlled, proprietary environment. There are still multiple networked systems, sharing master station functions. There are still RTUs utilizing protocols that are vendor-proprietary. The major improvement in the third generation is that of opening the system architecture, utilizing open standards and protocols and making it possible to distribute SCADA functionality across a WAN and not just a LAN. Open standards eliminate a number of the limitations of previous generations of SCADA systems. The utilization of off-the-shelf systems makes it easier for the user to connect third party peripheral devices (such as monitors, printers, disk drives, tape drives, etc.) to the system and/or the network. As they have moved to "open" or "off-the-shelf" systems, SCADA vendors have gradually gotten out of the hardware development business. These vendors have looked to system vendors such as Compaq, Hewlett-Packard, and Sun Microsystems for their expertise in developing the basic computer platforms and operating system software. This allows SCADA vendors to concentrate their development in an area where they can add specific value to the system–that of SCADA master station software. The major improvement in third generation SCADA systems comes from the use of WAN protocols such as the Internet Protocol (IP) for communication between the master station and communications equipment. This allows the portion of the master station that is responsible for communications with the field devices to be separated from the master station "proper" across a WAN. Vendors are now producing RTUs that can communicate with the master station using an Ethernet connection. Figure 3.3 represents a networked SCADA system.

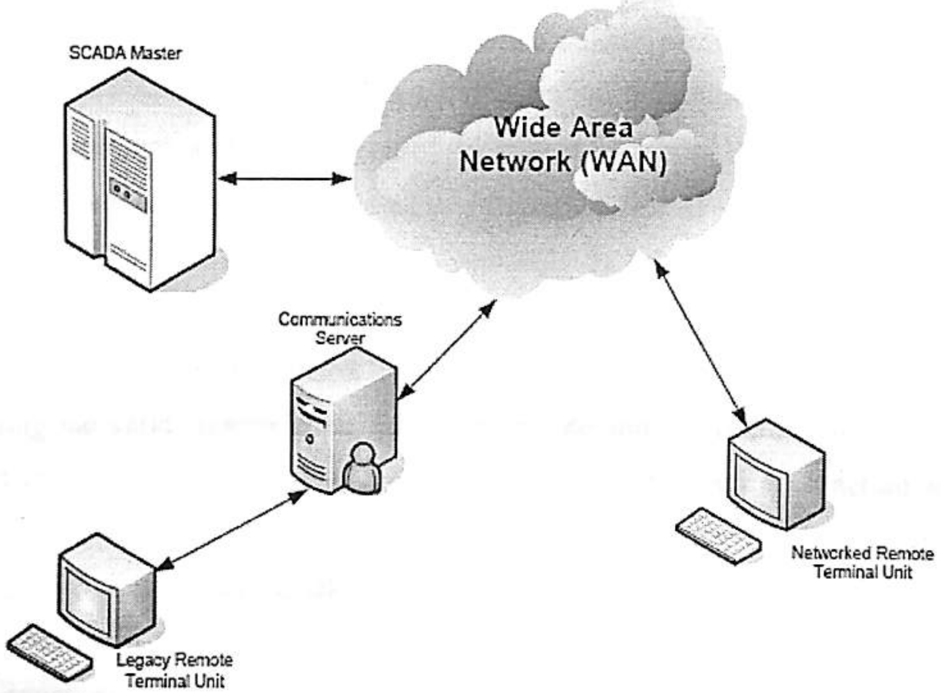


Figure 3.3: Third Generation SCADA System [5]

Another advantage brought about by the distribution of SCADA functionality over a WAN is that of disaster survivability. The distribution of SCADA processing across a LAN in second-generation systems improves reliability, but in the event of a total loss of the facility housing the SCADA master, the entire system could be lost as well. By distributing the processing across physically separate locations, it becomes possible to build a SCADA system that can survive a total loss of any one location. For some organizations that see SCADA as a super-critical function, this is a real benefit.

4.0 SCADA Protocols

In a SCADA system, the RTU accepts commands to operate control points, sets analog output levels, and responds to requests. It provides status, analog and accumulated data to the SCADA master station. The data representations sent are not identified in any fashion other than by unique addressing. The addressing is designed to correlate with the SCADA master station database. The RTU has no knowledge of which unique parameters it is monitoring in the real world. It simply monitors certain points and stores the information in a local addressing scheme. The SCADA master station is the part of the system that should "know" that the first status point of RTU number 27 is the status of a certain circuit breaker of a given substation. This represents the predominant SCADA systems and protocols in use in the utility industry today. Each protocol consists of two message sets or pairs. One set forms the master protocol, containing the valid statements for master station initiation or response, and the other set is the RTU protocol, containing the valid statements an RTU can initiate and respond to. In most but not all cases, these pairs can be considered a poll or request for information or action and a confirming response. The SCADA protocol between master and RTU forms a viable model for RTU-to-Intelligent Electronic Device (IED) communications. Currently, in industry, there are several different protocols in use. The most popular are International Electro technical Commission (IEC) 60870-5 series, specifically IEC 60870-5-101 (commonly referred to as 101) and Distributed Network Protocol version 3 (DNP3).

4.1 IEC 60870-5-101

IEC 60870-5 specifies a number of frame formats and services that may be provided at different layers. IEC 60870-5 is based on a three-layer Enhanced Performance Architecture (EPA) reference model (see Figure 4.1) for efficient implementation within RTUs, meters, relays, and other Intelligent Electronic Devices (IEDs). Additionally, IEC

60870-5 defines basic application functionality for a user layer, which is situated between the Open System Interconnection (OSI) application layer and the application program. This user layer adds interoperability for such functions as clock synchronization and file transfers. The following descriptions provide the basic scope of each of the five documents in the base IEC 60870-5 telecontrol transmission protocol specification set. Standard profiles are necessary for uniform application of the IEC 60870-5 standards. A profile is a set of parameters defining the way a device acts. Such profiles have been and are being created. The 101 profile is described in detail following the description of the applicable standards.

- IEC 60870-5-1 (1990-02) specifies the basic requirements for services to be provided by the data link and physical layers for telecontrol applications. In particular, it specifies standards on coding, formatting, and synchronizing data frames of variable and fixed lengths that meet specified data integrity requirements.

- IEC-60870-5-2 (1992-04) offers a selection of link transmission procedures using a control field and optional address field; the address field is optional because some point-to-point topologies do not require either source or destination addressing.
- IEC 60870-5-3 (1992-09) specifies rules for structuring application data units in transmission frames of telecontrol systems. These rules are presented as generic

.

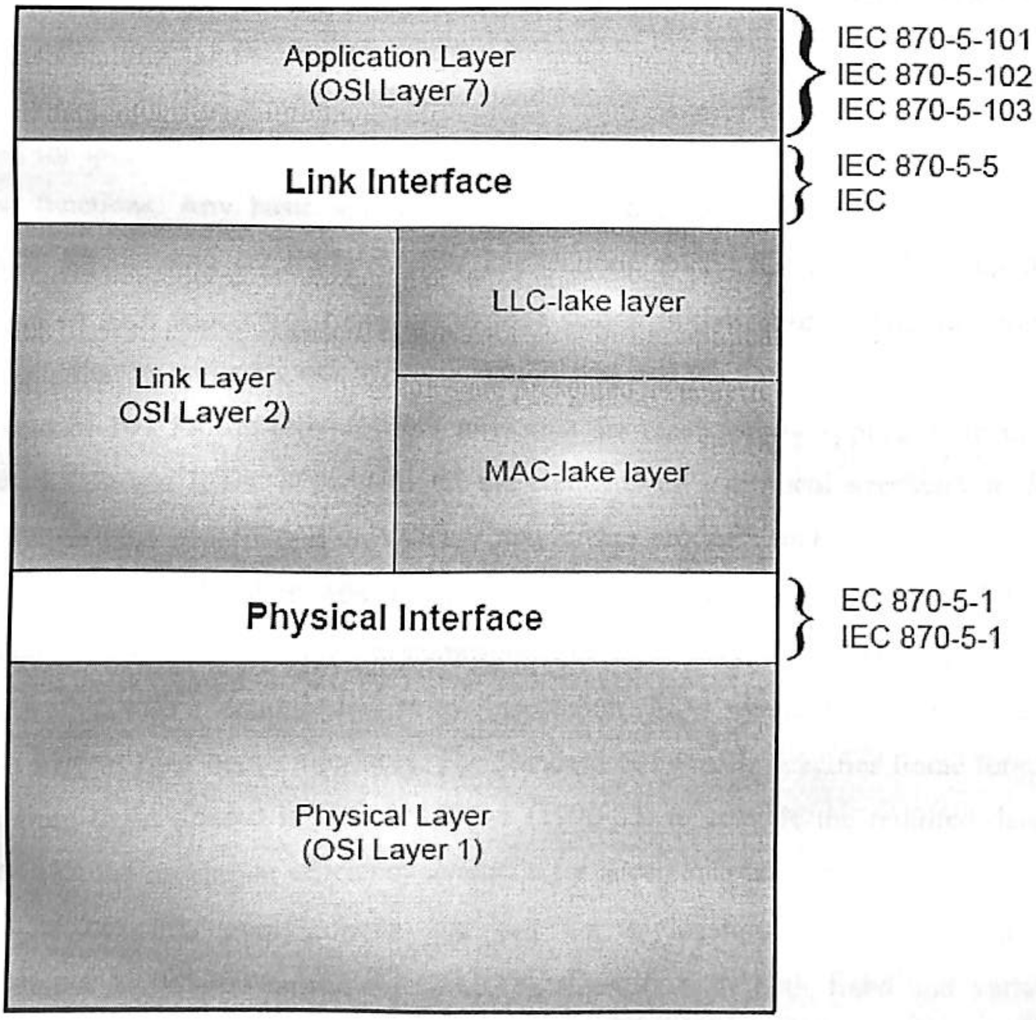


Figure 4.1: Enhanced Performance Architecture

Standards that may be used to support a great variety of present and future telecontrol applications. This section of IEC 60870-5 describes the general structure of application data and basic rules to specify application data units without specifying details about information fields and their contents

• IEC 60870-5-4 (1993-08) provides rules for defining information data elements and a common set of information elements, particularly digital and analog process variables that are frequently used in telecontrol applications.

• IEC 60870-5-5 (1995-06) defines basic application functions that perform standard procedures for telecontrol systems, which are procedures that reside beyond layer 7 (application layer) of the ISO reference model. These utilize standard services of the application layer. The specifications in IEC 60870-5-5 (1995-06) serve as basic standards for application profiles that are then created in detail for specific telecontrol tasks. Each application profile will use a specific selection of the defined functions. Any basic application functions not found in a standards document but necessary for defining certain telecontrol applications should be specified within the profile. Examples of such telecontrol functions include station initialization, cyclic data transmission, data acquisition by polling, clock synchronization, and station configuration.

The Standard 101 Profile provides structures that are also directly applicable to the interface between RTUs and IEDs. It contains all the elements of a protocol necessary to provide an unambiguous profile definition so vendors may create products that interoperate fully. At the physical layer, the Standard 101 Profile additionally allows the selection of International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) standards that are compatible with Electronic Industries Association (EIA) standards RS-2321 and RS-4852, and also support fiber optics interfaces. The Standard 101 Profile specifies frame format FT 1.2, chosen from those offered in IEC 60870-5-1 (1990-02) to provide the required data integrity together with the maximum efficiency available for acceptable convenience of implementation. FT 1.2 is basically asynchronous and can be implemented using standard Universal Asynchronous Receiver/Transmitters (UARTs). Formats with both fixed and variable block length are permitted.

At the data link layer, the Standard 101 Profile species whether an unbalanced (includes multi-drop) or balanced (includes point-to-point) transmission mode is used together with which link procedures (and corresponding link function codes) are to be used. Also specified is an unambiguous number (address) for each link. The link transmission procedures selected from IEC 60870-5-2 (1992-04) specify that SEND/NO REPLY, SEND/CONFIRM, and REQUEST/RESPOND message transactions should be supported as necessary for the functionality of the end device. Additionally,

1 Interface between Data Terminal Equipment

2 Electrical Characteristics of Generators and Receivers for Use in Balanced Digital Multipoint Systems the Standard 101 Profile defines the necessary rules for devices that will operate in the unbalanced (multi-drop) and balanced (point-to-point) transmission modes. The Standard 101 Profile defines appropriate Application Service Data Units (ASDUs) from a given general structure in IEC 60870-5-3 (1992-09). The sizes and the contents of individual information fields of ASDUs are specified according to the declaration rules for information elements defined in the document IEC 60870-5-4 (1993-08). Type information defines structure, type, and format for information object(s), and a set has been predefined for a number of information objects. The predefined information elements and type information do not preclude the addition by vendors of new information elements and types that follow the rules defined by IEC 60870-5-4 (1993-08) and the Standard 101 Profile. Information elements in the Standard 101 Profile have been defined for protection equipment, voltage regulators, and metered values to interface these devices as IEDs to the RTU.

The Standard 101 Profile utilizes the following basic application functions, defined in
IEC 60870-5-5 (1995-06), within the user layer:

a) Station initialization

b) Cyclic data transmission

c) General interrogation

d) Command transmission

e) Data acquisition by polling

f) Acquisition of events

g) Parameter loading

h) File transfer

i) Clock synchronization

j) Transmission of integrated totals

k) Test procedure

Finally, the Standard 101 Profile defines parameters that support interoperability among multi-vendor devises within a system. These parameters are defined in 60870-5-102 and 60870-5-105. [6] The Standard 101 Profile provides a checklist that vendors can use to describe their devices from a protocol perspective. These parameters include baud rate, common address of ASDU field length, link transmission procedure, basic application functions, etc., Also contained in the check list is the information that should be contained in the ASDU in both the control and monitor directions. This will assist the

SCADA engineers to configure their particular system. The Standard 101 Profile application layer specifies the structure of the ASDU, as shown in Figure 4.1. The fields indicated as being optional per system will be determined by a system level parameter shared by all devices in the system. For instance, the size of the common address of ASDU is determined by a fixed system parameter, in this case one or two octets (bytes).

The Standard 101 Profile also defines two new terms not found in the IEC 60870-5-1 through 60870-5 base documents. The control direction refers to transmission from the controlling station to a controlled station. The monitor direction is the direction of transmission from a controlled station to the controlling station. Figure 4.2 shows the structure of ASDUs as defined in the IEC 60870-5-101 specification.

4.2 DNP3

DNP 3 protocol mostly used in SCADA system, It is based on the three enhance architecture (EPA) model content in the IEC 60870-5 Stands with some alteration to meet additional information of the user.

We are using DNP 3 protocol because it provides required functions as given below.

1. DNP3 is a protocol for transmission of data from point A to point B using serial communications
2. DNP3 is specifically developed for inter-device communication involving SCADA RTUs, and provides for both RTU-to-IED and master-to-RTU/IED.
3. It is the protocol that fix well in the data acquisition.
4. It is design to work in wide area communication network.

DNP3 was developed with the following goals:

- *High data integrity.*

- *Flexible structure.*
- *Multiple applications.*
- *Minimized overhead.*
- *Open standard.*

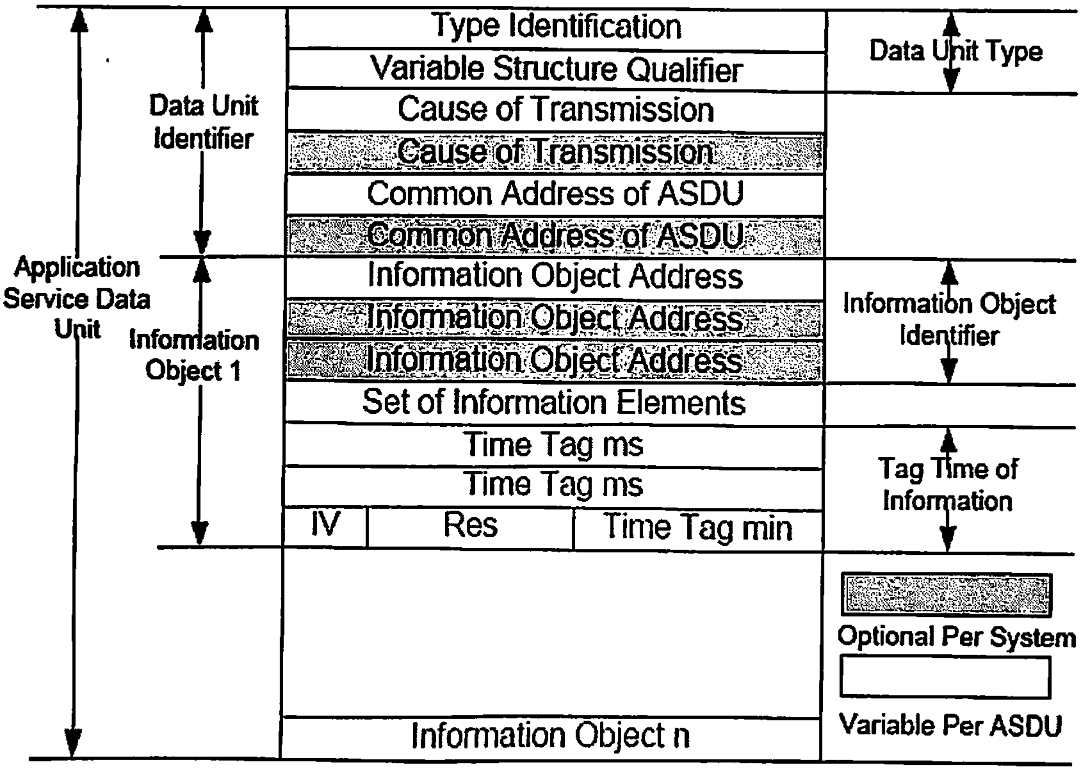


Figure 4.2: Structure of ADSUs in IEC 60870-5-101 (1995-11) [6]

The substation computer gathers data for transmission to the master such as:

• Binary input data that is useful to monitor two-state devices. For example, a circuit breaker is closed or tripped, or a pipeline pressure alarm shows normal or excessive.

• Analog input data that conveys voltages, currents, power, reservoir water levels and temperatures

• Count input data that reports kilowatt hours of energy

• Files that contain configuration data

The master station issues control commands that take the form of:

- Close or trip a circuit breaker, raise or lower a gate, and open or close a valve
- Analog output values to set a regulated pressure or set a desired voltage level

Other things the computers talk to each other about are synchronizing the time and date, sending historical or logged data, waveform data, etc. DNP3 was designed to optimize the transmission of data acquisition information and control commands from one computer to another. It is not a general purpose protocol for transmitting hypertext, multimedia or huge files. Figure 4.3 shows the client-server relationship and gives a simplistic view of the databases and software processes involved. The master or client is on the left side of Figure 4.3, and the slave or server is on the right side. A series of square blocks at the top of the server depicts its databases and output devices. The various data types are conceptually organized as arrays. An array of binary input values represents states of physical or logical Boolean devices. Values in the analog input array represent input quantities that the server measured or computed. An array of counters represents count values, such as kilowatt hours, that are ever increasing (until they reach a maximum and then roll over to zero and start counting again). Control outputs are organized into an array representing physical or logical on-off, raise-lower and trip-close points. Lastly, the array of analog outputs represents physical or logical analog quantities such as those used for set points.

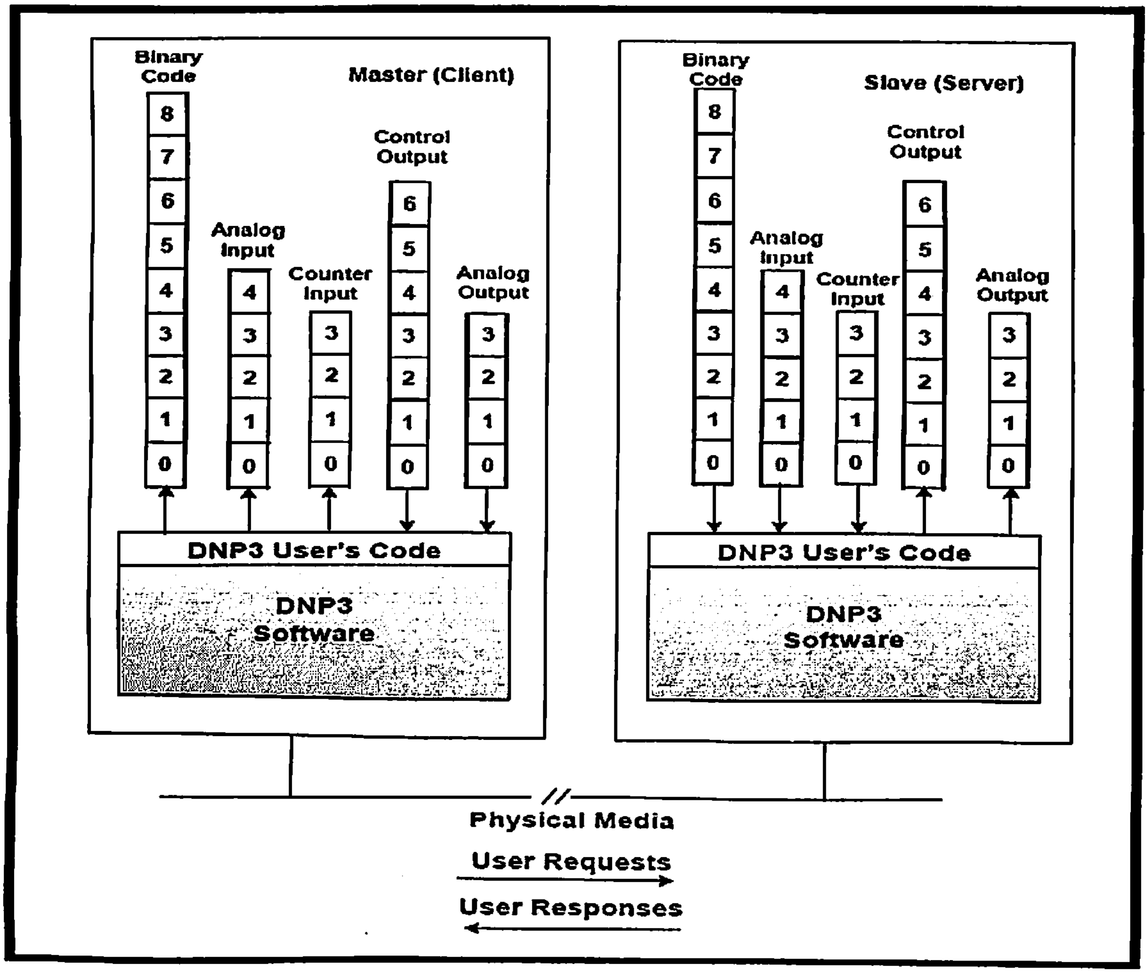


Figure 4.3: DNP3 Client Server Relationship [7]

The elements of the arrays are labeled 0 through N - 1 where N is the number of blocks shown for the respective data type. In DNP3 terminology, the element numbers are called the point indexes. Indexes are zero-based in DNP3, that is, the lowest element is always identified as zero (some protocols use 1-based indexing). Notice that the DNP3 client, or master, also has a similar database for the input data types (binary, analog and counter). The master, or client, uses values in its database for the specific purposes of displaying system states, closed-loop control, alarm notification, billing, etc. An objective of the client is to keep its database updated. It accomplishes this by sending requests to the server (slave) asking it to return the values in the server's database. This is termed polling. The server responds to the client's request by transmitting the contents of its database. Arrows are drawn at the bottom of Figure 4.1 showing the direction of the requests (toward the server) and the direction of the responses (toward the client). Later we will discuss systems whereby the slaves transmit responses without being asked.

The client and the server shown in Figure 4.3 each have two software layers. The top layer is the DNP3 user layer. In the client, it is the software that interacts between the databases and initiates the requests for the server's data. In the server, it is the software that fetches the requested data from the server's database for responding to client requests. It is interesting to note that if no physical separation of the client and server existed; eliminating the DNP3 might be possible by connecting these two upper layers together. However, since physical or possibly logical separation of the client and server exists, DNP3 software is placed at a lower level. The DNP3 user's code uses the DNP3 software for transmission of requests or responses to the matching DNP3 user's code at the other end. Data types and software layers will be discussed later in the report. However, it is important to first examine a few typical system architectures where DNP3 is used. Figure 4.4 shows common system architectures in use today. At the top is a simple one on- one system having one master station and one slave. The physical connection between the two is typically a dedicated or dial-up telephone line.

The second type of system is known as a multidrop design. One master station communicates with multiple slave devices. Conversations are typically between the client and one server at a time. The master requests data from the first slave, then moves onto the next slave for its data, and continually interrogates each slave in a round robin order. The communication media is a multi-dropped telephone line, fiber optic cable, or radio. Each slave can hear messages from the master and is only permitted to respond to messages addressed to it. Slaves may or may not be able to hear each other. In some multidrop forms, communications are peer-to-peer. A station may operate as a client for gathering information or sending commands to the server in another station. Then, it may change roles to become a server to another station.

The middle row in Figure 4.4 shows a hierarchical type system where the device in the middle is a server to the client at the left and is a client with respect to the server on the right. The middle device is often termed a sub-master. Both lines at the bottom of Figure 4.4 show data concentrator applications and protocol converters. A device may gather data from multiple servers on the right side of the figure and store this data in its database where it is retrievable by a master station client on the left side of the figure.

This design is often seen in substations where the data concentrator collects information from local intelligent devices for transmission to the master station. In recent years, several vendors have used Transport Control Protocol/Internet Protocol (TCP/IP) to transport DNP3 messages in lieu of the media discussed above.

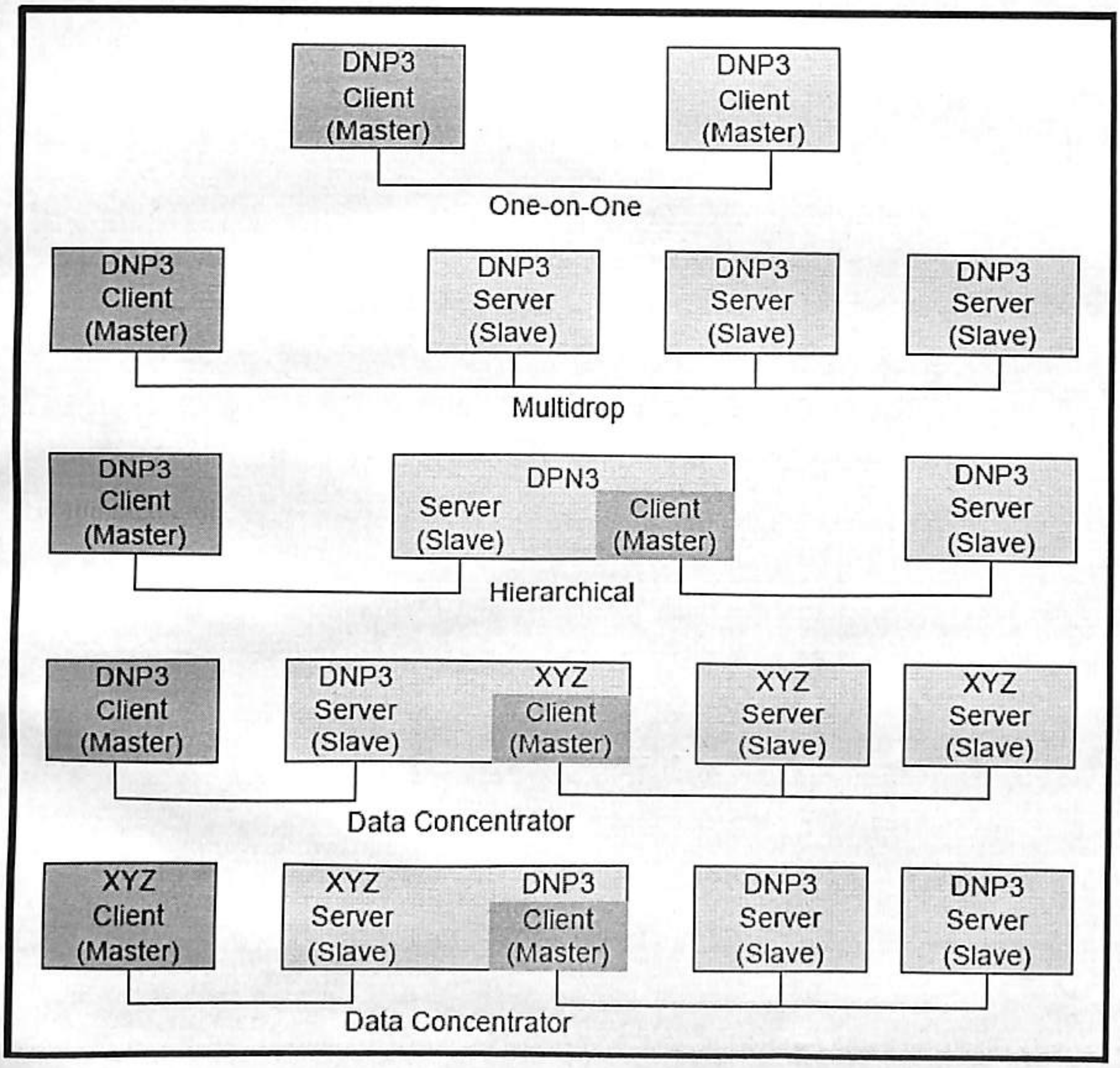


Figure 4.4: Common DNP3 Architectures in Use Today [7]

Link layer frames, which have not been discussed yet, are embedded into TCP/IP packets. This approach has enabled DNP3 to take advantage of Internet technology and permitted economical data collection and control between widely separated devices. Many communication circuits between the devices are susceptible to noise and signal distortion. The DNP3 software is layered to provide reliable data transmission and to affect an organized approach to the transmission of data and commands. Figure 4.5 shows the DNP3 architecture layers. The link layer has the responsibility of making the physical link reliable. It does this by providing error detection and duplicate frame detection. The link layer sends and receives packets, which in DNP3 terminology are called frames. Sometimes transmission of more than one frame is necessary to transport all of the information from one device to another. A DNP3 frame consists of a header and data section. The header specifies the frame size, which DNP3 station should receive the frame, which DNP3 device sent the frame, and data link control information. The data section is commonly called the payload and contains the data passed down from the layers above. Every frame begins with two sync bytes that help the receivers determine where the frame begins. The length specifies the number of octets in the remainder of the frame, not including Cyclical Redundancy Check (CRC) octets. The link control octet is used between sending and receiving link layers to coordinate their activities.

A destination address specifies which DNP3 device should process the data, and the source address identifies which DNP3 device sent the message. Having both destination and source addresses satisfies at least one requirement for peer-to-peer communications because the receiver knows where to direct its responses. Every DNP3 device must have a unique address within the collection of devices sending and receiving messages to and from each other. Three destination addresses are reserved by DNP3 to denote an all-call message; that is, all DNP3 devices should process the frame. Thirteen addresses are reserved for special needs in the future.

Receiver to confirm that the frame arrived. Using this feature is optional, and it is often not employed. It provides an extra degree of assurance of reliable communications. If a confirmation is not received, the link layer may retry the transmission. Some disadvantages are the extra time required for confirmation messages and waiting for multiple timeouts when retries are configured. It is the responsibility of the transport layer to break long messages into smaller frames sized for the link layer to transmit, or when receiving, to reassemble frames into the longer messages. In DNP3 the transport layer is incorporated into the application layer. The transport layer requires only a single octet within the message to do its work. Therefore, since the link layer can handle only 250 data octets, and one of those is used for the transport function, then each link layer frame can hold as many as 249 application layer octets. Application layer messages are broken into fragments. Fragment size is determined by the size of the receiving device's buffer. It normally falls between 2048 and 4096 bytes. A message that is larger than one fragment requires multiple fragments. Fragmenting messages is the responsibility of the application layer. Note that an application layer fragment of size 2048 must be broken into 9 frames by the transport layer, and a fragment size of 4096 needs 17 frames. The data payload in the link frame contains a pair of CRC octets for every 16 data octets. This provides a high degree of assurance that communication errors can be detected. The maximum number of octets in the data payload is 250, not including CRC octets. (The longest link layer frame is 292 octets if all the CRC and header octets are counted). One often hears the term "link layer confirmation" when DNP3 is discussed. A feature of DNP3's link layer is the ability of the transmitter of the frame to request the interestingly, it has been learned by experience that communications are sometimes more successful for systems operating in high noise environments if the fragment size is significantly reduced. The application layer works together with the transport and link layers to enable reliable communications. It provides standardized functions and data formatting with which the user layer above can interact. Before functions, data objects and variations can be discussed, the terms static, events and classes need to be covered.

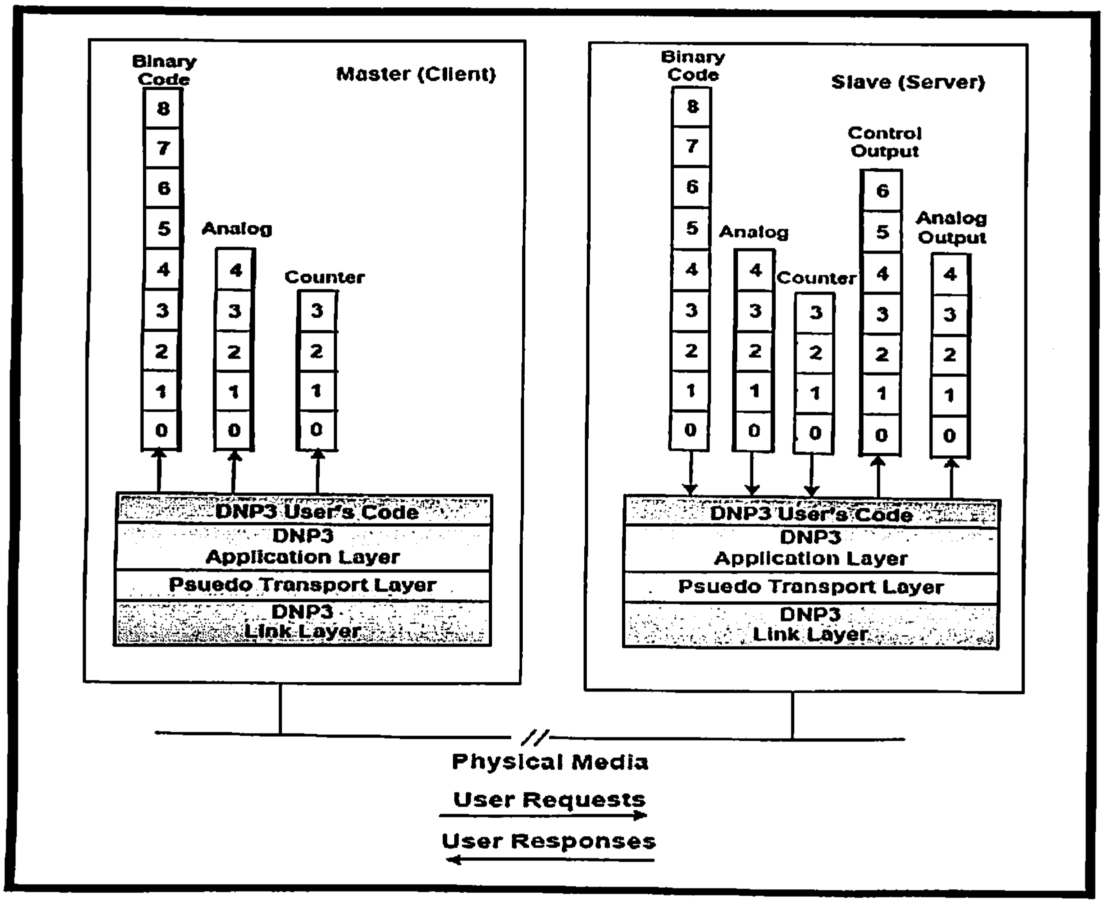


Figure 4.5: DNP3 Layers [8]

In DNP3, the term static is used with data and refers to the current value. Thus static binary input data refers to the present on or off state of a bi-state device. Static analog input data contains the value of an analog value at the instant it is transmitted. DNP3 allows a request for some or all of the static data stored in a slave device. DNP3 events are associated with something significant happening. Examples are state changes, values exceeding some threshold, snapshots of varying data, transient data and newly available information. An event occurs when a binary input changes from an "on" to an "off" state or when an analog value changes by more than its configured dead band limit. DNP3 provides the ability to report events with and without time stamps so that the client can generate a time sequence report. The user layer can direct DNP3 to request events. Usually, a client is updated more rapidly if it mostly polls for events from the server and only occasionally asks for static data as an integrity measure. The reason updates are faster is because the number of events generated between server interrogations is small and, therefore, less data must be returned to the client. DNP3 goes a step further by classifying events into three classes. When DNP3 was conceived, class 1 events were considered as having higher priority than class 2 events, and class 2 were higher than class 3 events. While that scheme can be still be configured, some DNP3 users have developed other strategies more favorable to their operation for assigning events into the classes. The user layer can request the application layer to poll for class 1, 2 or 3 events or any combination of them. DNP3 has provisions for representing data in different formats. Examination of analog data formats is helpful to understand the flexibility of DNP3. Static, current value, analog data can be represented by variation numbers as follows:

- A 32-bit integer value with flag
- A 16-bit integer value with flag
- A 32-bit integer value
- A 16-bit integer value
- A 32-bit floating point value with flag
- A 64-bit floating point value with flag

The flag referred to is a single octet with bit fields indicating whether the source is online, value contains are start value, communications are lost with the source, the data is forced and the value is over range. Not all DNP3 devices can transmit or interpret all six variations. DNP3 devices must be able to transmit the simplest variations so that any receiver can interpret the contents. Event analog data can be represented by these variations:

- A 32-bit integer value with flag
- A 16-bit integer value with flag
- A 32-bit integer value with flag and event time
- A 16-bit integer value with flag and event time
- A 32-bit floating point value with flag
- A 64-bit floating point value with flag
- A 32-bit floating point value with flag and event time
- A 32-bit floating point value with flag and event time

The flag has the same bit fields as the static variations.

It looks like a variation one or two analog events cannot be differentiated from a variation one or two static analog value. DNP3 solves this predicament by assigning object numbers. Static analog values are assigned as object 30, and event analog values are assigned as object 32. Static analog values, object 30, can be formatted in one of 6 variations, and event analog values, object 32, can be formatted in one of 8 variations. When a DNP3 server transmits a message containing response data, the message identifies the object number and variation of every value within the message. Object and variation numbers are also assigned for counters, binary inputs, controls and analog outputs. In fact, all valid data types and formats in DNP3 are identified by object and variation numbers. Defining the allowable objects and variations helps DNP3 assure interoperability between devices. DNP3's basic documentation contains a library of valid objects and their variations. The client's user layer formulates its request for data from the server by telling the application layer what function to perform, like reading, and specifying which objects it wants from the server. The request can specify how many objects it wants or it can specify specific objects or a range of objects from index number X through index number Y. The application layer then passes the request down through the transport layer to the link layer that, in turn, sends the message to the server. The link layer at the server checks the frames for errors and passes them up to the transport layer where the complete message is assembled in the server's application layer. The application layer then tells the user layer which objects and variations were requested. Responses work similarly, in that, the server's user layer fetches the desired data and presents it to the application layer that formats the data into objects and variations. Data is then passed downward, across the communication channel and upward to the client's application layer. Here the data objects are presented to the user layer in a form that is native to the client's database. One area that has not been covered yet is transmission of unsolicited messages. This is a mode of operating where the server spontaneously transmits a response, possibly containing data, without having received a specific request for the data. Not all servers have this capability, but those that do must be configured to operate in this mode. This mode is useful when the system has many slaves and the master requires notification as soon as possible after a change occurs. Rather than waiting for a master station polling cycle to get around to it, the slave simply transmits the change. To configure a system for unsolicited messages, a few basics need to be considered. First, spontaneous transmissions should generally occur infrequently, otherwise, too much contention can occur, and controlling media access via master station polling would be better. The second basic issue is that the server should have some way of knowing whether it can transmit without stepping on someone else's message in progress. DNP3 leaves specification of algorithms to the system implementer. One last area of discussion involves implementation levels. The DNP3 Users Group recognizes that supporting every feature of DNP3 is not necessary for every device. Some devices are limited in memory and speed and do not need specific features, while other devices must have the more advanced features to accomplish their task. DNP3 organizes complexity into three levels. At the lowest level, level 1, only very basic functions must be provided and all others are optional. Level 2 handles more functions, objects and variations, and level 3 is even more sophisticated. As a result only certain combinations of request formats and response formats are required. DNP3 is a protocol that fits well into the data acquisition world. It transports data as generic values, has a rich set of functions, and was designed to work in a wide area communications network. The standardized approach and public availability make DNP3 a protocol to be the standard for SCADA applications.

5.0 Deploying SCADA Systems

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. We will also look at their advantages and disadvantages.

5.1 Twisted-Pair Metallic Cable

Twisted-pair telecommunications cable is the most popular medium used by utilities and has existed in its present form for many years. The cables are essentially the same as those used by the Telephone Company and contain a number of pairs of conductor. Aerial cables would be more appropriate for installation in the utility's service area since the Utility may own a large number of distribution poles from which the cables could be suspended. The smallest aerial cables can be self-supporting, whereas large aerial cables have to be attached to supporting wires (messengers) by lashing wire. Table 5.1 shows the Twisted-Pair Cable advantages and disadvantages.

Advantages	Disadvantages
• No licensing, fewer approvals • Existing pole Infrastructure • Economical for short distances • Relatively high channel capacity (up to 1.54 MHz) for short distances	• Right-of-way clearance required for buried cable • Subject to breakage • Subject to water ingress • Subject to ground potential rise due to power faults and lightning • Failures may be difficult to pinpoint • Inflexible Network Configuration

Table 5.1: Twisted-Pair Advantages/Disadvantages [8]

5.2 Coaxial Metallic Cable

Coaxial cable is constructed of a center copper conductor, polyvinyl chloride (PVC) insulation, a braided or extruded copper shield surrounding the center conductor and PVC insulation, and a plastic jacket cover. Coaxial cable can transmit high frequency signals up to several MHz with low attenuation compared to twisted pair wires used for telephone service. Methods of installation used for existing systems in Europe and the

USA are underground, direct burial, overhead, and on existing power line structures.

Services usually supported are voice, data, and interoffice trunking. Table 5.2 shows the Coaxial Cable advantages and disadvantages.

Advantages	Disadvantages
• No licensing, fewer approvals • Existing pole Infrastructure • Economical for short distances • Higher channel capacity than Twisted-Pair Metallic • More immune to Radio Frequency (RF) noise interference the Twisted Pair Metallic	• Right-of-way clearance required for buried cable • Subject to breakage • Subject to water ingress • Subject to ground potential rise due to power faults and lightning • Failures may be difficult to pinpoint • Inflexible Network Configuration

Table 5.2: Coaxial Cable Advantages/Disadvantages [8]

5.3 Fiber Optic Cable

Fiber optic technology 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. Table 5.3 shows the Fiber Optic Cable advantages and disadvantages.

Advantages	Disadvantages
• Immune to electromagnetic interference	• Novel technology, i.e. new skills must be learned
• Immune to ground potential rise	• Expensive test equipment
• High channel capacity	• Inflexible network configuration
• Low operating cost	• Cable subject to breakage and water ingress
• No licensing requirement	

Table 5.3: Fiber Optic Cable Advantages/Disadvantages [8]

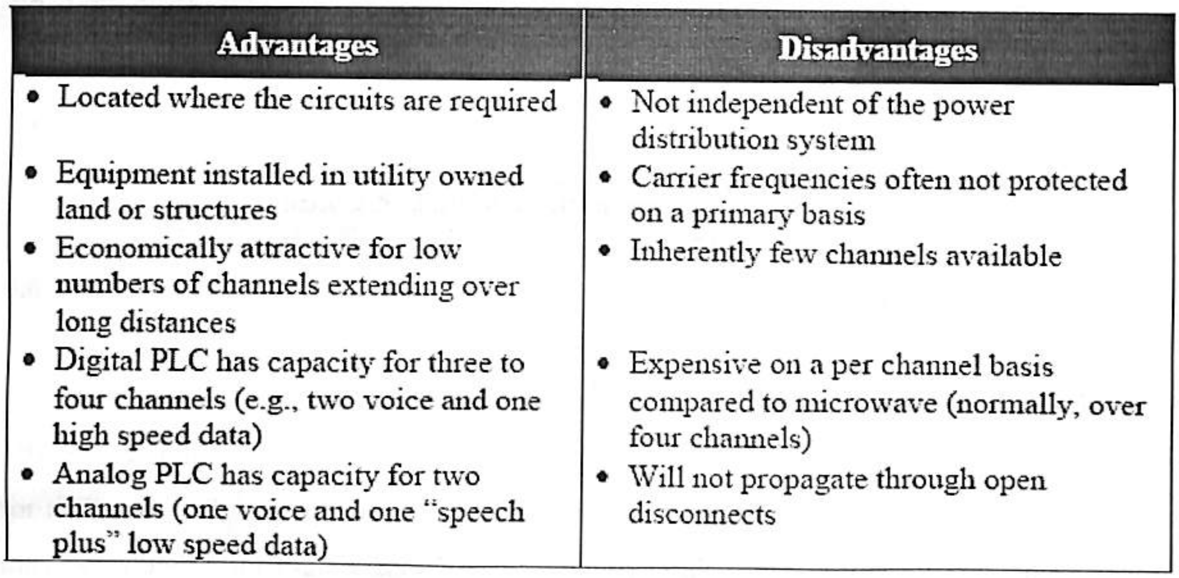
The cost per meter of fiber optic systems is expected to continually decrease. The cost of single mode fiber optic cables is now less than multimode fiber optic cable because of the increasing demand for single mode fiber. Conversely, the multimode fiber optic has limited distance and bandwidth characteristics. 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

5.4 Power Line Carrier

Power Line Carrier (PLC) was one of the first reliable communications media available to electric utilities for critical communications channels that could not be subjected to the intolerance and unreliability of leased (common carrier) telephone circuits. PLC uses the power transmission lines to transmit radio frequency signals in the range of 30 kHz to 500 kHz. The physical security of this communications is very high since the power line carrier equipment is located within the substations. PLC systems are used to provide voice, telemetry, SCADA, and relaying communications on portions of the 220/230 kV, 110/115 kV, or 66 kV interconnected power transmission network. Digital PLC technology is a relatively new technology. Power lines and their associated networks are not designed for communications use. They are hostile environments that make the accurate propagation of communication signals difficult. Two of the biggest problems faced in using power lines for communications are excessive noise levels and cable attenuation. Noise levels are often excessive, and cable attenuation at the frequencies of interest is often very large. The cost of PLC will probably increase at a greater rate than inflation because of decreasing demand. Communication transmission capacity of Single Side Band (SSB) PLC cannot be increased without purchasing a second or third PLC Radio Frequency (RF) channel at the same cost as original terminal equipment. Some cost can be saved by sharing dual frequency Traps, Line Tuning Units and coupling equipment. Digital PLC can be increased from one channel to three channels within the same RF bandwidth.

Table 5.4 shows the advantages and disadvantages.



Advantages	Disadvantages
• Located where the circuits are required	• Not independent of the power distribution system
• Equipment installed in utility owned land or structures	• Carrier frequencies often not protected on a primary basis
• Economically attractive for low numbers of channels extending over long distances	• Inherently few channels available
• Digital PLC has capacity for three to four channels (e.g., two voice and one high speed data)	• Expensive on a per channel basis compared to microwave (normally, over four channels)
• Analog PLC has capacity for two channels (one voice and one "speech plus" low speed data)	• Will not propagate through open disconnects

5.5 Satellites

The use of satellites has been investigated for a number of years. The satellites are positioned in geo-stationary orbits above the earth's equator and thus offer continuous coverage over a particular area of the earth. Satellites contain a number of radio transponders which receive and retransmit frequencies to ground stations within its "footprint," or coverage, on the earth's surface. A network facility on the ground tracks and controls the satellite. Earth stations are comprised of an antenna pointing at the satellite, a radio transceiver with a low-noise amplifier, and baseband equipment. Satellites use both the C-band and the Ku-band. Very Small Aperture Terminal (VSAT) technology has advanced to the point where a much smaller antenna (down to about one meter) can be used for Ku-band communications. This has resulted in the Ku-band being preferred for sites with modest communications requirements. VSAT technology is advancing steadily, and the capital costs have dropped substantially. Continual time-of use charges must be considered in the use of satellite communications. Developments in this area should be investigated when making a decision on the use of this technology.

Table 5.5 shows the Satellite system advantages and disadvantages.

Advantages	Disadvantages
• Wide area coverage	• Total dependency on a remote facility
• Easy Access to remote sites	• Less control over transmission
• Costs independent of distance	• Transmission time delay
• Low error rates	• Reduced transmission during solar equinox
• Adaptable to changing network patterns	• Continual leasing costs
• No right-of-way necessary, earth stations located at premises	

Table 5.5: Satellite Advantages/Disadvantages [8]

5.6 Leased Telephone Lines

Leased telephone circuits have long been used to meet communications needs. Most organizations use standard telephones connected to the Public Switched Network (PSN) for office communications and for routine voice traffic to stations. Leased dedicated circuits are used for dedicated communication requirements, such as telemetry and SCADA. Wideband channels may be available for high speed data signaling. Circuit characteristics can often be conditioned for many other uses, including voice and various types of low and medium speed data. Table 5.6 shows the Leased Circuit advantages and disadvantages.

Advantages	Disadvantages
• Small Capital Outlay	• Repair and maintenance is not controlled by the lessee
• Maintained circuit quality	• Circuits may not be available at some sites
• No communications expertise required	• Metallic links require protection against ground potential rise
• Adaptable to changing traffic patterns	• Continual leasing costs

Table 5.6: Leased Circuits Advantages/Disadvantages [8]

Practicaly we have two option for SCADA communication mediam optical fiber cable and satelite comminication.But we are using optical fiber cable due to some reasuns, following diffrence cleare the opinian for optical fibre cable .

Sr.no	Optical fiber cable	Satelite communication
1	Light beams are used to transmitt the data through cable.	High frequency radio signall sent through atmosphere and space.
2	Greater capacity , Data rates of hundreds of Gbps	Lesser capacity as compared to optical fiber cable.
3	Less distortion of signal, capable of high transmission rates	Must have unobstructed line of sight, signal highly susceptible to intervention
4	Expensive to purchase and install.	Avoids cost and effort to lay cable or wires; capable of high-speed transmission
5	Electromagnetic isolation, Greater repeater spacing.	Not Electromagnetic isolation.

6.0 SCADA IMPLIMENTATION AT GAS RESIVING STATION

At the gas resaving station mainly filtration skid, metering skid and pressure reduction or lead down skid, this facility are implemented now we will discuss them as above.

6.1 FILTRATION SKID

6.1.1 Filtration skid functionality

Each stream of filtration skid consists of one filter and its respective instrumentation. This filter separator filters out unwanted liquid/solid particles that may be with the process before feeding natural gas to the metering skid. The filter elements having filtration capacity of 5 microns and efficiency of 100% for solid >20 microns, 99.5% for solid > 15 micron and 99.5 % for liquid >15 micron. The discrete and analog signals from the various instruments installed on the skid are connected to the metering panel. The same signals are also repeated to SCADA.

6.1.2 Description of major equipment

The filtration line consist of the following major instruments, the detail description of the same is explained below.

Filtration skid equipment list

1. Manually operated Trunion mounted ball valves with limit switches at inlet.
2. Double chamber coalescing type filter separator
3. 2" Floating ball valves for inlet valve bypass for pressure equalization
4. 2" globe halves for inlet valve bypass for pressure equalization
5. Pressure gauge at inlet header and on filter separator
6. Temperature
7. Gauge at inlet header
8. Pressure transmitter at inlet header
9. Differential pressure transmitters across filter separator.
10. Pressure safety valve on filter separator
11. 2" Ball valve and 2" globe valve at filter drain point
12. Necessary junction boxes, cables, pneumatic ss-tubing duly installed

13. 2" Trunion mounted ball valve for filter cross over
14. 2" ball valve and 2" globe valve for venting

6.1.3 Filter separator

The FPFS series of filter separator is a multi-stage that provides optimal removal of both liquids and solids from a gas stream. As the contaminated gas passes through the filter separator it passes trough several distinct stages or regions. Each stages has a specific purpose and the cumulative effect provides a virtual contaminant free gas

The filter separator is a vertical filter with vane(FPFS W), the contaminated gas encounters a large inlet plenum which contains filter support tubes. The gas velocity reduces in the plenum and bulk separation of larger particles occurs due to gravity. Further separation occurs as a result of impingement of the contaminants on the labyrinth of tubes which results in convalescing into large particles which drop to the lower portion of the inlet chamber. In addition as the as tries to negotiate this maze of tubes a centrifugal force is imparted on the gas which removes solid and liquid particles down to 10 microns.

Next, the as passes through the filer elements. The solid particle are captured on the surface of the filter and I the depth of the filter media. The fine liquid particles flow through the element and coalesce with other liquid particles to form larger particles. These larger particles emerge from the final separation region. The filter elements are staggered to provide maximum filtering area and equal flow distribution across all filters. Finally the gas passes through the final separation chamber. This stage utilizes vane type separator elements which remove virtually all coalesced liquid flowing fro the filter separator elements. Vanes are mounted perpendicular to the as flow. In the vertical type contaminates are colleted in the main vessel itself out of the gas flow.

6.1.4 ISOLATION VALVE

One manually operated valve with limit switch is provided at the inlet of tee each filtration line. This valve is only operated after equalizing the pressure of both side of valve using equalizing the pressure at both side of valve using equalizing assembly consist of one 2" ball valve, one 2" globe valve and a restriction orifice. The limit switches gives the open/close positions of the valve. The valve status is indicated on station computer in control room and repeated to SCADA by interfacing it to an IS isolator located in control panel.

6.1.5 STREAM TRANSMITTER AND GAUGES

One pressure transmitter on the inlet header and one differential pressure transmitter on each filter will be provided for monitoring purpose. The output is fed to FC and repeated SCADA by interfacing it to an IS isolator located in control panel, their real time data will be available in FC, HMI will pickup those data from FC for Monitoring.

One temperature gauge will be provided on inlet header for local indication

One pressure gauge at inlet header and one pressure gauge on each filter provide local indication of pressure. A pressure safety valve, which is set at 94 barg, is installed on the filter unit. If pressure in the unit exceeds the set valve, the valve pops. The design is done as per API 520/526. It has 1" (inlet) x 2" (Outlet) connection to accommodate the flow.

6.2 METERING SKID AND COMPUTATIONAL SYSTEM

6.2.1 FUNCTIONALITY

Metering of the gas is done by means of ultrasonic flow meter. The inlet to the metering skid is from filtration skid. Flow capacity of each streams is 100% of the station capacity. Hence , at any point of time, any one stream shall be operating to achieve 100% station capacity with second available as standby. Changes over to second stream shall be manually in case the operating stream fails.

The dedicated flow computer per stream gathers on-line data from the field mounted instrumentation, performs corrections calculations and report the metering system product throughput. Additionally, process alarms are raised in the event that process conditions fall out side the operator determined limits.

The gas metering skid and computation system as a whole comprises of two major components

1. Field mounted metering equipment
2. Control Room metering mounted equipment

6.2.2 FIELD MOUNTED EQUIPMENT LIST

1. Senior Sonic Ultrasonic Meter.
2. Gas Chromatograph.
3. Meter-run as per P&ID.
4. Pressure transmitters for metering pressure measurement.
5. Temperature element (4 wire RTD) for metering temperature measurement along with Thermowell.
6. Temperature transmitter connected to temperature element.
7. Temperature gauge along with Thermowell.
8. 2" Ball valve Inlet bypass for pressure equalization.
9. 2" Globe valves inlet bypass for pressure equalization.
10. Gas over Oil Actuator valve at Inlet.
11. Trunion mounted ball valves with limit switch at Outlet.
12. Ball valve for cross over mode, verification operation.
13. Differential Pressure Gauge and Differential Pressure Switch across the Gas Over Oil Actuator.
14. Test Thermowell

6.2.3 CONTROL ROOM MOUNTED EQUIPMENT

1. Metering Panel consists of following major equipment
   a. Power Supply Units (230 V AC/ 110 V AC transformer)
   b. Flow Computer – FloBoss S600
   c. GC Controller – 2350A
   d. PID controller
   e. IS a barrier, repeaters, Relays, Converters etc.
2. Desktop PC as station computer and Printers.

DESCRIPTION OF MAJOR EQUIPMENT

6.2.4 FIELD MOUNTED EQUIPMENT

Ultrasonic meter:- Gas Flow meter.

The Gas Flow Meter measures the transit times of ultrasonic waves passing through the gas on four parallel planes to accurately determine the mean velocity of the gas flow through the meter. The four planes have been chosen to optimize the accuracy of the measurement regardless of the flow profile.

The four measurement paths are angled at 45° with respect to the pipe axis. Each path has two ultrasonic transducers acting alternately as transmitter and receiver. This permits the upstream and the downstream transit times to be measured. The transducers are mounted on the meter housing at defined locations, and the distances x and L are precisely determined during meter fabrication. These dimensions, along with a measurement of the electronic characteristics of each transducer pair, characterize the ultrasonic flow meter, which provides high accuracy and repeatability without the need for flow calibration!

The transit time for a signal travelling with the flow is less than the transit time when travelling against the flow. The differences in these transit times are used to calculate the flow's mean velocity. Since the equations are valid for gas flowing in either direction, the meter is inherently bi-directional. The final equation contains only the physical dimensions of the meter body and the transit times. The equation does not include the speed of sound in the flowing gas, therefore, the measurement of gas speed is independent of the factors which affect the speed of sound in the gas; i.e., temperature, pressure and composition.

FEATURES & ADVANTAGES OF THE GAS FLOW METER

- Unsurpassed measurement accuracy
- Field-proven reliability
- Extensive diagnostic and alarm system
- Unparalleled electronic interface
- PC laptop interface
- Modbus communications protocol
- Precision machining for high
- dimensional accuracy
- Intrinsically safe transducer design
- Proven and simple path configuration
- No line obstructions
- Low power consumption
- Sophisticated noise reduction

GAS OVER OIL ACTUATER (GOOA)

One Biffi make GOOA is provided on each metering stream inlet valve in the skid. The actuator is assembled to the inlet isolation valve. It consists of two open and two close limit switches. These limit switches are wired to S600 to know the status of the valve. S600 will send open and close command to it via digital signal. The pneumatic supply required for the actuator is provided from line. This pneumatic pressure acts on the hydraulic oil inside oil filled cylinder to generate required torque to operate the valve. A common pneumatic gas is diverted to the specific oil-cylinder to open or to close the valve depending on the command provided from Station Computer. However this actuator operation mode can be toggled between local / remote by means of Switch provided on it. This enables the user to operate the valve manually from the field itself using hand pump.

The actuator consists of following.

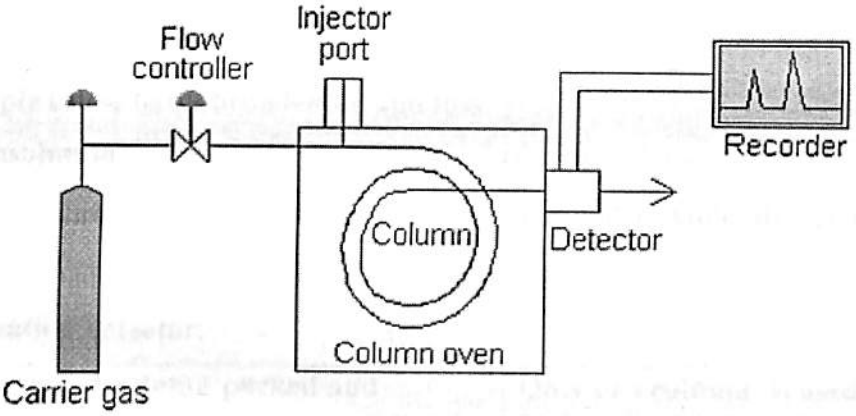
- Double Action Gas over oil cylinder
- Gas-Hydraulic tank

Chromatography:-

In the industries there are a number of different kinds of chromatography, which differ in the mobile and the stationary phase used.

- Paper Chromatography
- Column Chromatography
- Thin Layer Chromatography
- High Performance Liquid Chromatography
- Gas Chromatography

Gas chromatography - specifically gas-liquid chromatography - involves a sample being vaporized and injected onto the head of the chromatographic column. The sample is transported through the column by the flow of inert, gaseous mobile phase. The column itself contains a liquid stationary phase which is adsorbed onto the surface of an inert solid.



Two columns will fit inside the oven of our GCs. A heating element is used to raise the oven temperature, when desired, and thus raise the column temperature. GC columns typically have a metal identification tag clipped onto the column that lists column length and diameter, what material is inside, and the maximum operating temperature.

After components of the mixture move through the GC column, they reach a detector. Ideally, components of the mixture will reach the detector at varying times due to differences in the partitioning between mobile and stationary phases. The detector sends a signal to the chart recorder which results in a peak on the chart paper. The area of the peak is proportional to the number of molecules generating the signal.

Energy flow rate by the flow computers.

Basically in pipeline network two type of Chromatography will use

- Gas Chromatography
- High Performance Liquid Chromatography

But gas chromatography is the most use full type.

Difference between gas chromatography and high performance liquid chromatography.

Sr. no	Gas chromatography	High performance liquid chromatography
1	Find the gas concentration of gas component and calculate the calorific value	It is use to testing purpose like the drug and vitamin
2	We are use small sample because large sample cause band broadening and loss of resolution	Large sample will use
3	Two type of detector will use like thermal conductivity and flame ionization detector.	Only ultra violet detector will use
4	Two type of column packed and capillary are used for separation	Only one column is used that's why small amount is supplied
5	Moderate cost	This equipment is costly
6	This is a more volatile	This chromatography is less volatile
7	Carrier gas we are using is chemically inert with N2,He,and CO2	The carrier gas is not chemically inert

Carrier gas: He (common), N2, H2

Pinlet 10-50 psig

F=25-150 mL/min packed column

F=1-25 mL/min open tubular column

Column: 2-50 m coiled stainless steel/glass/Teflon

Oven: 0-400 °C ~ average boiling point of sample

Accurate to <1 °C

Detectors: FID, TCD, ECD, (MS)

Stream transmitters

Each metering stream consists of TT &PT for line temperature and pressure measurement.
A pressure transmitter is connected to pressure tap provided on the body of each USM. The transmitter
Provide metering line static pressure the TT is connected to a 4-wire RTD element mounted downstream of meter run. the TT provide line temp. These values are used for temperature and pressure composition in corrected flow calculation.
The transmitter are SMART type .the output is fed to FC by interfacing it to an IS isolator located in the control panel .metering pressure and temperature are made available to SCADA via analog output of flow computer .

6.3 Pressure Reduction Skid

6.3.1 Functionality

The pressure reduction skid is used primarily to control the outlet pressure. Inlet to the PRS is from the metering skid. This is achieved with two control valve mounted in series. The skid has one slam shut off valves, used for safety purpose. Its function is to close the stream if both the control valve fails and pressure at the outlet increases above its set point.

First is a monitor control valve to control the pressure in event of failure of second control valve which is active control valve. The active control valve normally controls pressure. This works as over as over ride control and at any point of time during operation, if flow increases above its set point, control valve will start controlling flow overriding its normal operation of pressure control.

6.3.2 Equipment List

1. Manually operated trunion mounted ball valves without limit switches.
2. Slam shut valve
3. Pressure control valve .
4. Pressure control valve with override flow control.
5. 2" floating ball valves with restriction orifice for inlet valve bypass for pressure equalization.
6. 2" globe valves ball for inlet valve bypass for pressure equalization.
7. Pressure gauges.
8. Temperature gauges.
9. Pressure transmitters.
10. Temperature Transmitter.

Description of major equipment

6.3.3 Slam shut valve (SSV)

It has automatic internal bypass mechanism which balances the pressure on both sides of the plug. The valve re-opening can be made only through a manual operation.

6.3.4 Pressure control valve

Pressure control valve is controlled by the dedicated PID controller The pressure set point will be given through station computer or by front keypad. The properly tuned controller will actuate the valve accordingly.

6.3.5 Pressure/flow control valve (active)

The flow control valve is controlled by PID of the flow computer. The pressure/flow set point is given to flow computer through station computer as well as keypad of flow computer.

6.3.6 Stream transmitter and gauges

Two pressure transmitters are provided at outlet of the PRS. Each pressure transmitter is dedicated to each control valve. A temperature transmitter is provided at the outlet of the PRS. These temperature transmitters are installed with a 4-wire RTD. The transmitters are SMART type. The output is fed to FC, HMI will pickup those data from FC and display for monitoring. One out of two PT and TT signals are also made available to SCADA by interfacing it to an IS isolator in the control panel.

Pressure gauges are provided at each stage of pressure reduction and temperature gauges are provided at upstream and downstream of each stream.

6.4 Flow Computer

The Flow Computer is a panel-mount flow computer designed specifically for hydrocarbon liquid and gas measurement where versatility and accuracy matter. The standard features of the unit make it ideal for fiscal measurement, custody transfer, batch loading and meter proving applications. The unit allows you to simultaneously meter liquids and gases by configuring multi-meter runs and multi-station applications.

The Flow Computer is designed for use either as a stand-alone flow computer or as a system component. The intelligent I/O boards fit both gas and liquid applications and support two meter runs and a header. Adding I/O boards (maximum 3) allows you to configure up to ten meter runs and two headers. Orifice, ultrasonic, turbine, positive displacement, coriolis, annubar and V-Cone flow meter types are all supported.

The uses distributed processing to achieve maximum performance. The main CPU incorporates a hardware floating point processor. Each additional card also has local processing to convert input and output from engineering units to field values and vice-versa, as well as running background tests and PID loops.

All metering calculations are performed using 64 bit (double) precision floating point numbers for the highest accuracy. Cumulative totals are stored in three separate memory locations (Tri-reg format) for maximum integrity. The Logicalc™ user language also allows double precision mathematical functions to be performed on the database objects.

The Flow Computer offers multiple communication interfaces:

One LAN port for Ethernet 10 baseT connectivity using TCP/IP protocol, an optional second Ethernet port can be added if required

HART communication is facilitated by way of a 12 channel I/O board, point-to-point and multi-drop architectures are supported (up to 50 transmitters)

An embedded web-server allows remote access to the flow computer. Security is provided by way of user name and password protection with a detailed event log for audit purposes. Supports Windows® Internet

Explorer® version 5 or greater

Two EIA-232 (RS-232) serial ports for connection to a printer or RTU

Three EIA-422/485 (RS-422/RS485) serial ports (up to 57600 bps baud) for connection to a Modbus SCADA data network or DCS Supervisory System

One dedicated configuration port for connection to the Daniel Config 600™ software

Configuration can be set through the keypad interface, the Config 600 Lite software interface, or the Config 600 Professional software interface. The Config 600 Lite and Config 600 Professional interfaces allow both download of new or modified configurations and upload of existing configuration from the Daniel S600. The keypad interface consists of a backlit LCD display, 29-button keypad, and an alarm status LED. The Flow Computer provides the following functions through the Config 600 configuration tool:

- Meter run and station totalization
- Batch totalization and correction
- 3-term PID control
- Flow balancing
- Flow scheduling
- Automatic proving sequence
- K factor linearization
- Valve monitor/control
- Sampler control
- Station densitometer
- Station gas chromatograph
- Forward, reverse and error totals

- Comprehensive maintenance mode Refer to Config 600 Configuration Software Data Sheet
  (DAN-LIQ-C600-DS-0306)

6.4.1 Functions:

- Batch totalization and correction
- Meter run and station totalization
- 3 term PID control
- Two stations and up to ten meter runs
- (depends on hardware configuration)
- Flow balancing
- Flow scheduling
- A utomatic prove sequence
- Meter factor linearization
- V alve monitor/control
- Sampler control

6.4.2 SPECIFICATIONS

I/O Capability:

- Analog Inputs: 0 to 5.2 V dc or 0 to 22 mA,>16 bits
- Analog Outputs: 0 to 21 mA, 12 bit minimum.
- 4-Wire RTD: PT100 (-100 to 200°C)
- Digital Input: 30 V max optically isolated
- Digital Output: Open Collector, 36 V max, 100mA
- Single or Dual Pulse Inputs: DC to 10 KHz, IP252/76, ISO 6551:1996, and API Chapter 5.5
  Level A, B or E
- Pulse Outputs: Open Collector, DC to 100 Hz
- Prover Pulse Bus: Open Collector, DC to 5 KHz
- Detector Switches: Supports 2 or 4 switchmode
- Small Volume Prover
- Optical Deflector Switches

- **Frequency Input:** DC to 10 KHz, 3 V P/P

CPU Capability:

- 50 MHz i80486DX2. 16 MB DRAM
- 1 MB SRAM (Battery Backed). 4 MB Flash
- Form 'C' Watchdog Relay
- Real-time Operating System Windriver VxWorks

Calculations:

- **Gas:** AGA 3, AGA 5, AGA 7, AGA 8, AGA 10,ISO 5167, ISO 6976, NX 19, SGERG, GPA
  2172 & 2145, PTZ, GOST 8.563.1 & 2 (97
- **Liquid:** API 2540, API 11 -2-1, API 11 -2-2
- Prover: Uni-directional, Bi-directional, Small
  Volume Provers, Master Meter, Dual Chronometry. Up to 4 sphere switch

Operating:

- **Operating Temperature:** 0 to 60°C (32°F to 40°F)
- **Storage Temperature:** -40 to 70°C (-40°F to158°F)
- **Operating Humidity:** To 90% non condensing
- **Weight:** 4.3 kg. (9.8 lbs.)

Input /output

The flow computer has the following hardwired I/O signals

- ➢ Stream pressure input from filtration skid(4-20 mA)
- ➢ Differential pressure input across filter (4-20 mA)
- ➢ Inlet valve open/close status from filtration skid (digital input)
- ➢ Stream pressure input from metering skid (4-20 mA)
- ➢ Stream temperature input from metering skid (4-20 mA)
- ➢ Stream pressure output from metering skid (4-20 mA)
- ➢ Stream temperature output from metering skid (4-20 mA)
- ➢ Standard volume flowrate output from metering skid (4-20 mA)
- ➢ Inlet valve open/close status from metering skid (Digital input)
- ➢ Inlet valve GODA open/close command to metering skid (Digital output)

- Outlet valve open/close status from metering skid(digital input)
- SSV open/close status from PRS (Digital input)
- Flow control valve output to PRS flow control valve (4-20 mA)
- Flow control valve feedback from PRS flow control valves (4-20 mA)
- Stream temperature input from PRS (4-20 mA)
- Stream pressure input from PRS (4-20 mA)

Signals from PRS and filtration skid will be only for display purpose, it will be mot utilized in metering system calculation.

6.4.3 Flow computer communication interface

Device	Setting
To USM Flow Meter	Serial RS485 link on Com Port 5 Modbus ASCII 9600,1, Even, Device Address 32
To Gas Chromatograph	Serial RS232 link on Com Port 4 Modbus ASCII 9600,8,1, None
To RTU/SCADA	Serial RS 485 link on COM port 6. Read only port for monitoring of metering data.
Station computer-HMI	Ethernet port with IP address 192.168.101.10 Modbus TCP, Port No 502

6.4.4 Mode of operation

During normal operation the flow computer is automatically set to one of the following modes:

ON-LINE: On-line is when the observed flow rate value is above he low flow cut-off.

OFF-LINE: Off-line is when the observed valve is below the flow cut-off.

MAINTENANCE: Maintenance mode is typically used when calculation checks or associated calibration tests are required to be carried out.

Many objects within the flow computer have operational behavior associated with them.

These can be segregated in two types:

1. Active Object
2. Passive Object

Active and passive both objects have mode option associated with them, the modes are explained below.

MEASURED: The in-use value is derived from transmitter input

CALCULATED: The in-use value is derived from the calculation done in FC

LIVE: This mode is specifically associated with GC; the in-use composition will be derived from the data received from GC.

KEYPAD: the in-use value is an operator-entered KEYPAD value

KEYPAD: if measured value fails and go in to alarm mode the in-use value considers KEYPAD value automatically. If transmitter becomes normal it will again start considering MEASURED value as in-use.x

6.4.5 Stream pressure / flow control loop (PID)

PID control loop available in S600 will be used to control Active valve of Pressure Reduction Skid. The active control valve in the PRS should control pressure as per set-point in normal operation and should start controlling flow if flow rate goes beyond set limit. To accomplish this operation, two set points will be provided one will be pressure set-point value and second will be flow rate set-point value. Switching flow rate will be provided to define the switching point of the PID loop from pressure to flow control. If flow rate set point will be less then switching flow rate, an alarm will be raised.

The PID control loop can be operated in two different modes,

1. Manual and 2. Auto

Switching between both modes and its operations is possible from Flow computer. In manual mode of operation, user/operator to keys in value, in percentage, for 'FCV Manual Position' and flow control valve will be opened to the set valve position. The process set point is not used in this mode of operation. If the set point tracking option is enabled, then in Manual mode of operation set point always remains equal to the measurement value. This feature is in the stream flow computer that helps to achieve bumps less transfer from Manual to Auto mode.

In Auto mode of operation, PID control module will adjust the flow control valve output as per the error signal (set point - measurement) and tries to control the flow rate nearest to the flow set point value.

The following values will be available to operator from S600 as well as station computer.

PID setting

Pressure set-point

Flow rate set-point

Switching flow rate

Auto/Manual mode selection

Manual % opening

6.4.6 Alarm and event handling

Alarm handling

By default, the alarms are categorized into 3 alarm groups shown below. These alarms are representative of the alarms raised by the flow computer. All object mentioned in section 7.5 have alarms associated with them; those alarms are listed in the explanation below.

Computer Alarms

Detailed below is a list of the computer alarms that are not specifically related to the devices or configurable tasks:

No.	Alarm	Description
1.	Cold Start	The S600 has performed a cold start.
2.	Warm Start	The S600 has performed a warm start.
3.	Battery Fail	The battery voltage detected is below 2.8V; the battery should be replaced.
4.	Ram Fail	The CRC of a data module in RAM is incorrect.
5.	Rom Fail	The CRC of a data module in ROM is incorrect.
6.	Reset Required	An error has occurred which requires the flow computer totals to be reset.
7.	Tots Rollover	A totals rollover has occurred.

Event handling

These alarms usually refer to failures of the I/O devices.

No.	Alarm	Description
1.	USM Rx Fail	Communication failure with USM
2.	USM Err	USM VOG/VOS hi & Fatal cord, Cord fail alarm
3.	Temp Dev Err	Input signal has fallen below 3.5mA or has exceeded 20.5 mA.
4.	Press Dev Err	Input signal has fallen below 3.5mA or has exceeded 20.5mA
5.	GC Rx Fail	Communication failure with GC
6.	Press Dev Err	Input signal has fallen below 3.5mA or has exceeded 20.5mA

6.4.7 Units of measurment

Units of measurement are as follows:

Parameter	Gas	Rollover	Decimal places
Static pressure	Kg/cm2g	-	2
Temperature	^{0}C	-	2
Density	Kg/m^3	-	4
Gross volume flow rate	m3/Hr	-	2
Standard volume flow rate	Sm3/Hr	-	2
Energy flow rate	GJ/Hr	-	2
Mass flow rate	ton/Hr	-	2
Calorific value	GJ/Sm3	-	3
Gross volume total	m3	10	2
Net volume total	Sm3	10	2

Parameter	Gas	Rollover	Decimal places
Energy to'al	GJ	12	2
Mass	Tones	12	2

6.4.8 Totalization

The primary flow measurement is uncorrected volumetric flow rate that is derived from the USM data. The standard volume flow rates are derived from uncorrected volumetric flow rate.

Each total is held as two discrete values, a displayed total and a remainder. Increments are added into the remainder and are only added into the displayed total when the remainder overflows.

The displayed total is truncated, i.e. not rounded up.

e.g.:	Actual Total	=	10.57382
	Displayed Total	=	10.5
	Remainder	=	0.07382

The value of each total is held in triple registers for increased security. The displayed total and the remainder are held in discrete registers. A total of six registers are used in order to hold the value of each total.

A partial total fail alarm is raised if the value held in one register differs from the other two associated registers. A total fail alarm is raised if the values held in each of the three associated registers differ.

The cumulative total represents the quantity of the relevant parameter that has been registered by the flow computer since its totals were last reset excluding any amount, which has passed whilst the flow computer has been put in maintenance mode.

The hourly total represents the quantity of the relevant parameter that has been registered by the computer since the last hour end occurred excluding any amount, which has passed whilst the flow computer has been put in maintenance mode.

The previous hourly total represents the quantity of the relevant parameter that has been registered by the computer until the next hour end is passed, excluding any amount, which has passed whilst the flow computer has been put in maintenance mode.

The daily total represents the quantity of the relevant parameter that has been registered by the computer since the last day end occurred, excluding any amount, which has passed whilst the flow computer has been put in maintenance mode.

The previous daily total represents the quantity of the relevant parameter that was registered by the computer between the last day end and the last but one day end, excluding any amount which has passed whilst the flow computer has been put in maintenance mode.

End of Day

A day is deemed to have ended when the flow computer time clock passes the associated base time, where the base time is the hour allocated (0 - 23) to determine when, for metering purposes, one day finishes and the next day commences.

This system will be configured for Base time end of day at 06:00 hrs.

At day end the current daily displayed total is copied into the previous day displayed total and the current daily displayed total is reset to zero. It should be noted that the associated current daily remainder (which is not displayed) would remain unchanged.

The following example shows the transfer of totals over a five-day period; the values shown are those recorded just after the relevant base times.

Period	Sum of daily increments	Cumulative Total		Daily Total	Previous period total
		DISPLAYED	REMAINDER		
1	10.57382	10.5	0.07382	10.6	0.0
2	11.66431	22.2	0.03813	11.7	10.6
3	7.14692	29.3	0.08505	7.1	11.7
4	8.1903	37.5	0.07535	8.2	7.1
5	9.99999	47.5	0.07534	10.0	8.2

Display Resolution

The maximum number of characters available in order to display a total is 10, 9 if a decimal point is utilized.

The resolution selected for each cumulative total should be such that the time interval between rollovers of each total, when operating at maximum flow rate (i.e. relevant flow rate Hi Limit) is greater than three calendar months.

The cumulative total continues to increase until an additional increment produces a total, which cannot be displayed within the relevant total resolution. At this time a total "ROLLOVER" will occur, an example of which is given below.

Rollover example of a total with a resolution of seven digits before the decimal point and one digit after the decimal point is as follows.

Current Total (Pre-Rollover)	9999998.6
Increment	3.2
Actual Total (If No Rollover)	10000001.8
Displayed Total (With Rollover)	1.8

Following rollover of a total an associated printout shall be generated.

Totals Reset

A 'totals reset' will reset all totals and therefore this function should be treated with extreme caution. The totals may be reset by selecting 'totals reset' from the front panel, or when initiating a 'cold start'. However, 'totals reset' and 'cold start' require the user to enter a password with the proper security level to execute. Thus accidental reset is not possible.

Display layout

The following is representative of the data that will be available as a minimum on th front panel of the flow computer. The actual displays will be available when configuratio of the computers is completed

Display Item	Parameters	Units
Mass Total	Cumulative	Tons
Mass Flowrate		Ton/Hr
Std Vol Total	Cumulative	m3
Std Vol Flowrate		m3/Hr
Energy Total	Cumulative	GJ
Energy Flowrate		GJ/Hr
Gross Vol Total	Cumulative	Sm3
Gross Vol Flowrate		Sm3/Hr
Stream Temperature	Downstream	°C
Stream Pressure	Downstream	Kg/cm2g
Standard Compressibility	In-use, calc and keypad	-

6.4.9 Report system

The following report can be configured in the S600

1. Current report
2. Hourly Report
3. Daily Report
4. Weekly Report
5. Monthly Report

Base time for the report will be as here under.

Day Start: 06:00:00.

Week Start: Sunday.

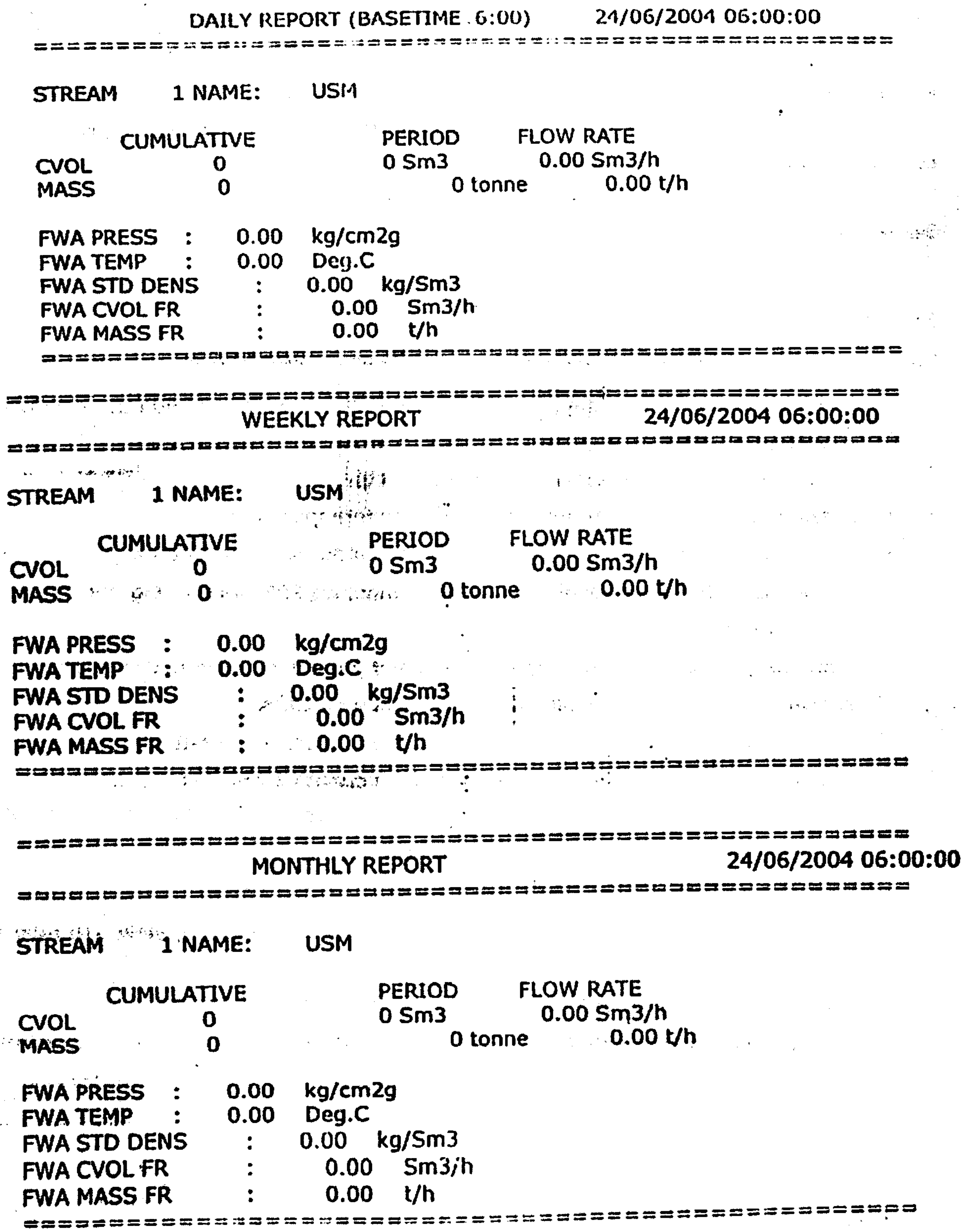
Month Start: 1st of the month.

6.4.10 Typical report format

These report formats are flow computer standard & cannot be customised)

Below is the typical report format which will be made project specific after getting input from customer. The format below may change as per their requirement, which they need to specify at design time.

```
==================================================================
                                  CURRENT REPORT         24/06/2004 12:00:00
==================================================================
STREAM       1 NAME:        FT-1001

           CUMULATIVE                 FLOW RATE
MASS                 0 ton            0.00 t/h
CVOL                 0  Sm3           0.00 Sm3/h

INUSE PRESS          :     0.00   Kg/cm2g
INUSE TEMP   :     0.00    Deg.C
INUSE STD DENS:      0.00     kg/Sm3

==================================================================

==================================================================
HOURLY REPORT (BASETIME  6:00)        24/06/2004 06:00:00
==================================================================

STREAM     1 NAME:        USM

           CUMULATIVE                 PERIOD       FLOW RATE
CVOL                 0                0 Sm3          0.00 Sm3/h
MASS                 0                     0 ton          0.00 t/h

FWA PRESS    :      0.00    kg/cm2g
FWA TEMP     :      0.00    Deg.C
FWA STD DENS       :      0.00    kg/Sm3
FWA CVOL FR ,      :        0.00    Sm3/h
FWA MASS FR        :        0.00    t/h

==================================================================
```



```
              DAILY REPORT (BASETIME 6:00)        24/06/2004 06:00:00
=====================================================================

STREAM      1 NAME:      USM

          CUMULATIVE              PERIOD       FLOW RATE
CVOL              0               0 Sm3         0.00 Sm3/h
MASS              0                    0 tonne        0.00 t/h

FWA PRESS     :     0.00    kg/cm2g
FWA TEMP      :     0.00    Deg.C
FWA STD DENS        :    0.00    kg/Sm3
FWA CVOL FR         :       0.00    Sm3/h
FWA MASS FR         :       0.00    t/h
=====================================================================

=====================================================================
                WEEKLY REPORT                   24/06/2004 06:00:00
=====================================================================

STREAM      1 NAME:      USM

          CUMULATIVE              PERIOD       FLOW RATE
CVOL              0               0 Sm3         0.00 Sm3/h
MASS              0                    0 tonne        0.00 t/h

FWA PRESS     :     0.00    kg/cm2g
FWA TEMP      :     0.00    Deg.C
FWA STD DENS        :    0.00    kg/Sm3
FWA CVOL FR         :       0.00    Sm3/h
FWA MASS FR         :       0.00    t/h
=====================================================================

=====================================================================
                MONTHLY REPORT                      24/06/2004 06:00:00
=====================================================================

STREAM      1 NAME:      USM

          CUMULATIVE              PERIOD       FLOW RATE
CVOL              0               0 Sm3         0.00 Sm3/h
MASS              0                    0 tonne        0.00 t/h

FWA PRESS     :     0.00    kg/cm2g
FWA TEMP      :     0.00    Deg.C
FWA STD DENS        :    0.00    kg/Sm3
FWA CVOL FR         :       0.00    Sm3/h
FWA MASS FR         :       0.00    t/h
=====================================================================
```

6.4.11 Station computer communication interface

Station computer shall have the following type of communications with its peripherals.

Device	Settings
Flow Computer # 1	TCP/IP Ethernet Link via Ethernet Switch on TCP/IP Address 192.168.101.1, Port 502, Modbus TCP
Flow Computer # 2	TCP/IP Ethernet Link via Ethernet Switch on TCP/IP Address 192.168.101.2, Port 502, Modbus TCP
PID Controller # 1	RS 485 link via PCI RS485 Card COM 2 Modbus RTU, 9600,8,1,Even, Device Address 1
PID Controller # 2	RS 485 link via PCI RS485 Card COM 3 Modbus RTU, 9600,8,1,Even, Device Address 2
Printer	Parallel Port
OPC Connectivity	Read only connectivity for monitoring data available in SC.

Data storage

As standard the system provides long term historical archiving as follows:

- As each alarm is raised and cleared, the alarm is added to an Alarm historian.
- The SC system also stores all automatic reports (Current, Hourly, Daily, Weekly, Monthly and Verification reports) and historical trend data on the hard disk. These reports format archived as binary files for security purpose. It should be noted that all reports can be only viewed on SC.

6.4.12 Security level for station computer

Password security

At the lowest security level all screens can be recalled and the data displayed. No password entry is required to display data. The default level is guest entry level. For data modification and system configuration, four password levels are provided. These password levels are as follows,

Level 0 Guest

Level 1 Operator entry level

Level 2 Engineer entry level

Level 3 Administrator entry level

Each operator entry field has a password level assigned to it. This means that this password level has to be enabled before the data field can be modified. The password level associated with each data field can be configured by the user under level 3 security. When a data item is to be enterd if the password is not enabled, the appropriate password level is requested. Once the password is enabled, data modification can be made for all fields with this password level or lower.

Level 0-Guest (default)

This security level allows the following special functions:-

View all data

Print the reports

Level 1-Operator entry level

This security level allows the following special functions:-

All functions associated with level 0

Alarm acknowledgement

Configure trend displays and process item tag names

Data modification i.e. High /low limit, keypad, modes etc.

Valve operation (open/close)

Level 2- Engineer entry level

This security level allows the following special functions:-

All functions associated with level 1

Report archiving into CD-R/CD-RW

Shut down supervisory computer.

Level 3 Administrator entry level

This security level allows the following special functions:-

All functions associated with level 1

Modifications of passwords

Software configuration and VBA scripting

LOG-IN and LOG-OUT

Password entry

On an attempt being made to modify any data and no password entry screen is presented in addition the password can be entered at any time by left clicking on the Log On/Off push button on the left of the display. This will present the password entry prompt.

The password can be any combination of up to 10 alpha/numeric characters. It should be noted that the password entry is case sensitive.

Modification of password

Under security manager the security/password modification screen is presented. This allows modification of the password for level 3 and below.

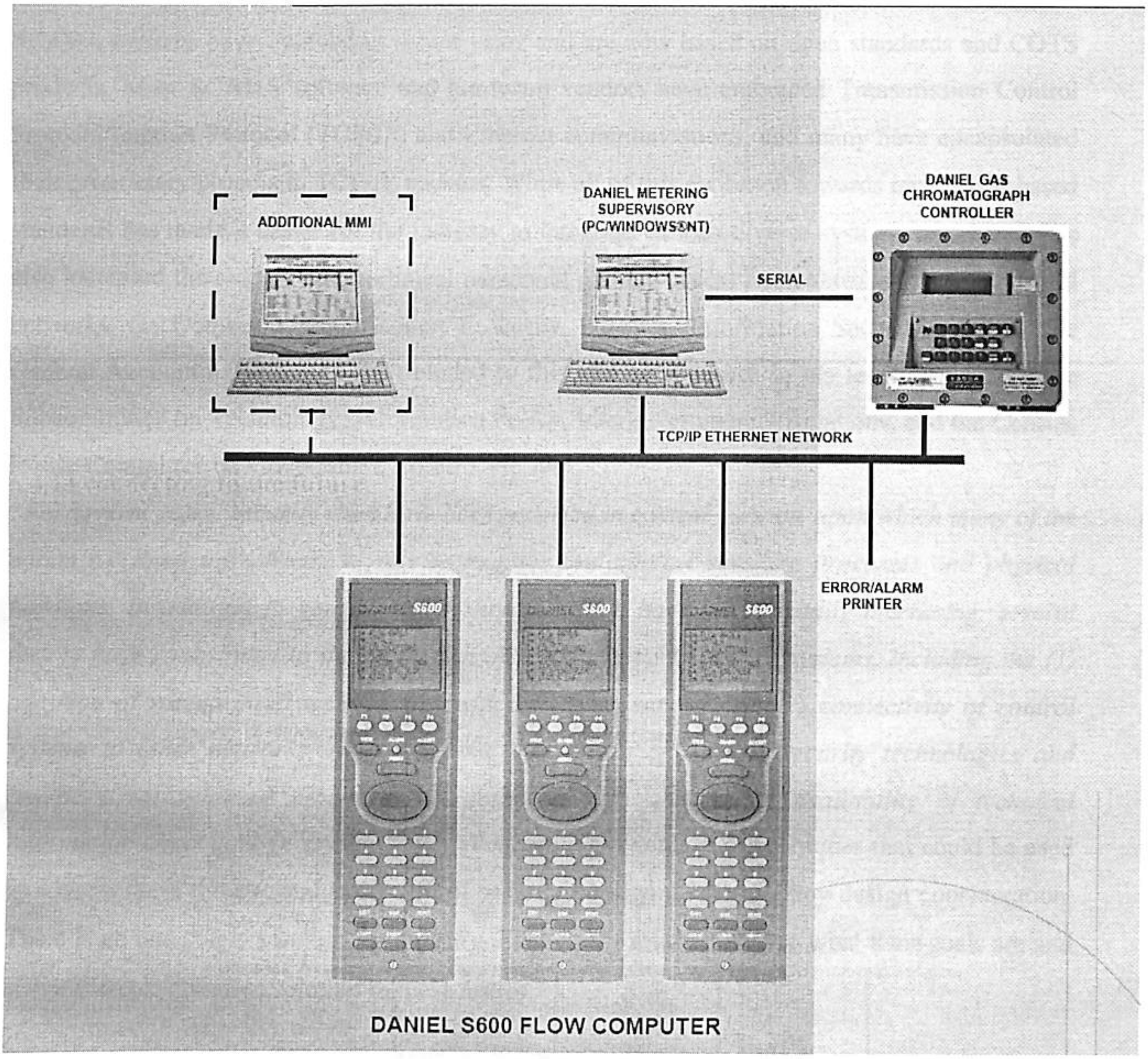
As mentioned previously, the password can be any combination of up to 10 alpha/numeric characters and it should be noted that on confirming new passwords, these are not evented to the printer with old and new values instead for security reasons.

Automatic Log out

If a user has accessed level 1, 2 or 3 and the supervisory computer monitor on keyword activity for fifteen continuous minutes; an automatic log-out of the accessed level will occur. The system will automatically default to Level 0-Guest.

To re access the system, the user has to re-enter the appropriate password. This has been configured to safeguard the security and integrity of the system.

6.4.13 connecting to the future


ADDITIONAL MMI
DANIEL METERING SUPERVISORY (PC/WINDOWS®NT)
DANIEL GAS CHROMATOGRAPH CONTROLLER
SERIAL
TCP/IP ETHERNET NETWORK
ERROR/ALARM PRINTER
DANIEL S600 FLOW COMPUTER

7.0 Security and Vulnerability of SCADA Systems

SCADA systems have evolved in recent years and are now based on open standards and COTS products. Most SCADA software and hardware vendors have embraced Transmission Control Protocol/Internet Protocol (TCP/IP) and Ethernet communications, and many have encapsulated their proprietary procols in TCP/IP packets. While all of this evolution towards more open-based standards has made it easier for the industry to integrate various diverse systems together, it has also increased the risks of less technical personnel gaining access and control of these industrial networks. On October 1, 2003 Robert F. Dacey, Director, Information Security Issues at the General Accounting Office (GAO) eluded to this and other issues in his testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform. He said:

"For several years, security risks have been reported in control systems, upon which many of the nation's critical infrastructures rely to monitor and control sensitive processes and physical functions. In addition to general cyber threats, which have been steadily increasing, several factors have contributed to the escalation of risks specific to control systems, including the (1) adoption of standardized technologies with known vulnerabilities, (2) connectivity of control systems to other networks, (3) constraints on the use of existing security technologies and practices, (4) insecure remote connections, and (5) widespread availability of technical information about control systems". [9] There are many tools and techniques that could be used to address these threats, and flexibility of security configurations is a key design consideration. There is no one magic solution for industry. Each entity must determine what their goals are and arrive at a cost effective solution to these issues.

7.1 Attacks against SCADA Systems

In today's corporate environment, internal networks are used for all corporate communications, including SCADA. SCADA systems are therefore vulnerable to many of the same threats as any TCP/IP-based system. SCADA Administrators and Industrial Systems Analysts are often deceived into thinking that since their industrial networks are on separate systems from the corporate network, they are safe form outside attacks. PLCs and RTUs are usually polled by other 3rd party vendor-specific networks and protocols like RS-232, RS-485, MODBUS4, and DNP, and are usually done over phone lines, leased private frame relay circuits, satellite systems, licensed and spread spectrum radios, and other token-ring bus topology systems. This often gives the SCADA System Administrators a false sense of security since they assume that these end devices are protected by these non-corporate network connections. Security in an industrial network can be compromised in many places along the system and is most easily compromised at the SCADA host or control room level. SCADA computers logging data out to some back-office database repositories must be on the same physical network as the back-end database systems; or have a path to access these database systems. This means that there is a path back to the SCADA systems and eventually the end devices through their corporate network. Once the corporate network is compromised, then any IP-based device or computer system can be accessed. These connections are open 24x7 to allow full-time logging, which provides an opportunity to attack the SCADA host system with any of the following attacks:

- Use a Denial of Service (DoS) attack to crash the SCADA server leading to shut down condition (System Downtime and Loss of Operations)
- Delete system files on the SCADA server (System Downtime and Loss of Operations)
- Plant a Trojan and take complete control of system (Gain complete control of system and be able to issue any commands available to Operators)
- Log keystrokes from Operators and obtain usernames and passwords (Preparation for future take down)
- Log any company-sensitive operational data for personal or competition usage (Loss of Corporate Competitive Advantage)
- Change data points or deceive Operators into thinking control process is out of control and must be shut down (Downtime and Loss of Corporate Data)
- Modify any logged data in remote database system (Loss of Corporate Data)
- Use SCADA Server as a launching point to defame and compromise other system components within corporate network. (IP Spoofing)

The impact of these and other SCADA Security Risks is summarized in Table 6.1.

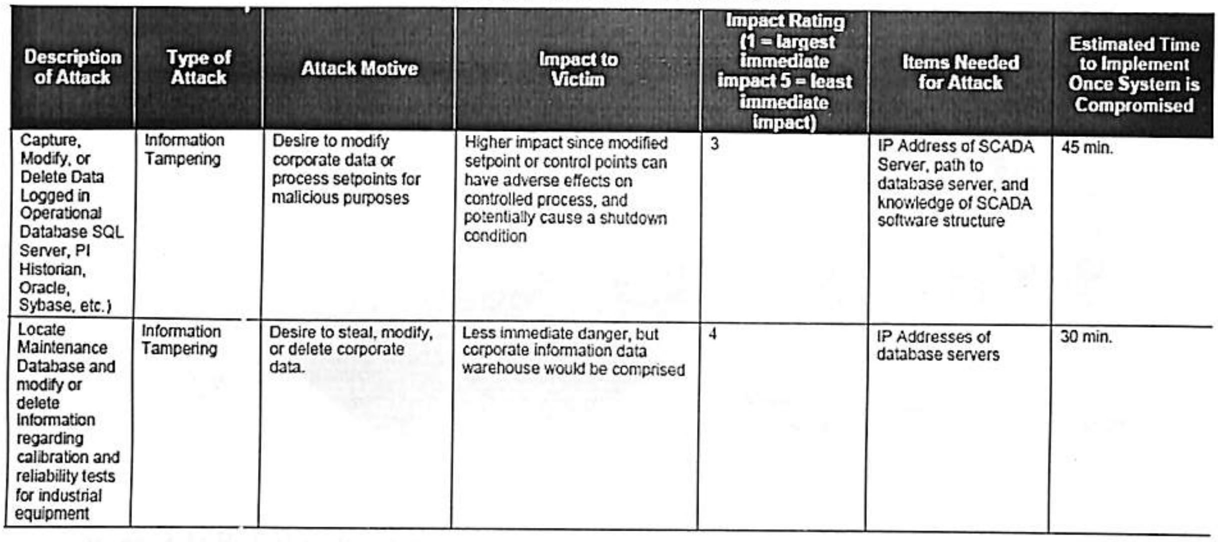
Table 6.1: SCADA Attack Matrix [10]

Description of Attack	Type of Attack	Attack Motive	Impact to Victim	Impact Rating (1 = largest immediate impact 5 = least immediate impact)	Items Needed for Attack	Estimated Time to Implement Once System is Compromised
Denial of Service	System Shutdown	Wish to take down server and cause immediate shutdown situation	SCADA Server locks up and must be rebooted. When SCADA Server comes back on-line, it locks up again. Operations can no longer monitor or control process conditions, and the system will ultimately need to be shut down	2	Ability to flood the server with TCP/IP calls, the IP Address of SCADA Server, and the path to the server	5 min.
Delete System Files (Low-level format on all local drives)	System Shutdown	Wish to take down server and cause immediate shutdown situation	Critical Server and SCADA files are lost and operations can no longer monitor process or control plant or facility	4	IP Address of SCADA Server, path to server, and permission to delete files permission can be escalated used other tools)	15 min.
Take Control of SCADA System	Gain Control	Gain control of SCADA System to impact damage on industrial systems, possibly causing environmental impact, and damage corporate identity through public exposure	Highest impact, since attacker can then manually override safety systems, shut down the system, or takes control of the plant operational conditions.	1	IP Address of SCADA Server, path to server, and either Trojan or back door installed. (Can also use PCAnywhere, Terminal Services, SMS, or other system admin services.)	1 hr.
Log Keystrokes, Usernames, Passwords, System Setpoints, and any Operational Information	Information Mining	Gain Information for future attacks or satisfy curiosity	Lower immediate impact, but information gained can be used for future attacks.	4	IP Address of SCADA Server, path to server, and software or mechanism for logging the keystroke activities.	15 min.

Table 6.1: SCADA Attack Matrix [10]

Description of Attack	Type of Attack	Attack Motive	Impact to Victim	Impact Rating (1 = largest immediate impact 5 = least immediate impact)	Items Needed for Attack	Estimated Time to Implement Once System is Compromised
Change Data Points or Change Setpoint(s) in SCADA System	Information Tampering	Desire to modify corporate data or process setpoints for malicious purposes	Higher impact since modified setpoint or control points can have adverse effects on controlled process, and potentially cause a shutdown condition	2	IP Address of SCADA Server, access to these servers, and some knowledge of SCADA software system inner workings	45 min.
Log any Operational or Corporate data for personal gain or sell to competition or hold as ransom	Information Mining	Try to steal corporate data and either sell to other companies or hold for ransom amount	Low environmental or immediate damage, but can damage corporate image if attacker builds attention to the fact that this system was compromised	4	IP Addresses of SCADA and database servers. (Would not even need IP addresses if protocol sniffer/logger used to sniff TCP/IP traffic.)	30 min.
Modify Data points on SCADA graphics to deceive Operators that system is out of control and must ESD (Emergency Shut Down)	System Shutdown	Cause danger to the facility or company by staging a false alarm shutdown of the plant or facility	Operations can no longer trust the SCADA System, and the attacker has deceived the Operator into thinking that there was an emergency condition in the plant	2	IP Addresses of SCADA servers, and access to them through the company network	45 min.

Table 6.1: SCADA Attack Matrix [10]



Description of Attack	Type of Attack	Attack Motive	Impact to Victim	Impact Rating (1 = largest immediate impact 5 = least immediate impact)	Items Needed for Attack	Estimated Time to Implement Once System is Compromised
Capture, Modify, or Delete Data Logged in Operational Database SQL Server, PI Historian, Oracle, Sybase, etc.)	Information Tampering	Desire to modify corporate data or process setpoints for malicious purposes	Higher impact since modified setpoint or control points can have adverse effects on controlled process, and potentially cause a shutdown condition	3	IP Address of SCADA Server, path to database server, and knowledge of SCADA software structure	45 min.
Locate Maintenance Database and modify or delete Information regarding calibration and reliability tests for industrial equipment	Information Tampering	Desire to steal, modify, or delete corporate data.	Less immediate danger, but corporate information data warehouse would be comprised	4	IP Addresses of database servers	30 min.

7.2 Developing a SCADA Security Strategy

For a company to protect its infrastructure, it should undertake the development of a security strategy that includes specific steps to protect any SCADA system. Such a strategy may include the following approach. Developing an appropriate SCADA security strategy involves analysis of multiple layers of both the corporate network and SCADA architectures including firewalls, proxy servers, operating systems, application system layers, communications, and policy and procedures. Strategies for SCADA Security should complement the security measures implemented to keep the corporate network secure Figure 6.1 below illustrates the typical corporate network "ring of defenses" and its relationship with the SCADA network. Successful attacks can originate from either Internet paths through the corporate network to the SCADA network, or from internal attacks from within the corporate office. Alternatively, attacks can originate from within the SCADA network from either upstream (applications) or downstream (RTUs) paths. What is an appropriate configuration for one installation may not be cost effective for another. Flexibility and the employment of an integrated and coordinated set of layers are critical in the design of a security approach.

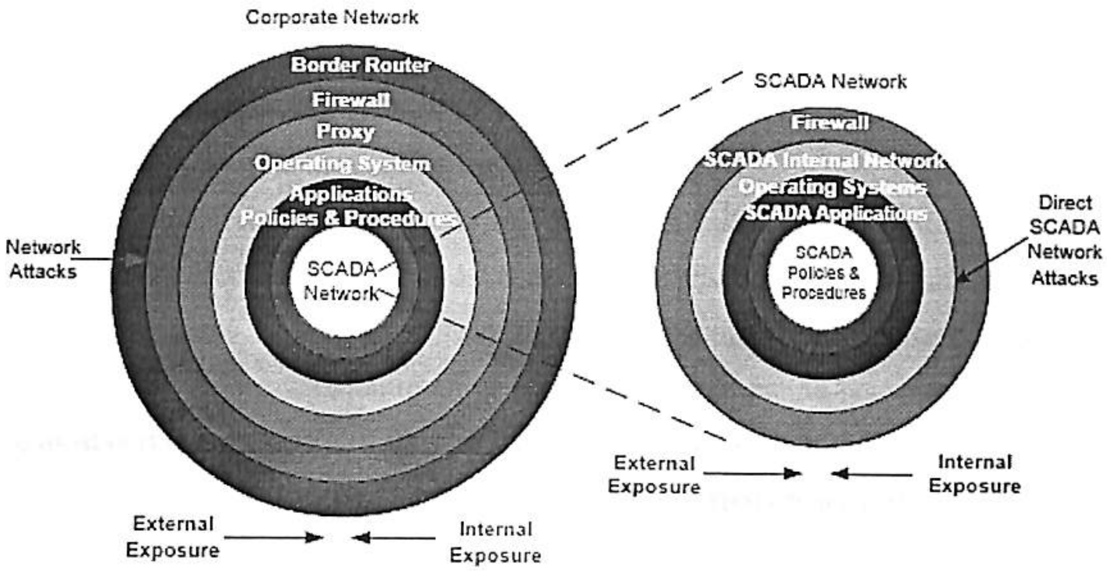


Figure 7.1: Relationship Between Corporate and SCADA Networks [10]

Most corporate networks employ a number of security countermeasures to protect their networks. Some of these and a brief description of their functions are as follows:

- Border Router and Firewalls–Firewalls, properly configured and coordinated, can protect passwords, IP addresses, files and more. However, without a hardened operating system, hackers can directly penetrate private internal networks or create a Denial of Service condition.
- **Proxy Servers–**A Proxy server is an internet server that acts as a firewall, mediating traffic between a protected network and the internet. They are critical to re-create TCP/IP packets before passing them on to, or from, application layer resources such as Hyper Text Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP).

However, the employment of proxy servers will not eliminate the threat of application layer attacks.

- Operating Systems–Operating systems can be compromised, even with proper patching, to allow network entry as soon as the network is activated. This is due to the fact that operating systems are the core of every computer system and their design and operating characteristics are well known world wide. As a result, operating systems are a prime target for hackers. Further, in-place operating system upgrades are less efficient and secure than design-level migration to new and improved operating systems.

- Applications—Application layer attacks; i.e., buffer overruns, worms, Trojan Horse programs and malicious Active-X5 code, can incapacitate anti-virus software and bypass the firewall as if it wasn't even there.
- Policies and Procedures—Policies and procedures constitute the foundation of security policy infrastructures. They include requiring users to select secure passwords that are not based on a dictionary word and contain at least one symbol, capital letter, and number, and should be over eight characters long Users should not be allowed to use their spouse, child, or pet's name as their password. The above list is common to all entities that have corporate networks. SCADA systems for the most part coexist on the same corporate network [10]. The following list suggests ways to help protect the SCADA network in conjunction with the corporate network:
- SCADA Firewalls-SCADA Systems and Industrial Automation Networks, like corporate network operating systems, can be compromised using similar hacking methods. Oftentimes, SCADA systems go down due to other internal software tools or employees who gain access into the SCADA systems, often without any intention to take down these systems. For these reasons, it is suggested that strong firewall protection to wall off your SCADA networking systems from both the internal corporate network and the Internet be implemented. This would provide at least two layers of firewalls between the SCADA networking systems and the Internet.
- SCADA Internal Network Design—SCADA networks should be segmented off into their own IP segment using smart switches and proper sub-masking techniques to protect the Industrial Automation environment from the other network traffic, such as file and print commands. Facilities using Wireless Ethernet and Wired Equivalent Protocol (WEP) should change the default name of the Service Set Identifier6 (SSID). This will at least require someone driving by with a wireless card to know the name of the SSID, and have the appropriate encryption key for the wireless network.
- SCADA Server Operating Systems—Simply installing a firewall or segmenting

SCADA IP addresses will not ensure their SCADA Infrastructure is secure. An experienced hacker can often bypass firewalls with ease and can even use Address Resolution Protocol (ARP) trap utilities to steal Media Access Control (MAC) addresses. The hacker can also deploy IP spoofing techniques to maneuver through switched networks. Operating systems running the SCADA applications must also be maintained. SCADA applications on Windows NT, 2000, or XP are properly patcned against the latest vulnerabilities, and that all of the default NULL NT accounts and administrator accounts have been removed or renamed. SCADA applications running in UNIX, LINUX, Novell, or any other Operating System (OS), must also be maintained as above. All operating systems have back doors and default access accounts that should be removed and cleaned off of these SCADA Servers.

• SCADA Applications–You must also address security within the SCADA application itself. Trojan horses and worms can be inserted to attack application systems, and they can be used to manipulate data or issue commands on the server. There have even been cases of Trojan horses being deployed that completely emulate the application. The operator or user thinks that he is clicking on a command to stop a pump or generate a graph of the plant, but he is actually clicking on buttons disguised to look like the SCADA screen, and these buttons start batch files that delete the entire hard drive, or send out pre-derived packets on the SCADA system that turn all outputs to ON or "1" state. Trojan horses and viruses can also be planted through an email opened by another computer in the plan, and then it is silently copied over to adjacent SCADA servers, where they wait until a specified time to run. Many times plant control rooms will have corporate computers with the Internet and email active on them within the same physical room, and network switches as SCADA computers. Methodologies to mitigate against these types of situations are: the use of anti-virus software running on the computer where the SCADA application resides; systems administrators disabling installation of any unauthorized software unless the user has administrator access; and Policies and Procedures applicable to SCADA systems, which are addressed below.

• SCADA Policies and Procedures–SCADA policies and procedures associated with remote vendor and supervisory access, password management, etc. can significantly impact the vulnerabilities of the SCADA facilities within the SCADA network. Properly developed Policies and Procedures that are enforced will greatly improve the security posture of the SCADA system. In summary, these multiple "rings of defense" must be configured in a complementary and organized manner, and the planning process should involve a cross-team with senior staff support from operations, facility engineering, and Information Technology (IT). The SCADA Security team should first analyze the current risks and threat at each of the rings of defense, and then initiate a work plan and project to reduce the security risk, while remembering to avoid any major impacts to operations.

8.0 Work carried out by me

I studied the process and list out the field instrument those are require for the measurement, like different transducer, some special instrument like gas chromatography and its type. now we are discuss the different parameter and its type and why we choose this particular one.

1. Temperature transducer: - It having the different types likes

- Thermocouple
- RTD
- Thermister

We are using **RTD pt 100** type because this device is suitable for temperature range -20 to 160 ^{0}c and its response is good it will give you 100 ohm resistance at 0 ^{0}c.other temperature transducer like thermocouple it will use for high temperature measurement, and thermister will use for low temperature measurement.

2. Pressure transducer:-type available is as follow

- Bourdon tube
- Bellow
- Strain gauge

These are the main type of the pressure transducer but we are using bourdon tube type because its rang 0-100 psi it will be working accurately in this range .strain gauge is not suitable for this range

3. Transmission medium: - We have different types of cable available for transmitting the data following are the types

- Twisted-Pair Metallic Cable
- Coaxial Metallic Cable
- Fiber Optic Cable
- Power Line Carrier
- Satellites
- Leased Telephone Lines

We are using fiber optic cable because it having following advantages over the copper wire

- **SPEED:** Fiber optic networks operate at high speeds - up into the gigabits
- **BANDWIDTH:** large carrying capacity
- **DISTANCE:** Signals can be transmitted further without needing to be "refreshed" or strengthened.
- **RESISTANCE:** Greater resistance to electromagnetic noise such as radios, motors or other nearby cables.
- **MAINTENANCE:** Fiber optic cables costs much less to maintain.

4. Protocol:-

We are using DNP 3 protocol because it provides required functions as given below.

5. DNP3 is a protocol for transmission of data from point A to point B using serial communications
6. DNP3 is specifically developed for inter-device communication involving SCADA RTUs, and provides for both RTU-to-IED and master-to-RTU/IED.
7. It is the protocol that fix well in the data acquisition.
8. It is design to work in wide area communication network.

5. Architecture of SCADA system: - We have the three type of architecture

- First Generation – Monolithic
- Second Generation – Distributed
- Third Generation – Networked

We are commonly use this architecture because it will provided

- Open system architecture
- Utilizing open standard and protocol
- Making it possible to distribute SCADA functionality across WAN.
- System make easier for the user to third party periphery devices (such as monitor ,printer, disk drive etc .)

How they can give the authority to change the parameter for different level person of the organization

Guest (default):- It allow to view all data and print the report.

Operator: - It allows all function associated with guest.

- Alarm acknowledgment.
- Configure the display and tag names.
- Data modification.
- Valve operation.

Engineer: - It allows all function associated with operater.

Report archiving in to cd-R/cd-RW.

Shut down supervisory computer

Administrator: - All function associated with level 2.

Modification of password.

Software configuration and VBA scripting

Benefits we gate from this system.

- Report management.
- Alarm summary.
- Real time data analysis.
- Process of data gathering is fairly simple
- Link failure can easily be detected

Segregate the field instrument parameter in the form of monitoring and controlling with type of signal they have been required to operate.

Monitoring parameter	Controlling parameter	Type of signal Analog/digital
Filtration skid		
Pressure transmitter		Analog
Differential pressure transmitter		Analog
Temperature gauge (RTD pt 100)		Analog
	Pressure safety valve	Digital
	Control valve Limit switch's	Digital
Metering skid		
Ultrasonic meter Measure the flow rate		Analog
Pressure transmitter		Analog
Temperature gauge (RTD pt 100)		Analog
	Gas over oil actuator(GOOA)	Digital
	Gas chromatography	Digital
LADE DOWN SKID		
Pressure transmitter		Analog
Temperature gauge (RTD pt 100)		Analog
	Slam shut of valve (SSV)	Digital
Pressure control valve (monitor)		Analog
	Pressure control valve (active)	Digital

9.0 Observations and Conclusions

1. Most hazardous liquid and gas pipeline operators use SCADA system to monitor and control their pipelines.
2. Operators reported that SCADA system enhance both the safety and efficiencies of pipeline operations.
3. Implementation of graphical standards developed for pipeline operations will increase the likelihood that leaks will be detected quickly and that resulting damage from the leaks will be minimize.
4. An effective alarm review /audit system will increase the likelihood of controller appropriately responding to alarms associated with pipeline leaks.
5. Today's SCADA systems are able to take advantage of the evolution from mainframe based to client/server architectures. These systems use common communications protocols like Ethernet and TCP/IP to transmit data from the field to the central master control unit.
6. SCADA protocols have also evolved from closed proprietary systems to an open system, allowing designers to choose equipment that can help them monitor their unique system using equipment from variety of vendors
7. SCADA systems, like other computer systems, are subject to many common security attacks such as viruses, denial of service, and hijacking of the system
8. Because SCADA systems use leased telephone lines, twisted pair cable, microwave radio, and spread spectrum techniques, they have many of the same security vulnerabilities
9. While SCADA protocols are more open today, there is no clear consensus of which protocol is best. IEC 60870-5 series and DNP3 have many similarities but are not 100% compatible.

10.0 Recommendations

The fire and gas detection system is required to correlate with station control system.

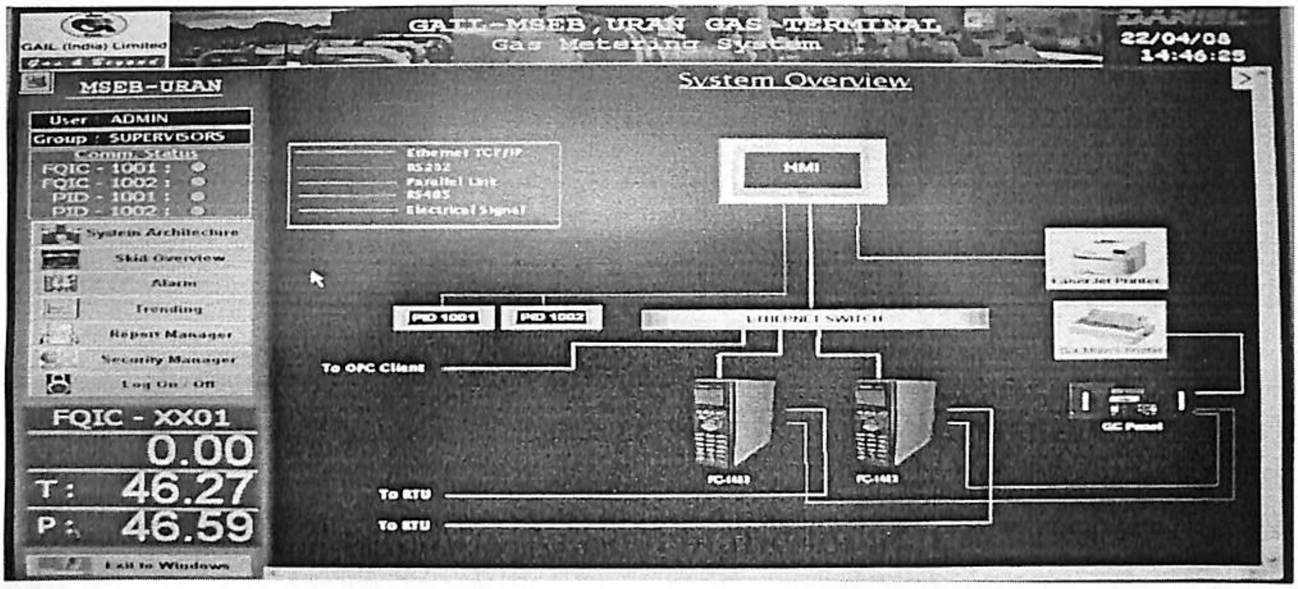
Several issues need to be addressed, especially in the area of vulnerabilities associated with computer usage and the communications within SCADA systems.

- Monitor and participate, as appropriate, in the IEEE standards process as it relates to SCADA systems, especially in security features or requirements with SCADA Standards.
- NCS should pursue, with the developers of SCADA protocols, incorporation of security features internal to the protocol rather than external.

Following areas for improvement has been observed during execution of projects.

- All losses like rework, time loss and excess consumption could be indentified to initiate corrective action.
- By providing safety shoes minor injuries could be reduce.
- Training on Emergency preparedness, safety, fire will improve work Environment & Enhance competency.
- 5 S is required in stores to reduce waste of time to search of items.

Appendix A: Schematic format



GAIL-MSEB, URAN GAS TERMINAL
Gas Metering System

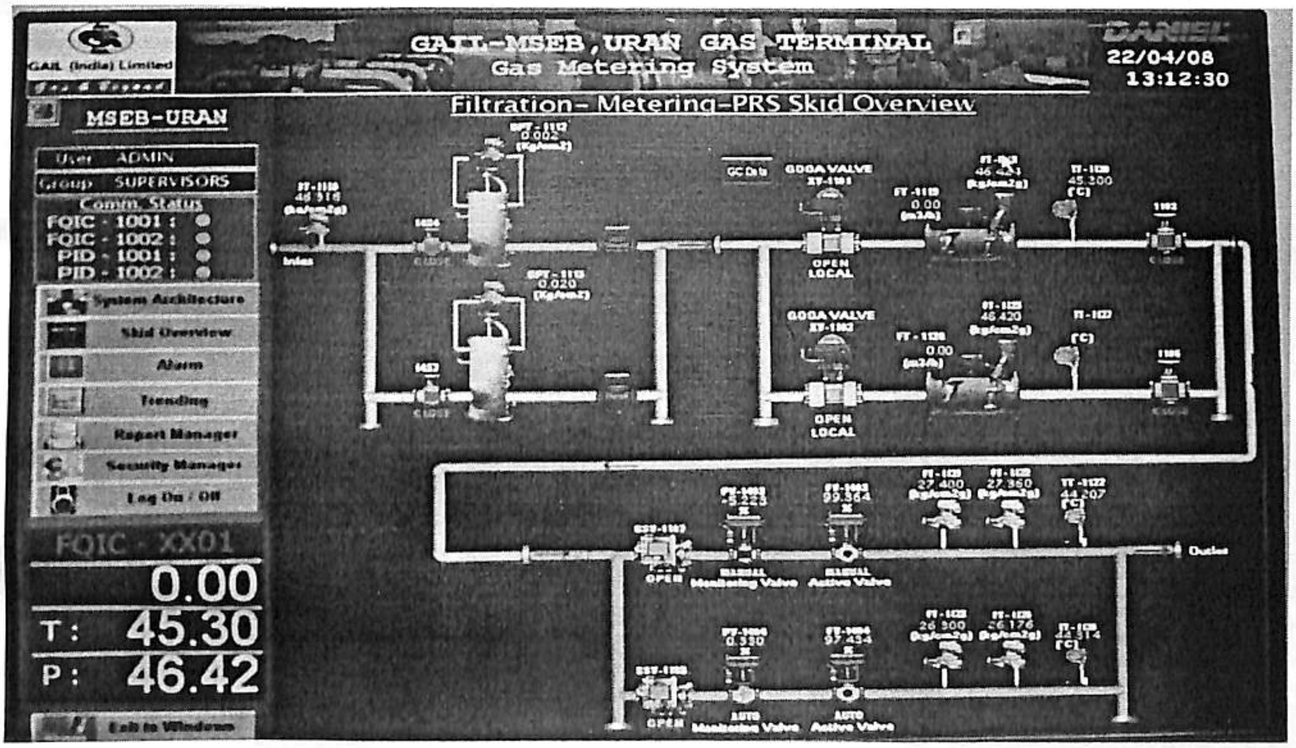
22/04/08
14:46:25

MSEB-URAN

User : ADMIN
Group : SUPERVISORS

FQIC - XX01
0.00
T: 46.27
P: 46.59

System overview



GAIL-MSEB, URAN GAS TERMINAL
Gas Metering System

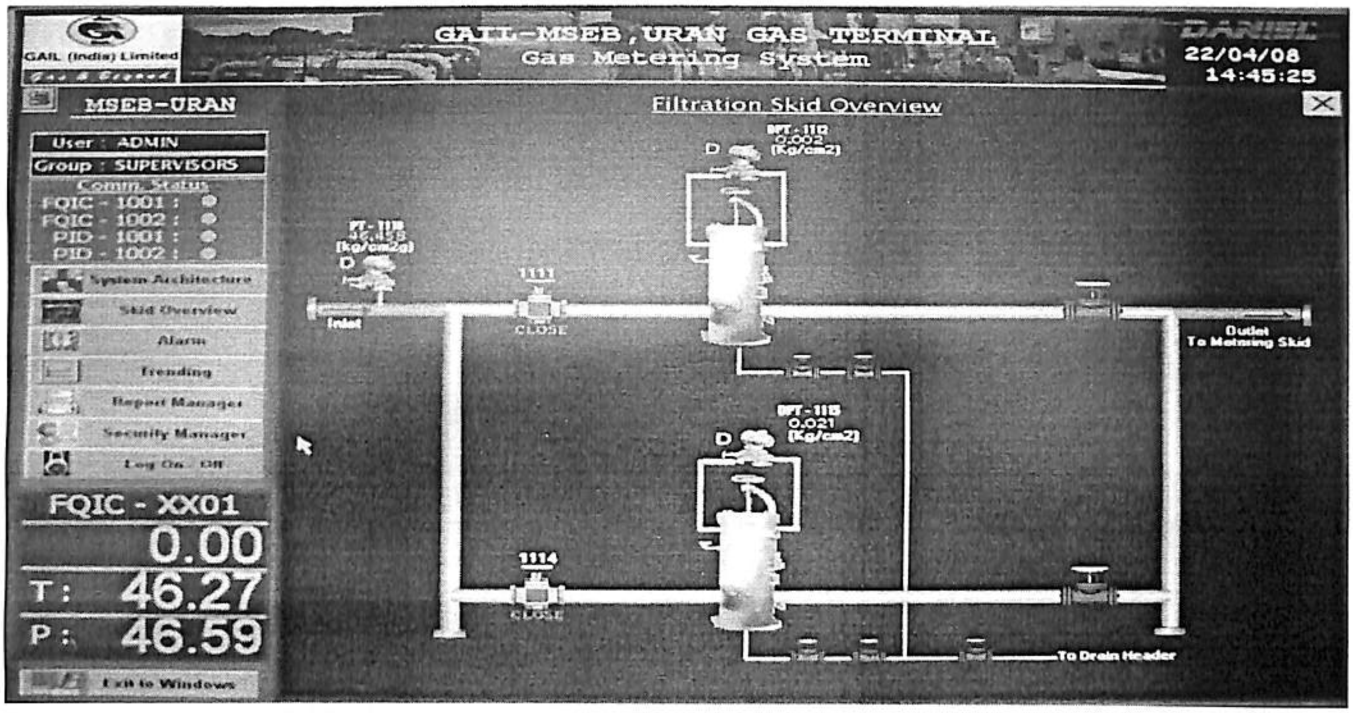
22/04/08
13:12:30

MSEB-URAN

User ADMIN
Group SUPERVISORS

FQIC - XX01
0.00
T: 45.30
P: 46.42

Skid overview



GAIL-MSEB,URAN GAS TERMINAL
Gas Metering System

22/04/08
14:45:25

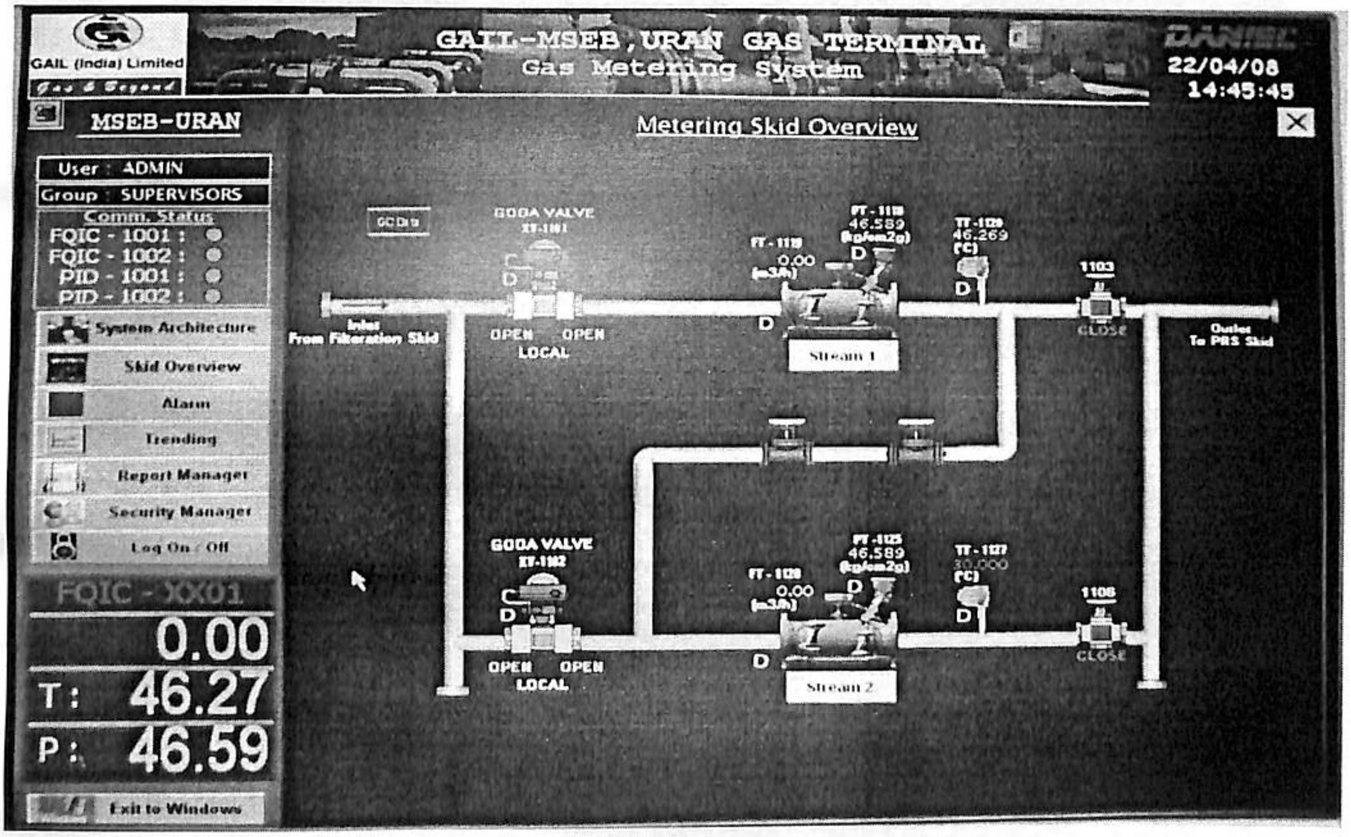
MSEB-URAN

Filtration Skid Overview

User : ADMIN
Group : SUPERVISORS

Comm. Status
FQIC - 1001 : ●
FQIC - 1002 : ●
PID - 1001 : ●
PID - 1002 : ●

FQIC - XX01
0.00
T: 46.27
P: 46.59



GAIL-MSEB,URAN GAS TERMINAL
Gas Metering System

22/04/08
14:45:45

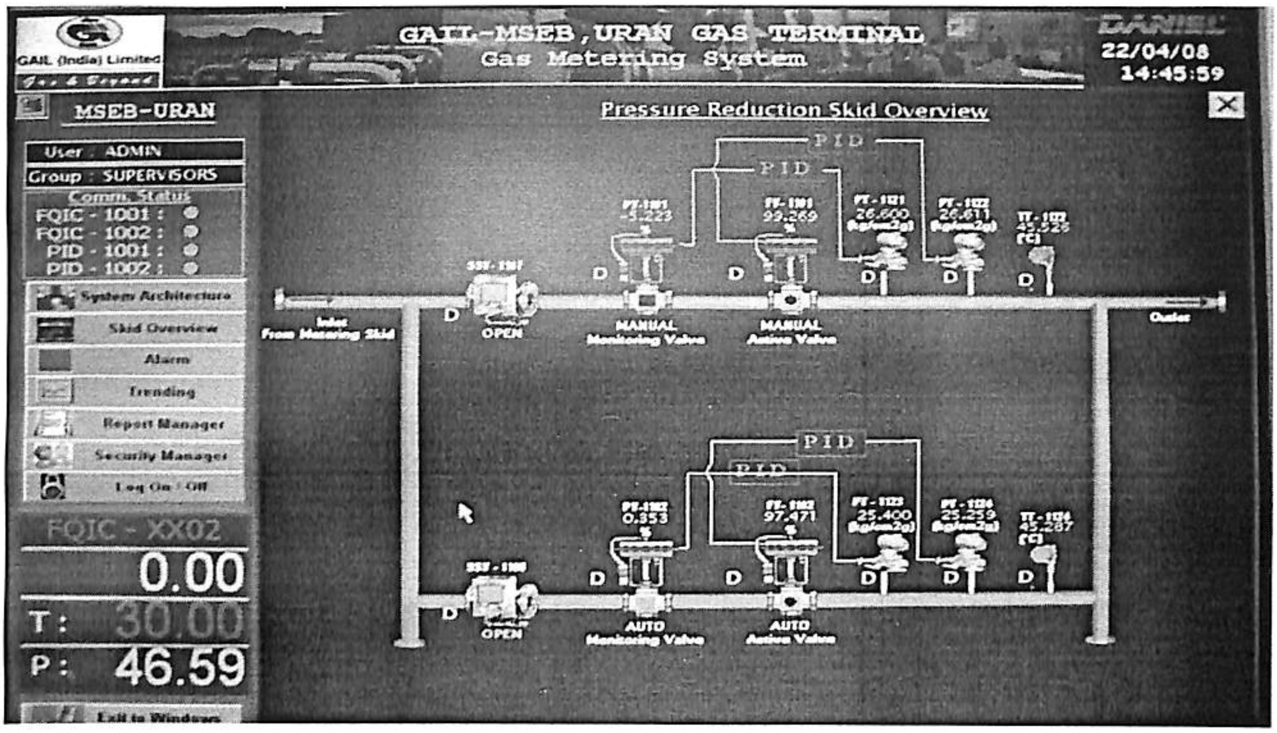
MSEB-URAN

Metering Skid Overview

User : ADMIN
Group : SUPERVISORS

Comm. Status
FQIC - 1001 : ●
FQIC - 1002 : ●
PID - 1001 : ●
PID - 1002 : ●

FQIC - XX01
0.00
T: 46.27
P: 46.59



User : ADMIN

Group : SUPERVISORS

Comm. Status

FQIC - 1001 : ●

FQIC - 1002 : ●

PID - 1001 : ●

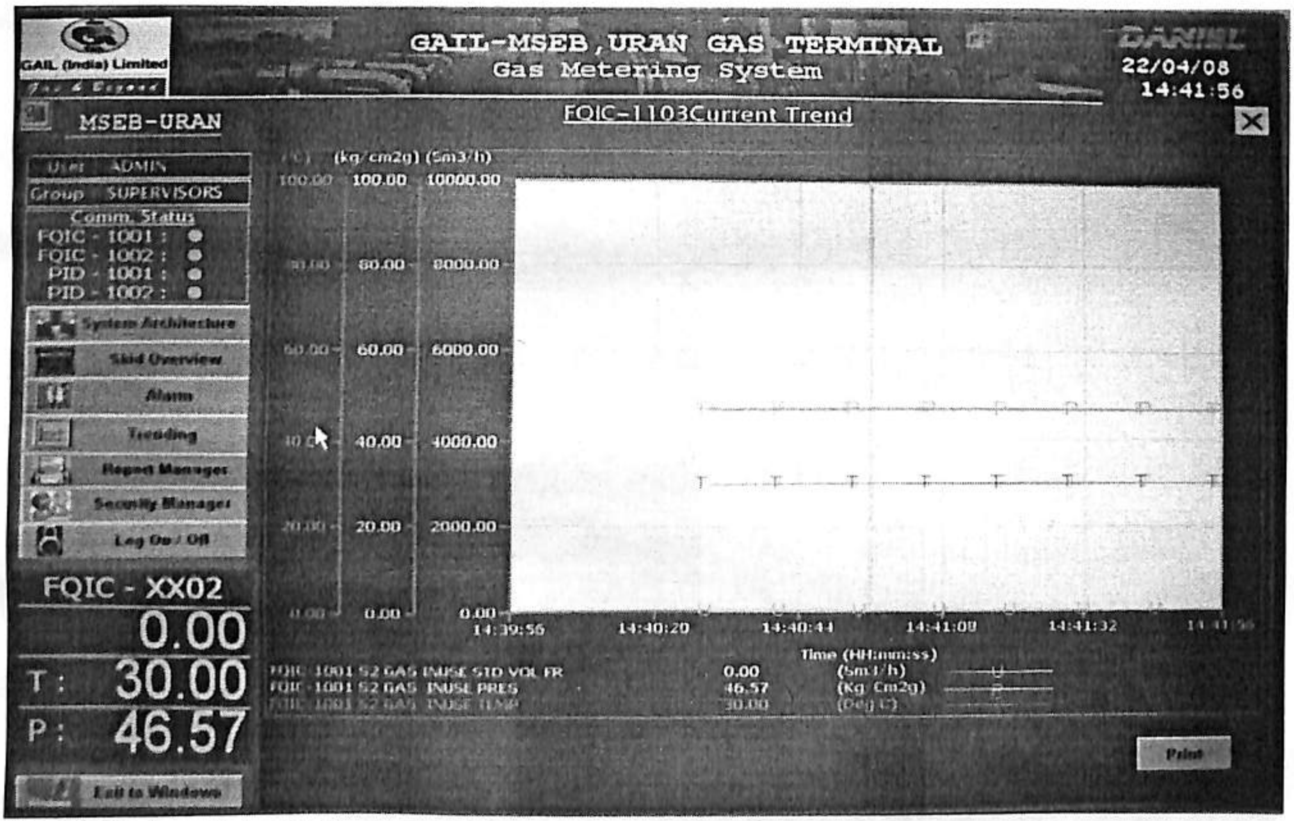
PID - 1002 : ●

FQIC - XX02

0.00

T: 30.00

P: 46.59



User : ADMIN

Group : SUPERVISORS

Comm. Status

FQIC - 1001 : ●

FQIC - 1002 : ●

PID - 1001 : ●

PID - 1002 : ●

FQIC - XX02

0.00

T: 30.00

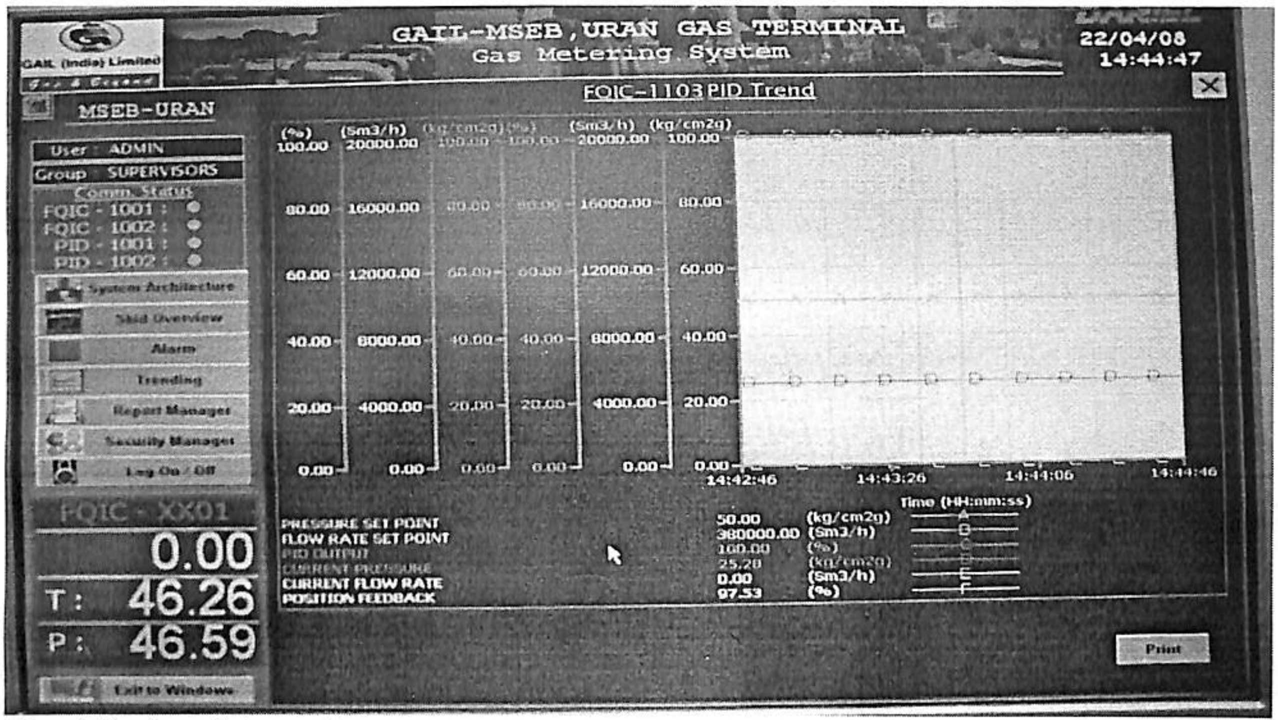
P: 46.57

FQIC-1001 S2 GAS INUSE STD VOL FR 0.00 (Sm3/h)

FQIC-1001 S2 GAS INUSE PRES 46.57 (Kg Cm2g)

FQIC-1001 S2 GAS INUSE TEMP 30.00 (Deg C)

Trend display of stream 2



GAIL-MSEB, URAN GAS TERMINAL
Gas Metering System

22/04/08
14:44:47

FQIC-1103 PID Trend

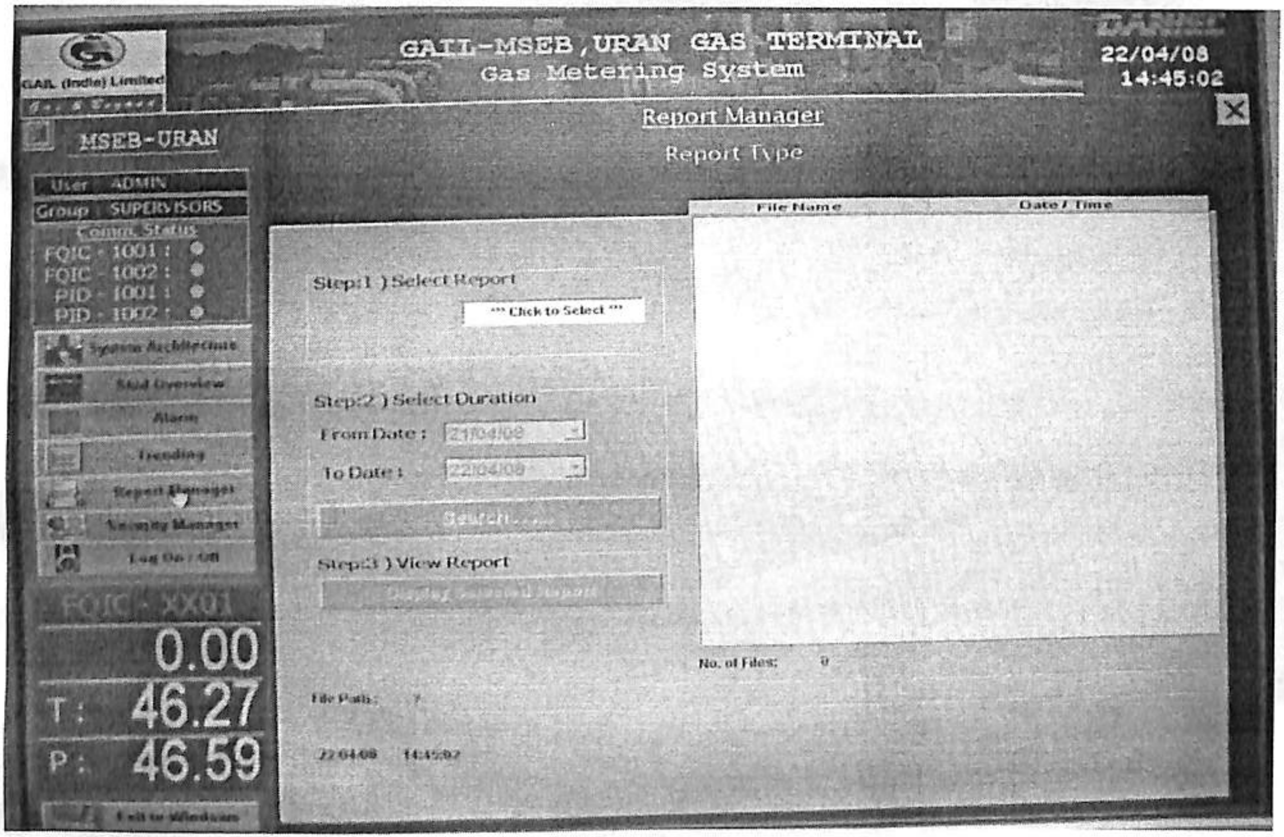
User : ADMIN
Group : SUPERVISORS

Comm. Status
FQIC - 1001 : ●
FQIC - 1002 : ●
PID - 1001 : ●
PID - 1002 : ●

FQIC - XX01
0.00
T: 46.26
P: 46.59

PRESSURE SET POINT	50.00	(kg/cm2g)
FLOW RATE SET POINT	380000.00	(Sm3/h)
PID OUTPUT	100.00	(%)
CURRENT PRESSURE	25.20	(kg/cm2g)
CURRENT FLOW RATE	0.00	(Sm3/h)
POSITION FEEDBACK	97.53	(%)

Trend display of stream 1



GAIL-MSEB, URAN GAS TERMINAL
Gas Metering System

22/04/08
14:45:02

Report Manager

Report Type

User : ADMIN
Group : SUPERVISORS

Comm. Status
FQIC - 1001 : ●
FQIC - 1002 : ●
PID - 1001 : ●
PID - 1002 : ●

FQIC - XX01
0.00
T: 46.27
P: 46.59

Step:1) Select Report

Step:2) Select Duration
From Date : 21/04/08
To Date : 22/04/08

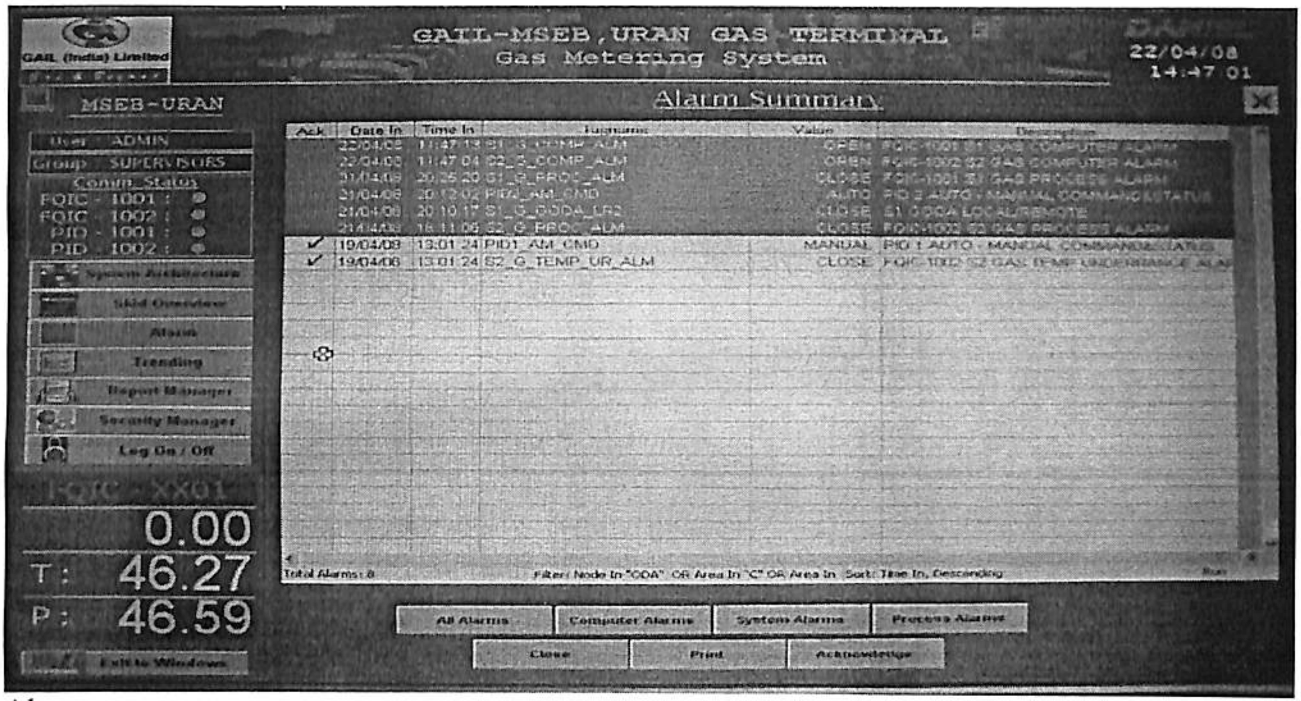
Step:3) View Report

No. of Files: 0

File Path: ?

22/04/08 14:45:02

Report format



GAIL-MSEB,URAN GAS TERMINAL

Gas Metering System

22/04/08
14:47 01

MSEB-URAN

Alarm Summary

User ADMIN

Group SUPERVISORS

Comm_Status

FQIC - 1001 : ●
FQIC - 1002 : ●
PID - 1001 : ●
PID - 1002 : ●

Ack	Date In	Time In	Tagname	Value	Description
	22/04/08	11:47:13	S1_G_COMP_ALM	OPEN	FQIC-1001 S1 GAS COMPUTER ALARM
	22/04/08	11:47:04	S2_G_COMP_ALM	OPEN	FQIC-1002 S2 GAS COMPUTER ALARM
	21/04/08	20:25:20	S1_G_PROC_ALM	CLOSE	FQIC-1001 S1 GAS PROCESS ALARM
	21/04/08	20:12:02	PID2_AM_CMD	AUTO	PID 2 AUTO - MANUAL COMMAND STATUS
	21/04/08	20:10:17	S1_G_CODA_LR2	CLOSE	S1 CODA LOCAL/REMOTE
	21/04/08	16:11:06	S2_G_PROC_ALM	CLOSE	FQIC-1002 S2 GAS PROCESS ALARM
✓	19/04/08	13:01:24	PID1_AM_CMD	MANUAL	PID 1 AUTO - MANUAL COMMAND STATUS
✓	19/04/08	13:01:24	S2_G_TEMP_UR_ALM	CLOSE	FQIC-1002 S2 GAS TEMP UNDERRANGE ALA

Total Alarms: 8 Filter: Node In "CODA" OR Area In "C" OR Area In Sort: Time In, Descending

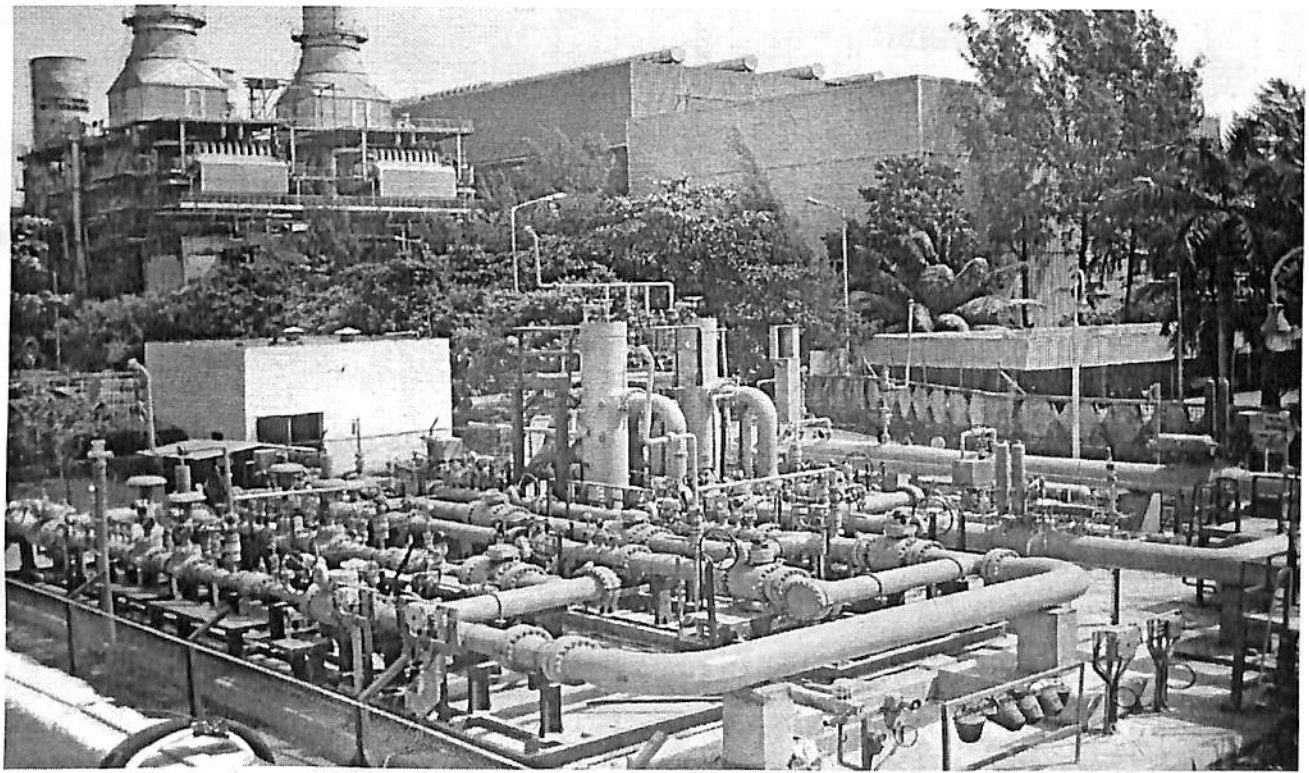
FQIC - XX01

0.00

T: 46.27

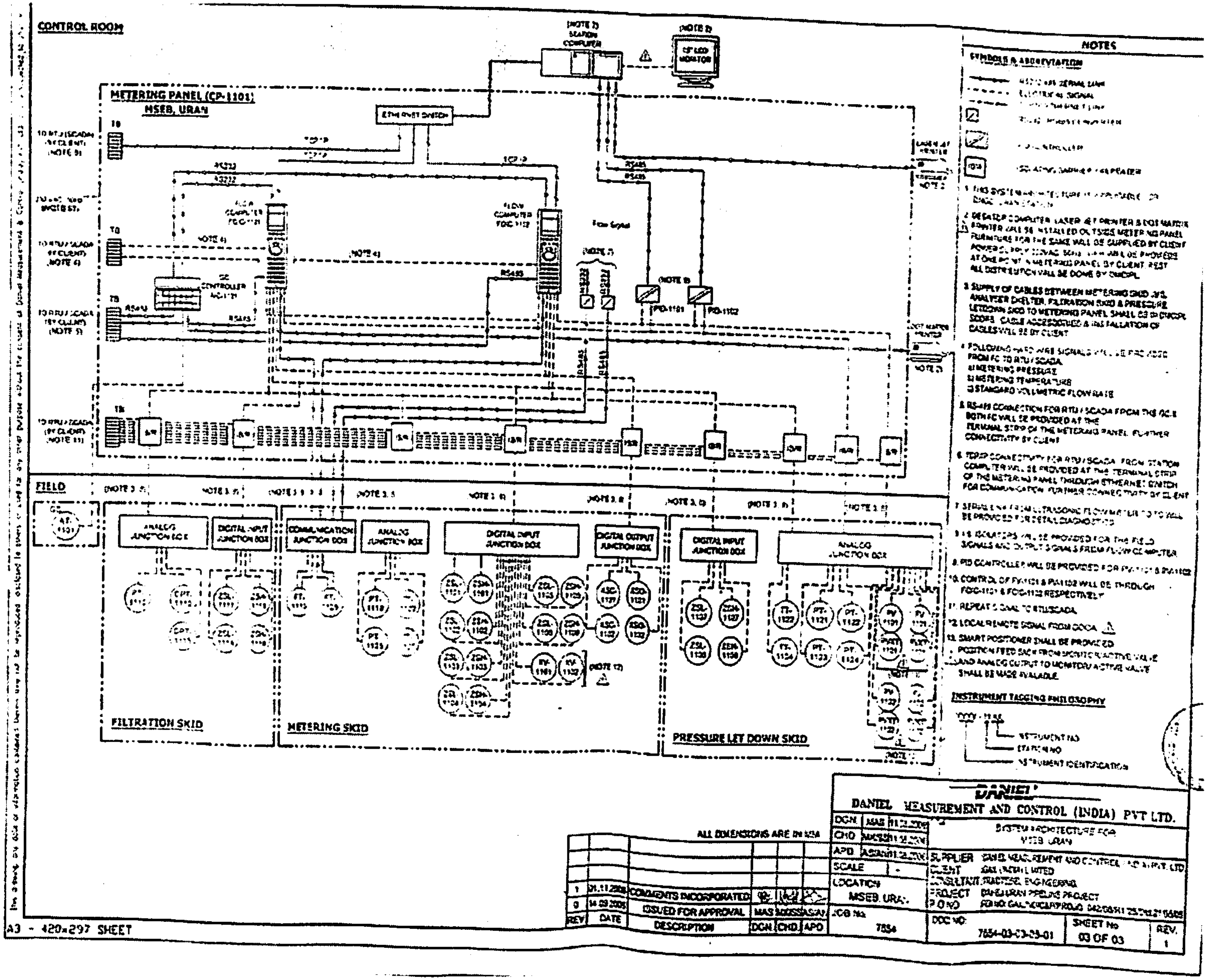
P: 46.59

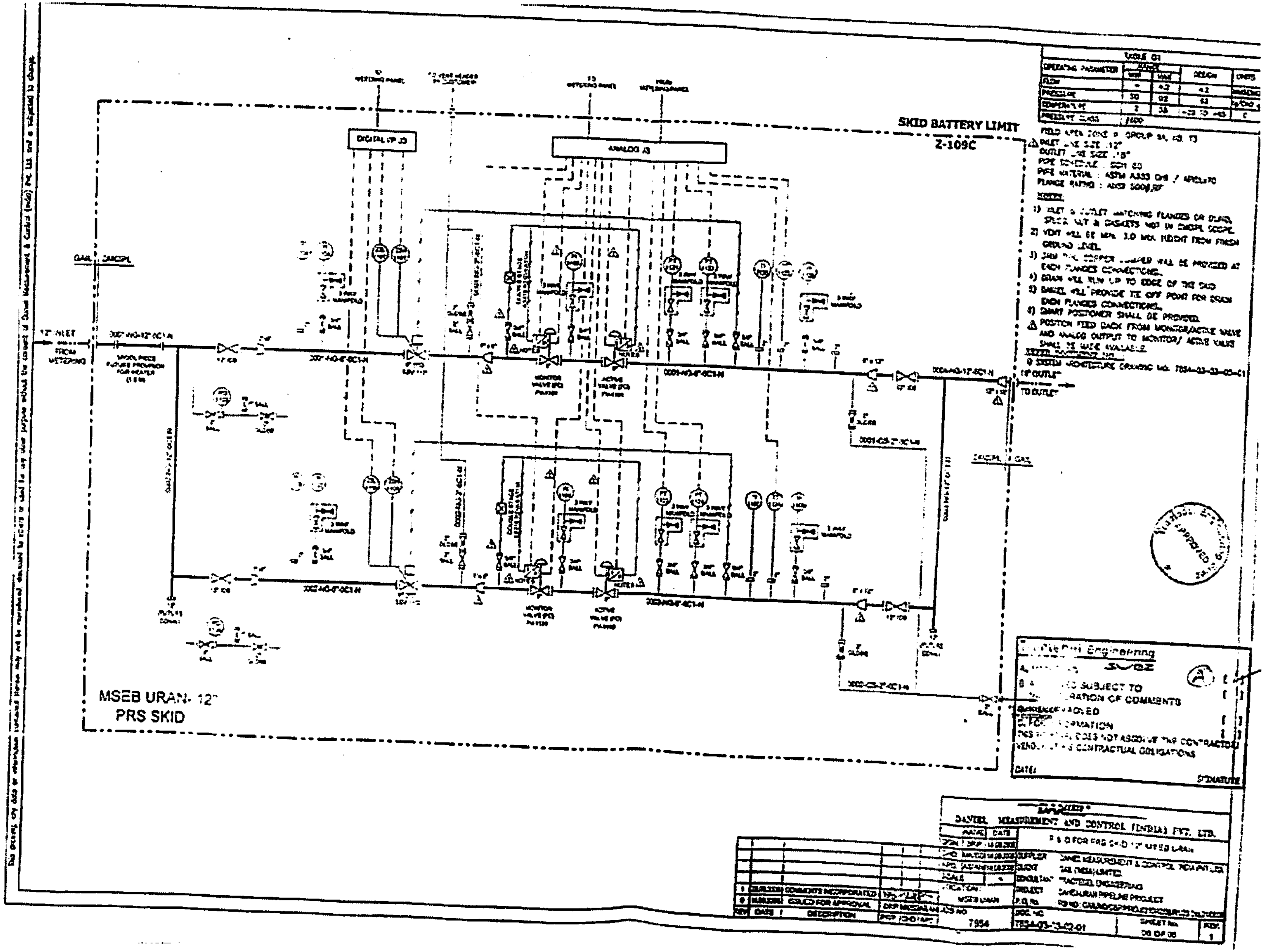
Alarm summary

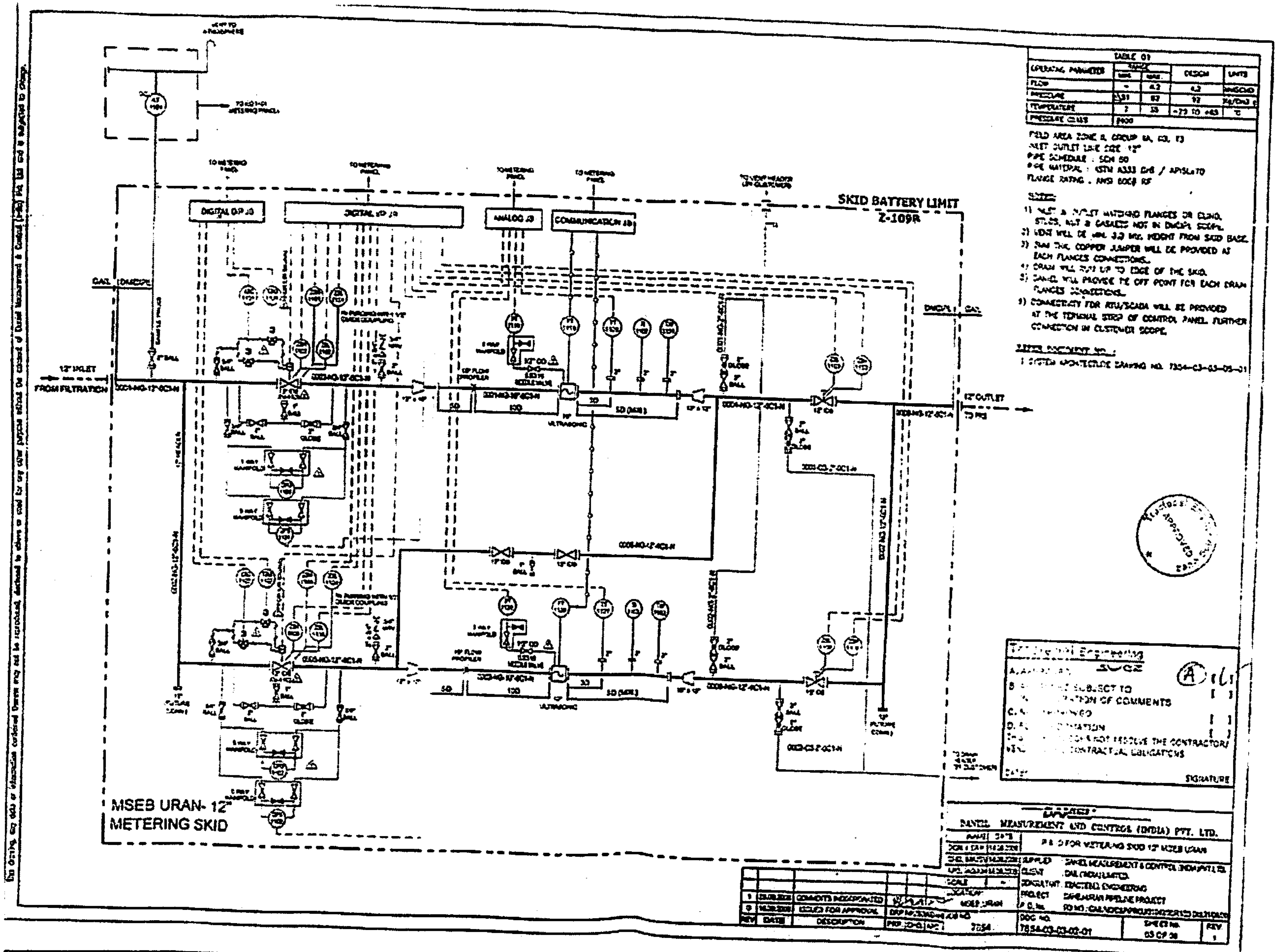


Gas receiving station at MSEB URAN

Appendix B: Termination Diagram




SKID BATTERY LIMIT
Z-109C
DIGITAL I/P JB
ANALOG JB
12" INLET FROM METERING
GAIL | DANCIPL
DANCIPL | GAIL
12" OUTLET
TO OUTLET
MONITOR VALVE (PCV)
ACTIVE VALVE (PCV)
3 WAY MANIFOLD
3/4" BALL
2" GLOBE
SSV
MSEB URAN- 12"
PRS SKID
TABLE 01
OPERATING PARAMETER
DESIGN
UNITS
FLOW
PRESSURE
TEMPERATURE
PRESSURE CLASS
INLET LINE SIZE : 12"
OUTLET LINE SIZE : 8"
PIPE SCHEDULE : SCH 80
PIPE MATERIAL : ASTM A333 Gr6 / API5LX70
FLANGE RATING : ANSI 600# RF
NOTES:
1) INLET & OUTLET MATCHING FLANGES OR BLIND, SPECS, NUT & GASKETS NOT IN DANIEL SCOPE.
2) VENT WILL BE MIN. 3.0 MTR. HEIGHT FROM FINISH GROUND LEVEL.
3) SMM THK. COPPER JUMPER WILL BE PROVIDED AT EACH FLANGES CONNECTIONS.
4) DRAIN WILL RUN UP TO EDGE OF THE SKID.
5) DANIEL WILL PROVIDE TIE OFF POINT FOR DRAIN EACH FLANGES CONNECTIONS.
6) SMART POSITONER SHALL BE PROVIDED.
POSITION FEED BACK FROM MONITOR/ACTIVE VALVE AND ANALOG OUTPUT TO MONITOR/ ACTIVE VALVE SHALL BE MADE AVAILABLE.
SYSTEM ARCHITECTURE DRAWING NO. 7954-03-33-00-01
SUBJECT TO INCORPORATION OF COMMENTS
APPROVED
FOR INFORMATION
THIS APPROVAL DOES NOT ABSOLVE THE CONTRACTOR/ VENDOR OF HIS CONTRACTUAL OBLIGATIONS
DATE:
SIGNATURE
DANIEL MEASUREMENT AND CONTROL (INDIA) PVT. LTD.
NAME
DATE
P & ID FOR PRS SKID 12" MSEB URAN
SUPPLIER
CLIENT
CONSULTANT
PROJECT
P.O. No.
DOC. NO.
7954-03-13-02-01
SHEET No.
REV.
1
COMMENTS INCORPORATED
ISSUED FOR APPROVAL
REV
DATE
DESCRIPTION
7954



OPERATING PARAMETER	RANGE		DESIGN	UNITS
	MIN.	MAX.		
FLOW	-	4.2	4.2	MMSCMD
PRESSURE	33.31	87	92	Kg/Cm2 g
TEMPERATURE	3	35	-29 TO +65	°C
PRESSURE CLASS	#600			

FIELD AREA ZONE II, GROUP IIA, IIB, T3
INLET OUTLET LINE SIZE : 12"
PIPE SCHEDULE : SCH 80
PIPE MATERIAL : ASTM A333 GR6 / API5L×70
FLANGE RATING : ANSI 600# RF

NOTES:

1) INLET & OUTLET MATCHING FLANGES OR ELBOW, STUDS, NUT & GASKETS NOT IN DMCIPL SCOPE.
2) VENT WILL BE MIN. 3.0 MTR. HEIGHT FROM SKID BASE.
3) 6MM THK. COPPER JUMPER WILL BE PROVIDED AT EACH FLANGES CONNECTIONS.
4) DRAIN WILL RUN UP TO EDGE OF THE SKID.
5) DANIEL WILL PROVIDE TIE OFF POINT FOR EACH DRAIN FLANGES CONNECTIONS.
6) CONNECTIVITY FOR RTU/SCADA WILL BE PROVIDED AT THE TERMINAL STRIP OF CONTROL PANEL. FURTHER CONNECTION IN CUSTOMER SCOPE.

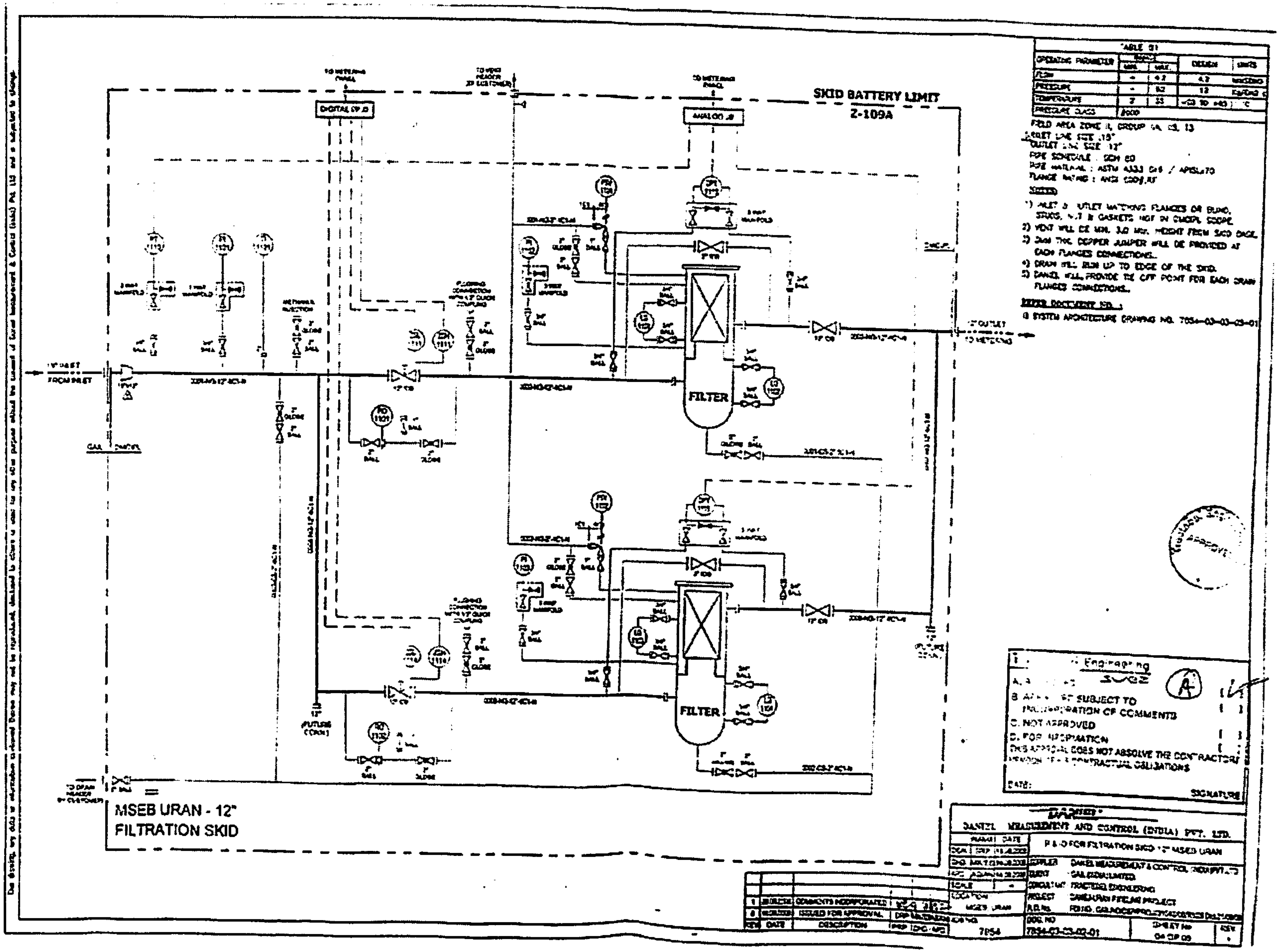
REFER DOCUMENT NO. :

1 SYSTEM ARCHITECTURE DRAWING NO. 7354-03-03-05-01

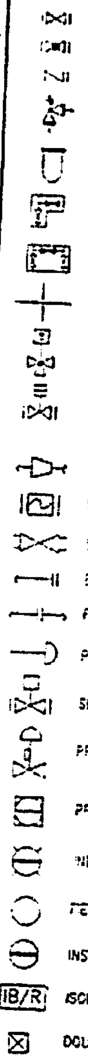
[illegible] Engineering
A. [illegible]
B. [illegible] SUBJECT TO [illegible] OF COMMENTS [ ]
C. [illegible] [ ]
D. [illegible] [ ]
[illegible] DOES NOT RELIEVE THE CONTRACTOR/ [illegible] CONTRACTUAL OBLIGATIONS
DATE: SIGNATURE

DANIEL MEASUREMENT AND CONTROL (INDIA) PVT. LTD.
P & ID FOR METERING SKID 12" MSEB URAN
SUPPLIER: DANIEL MEASUREMENT & CONTROL (INDIA) PVT. LTD.
CLIENT: GAIL (INDIA) LIMITED.
CONSULTANT: [illegible] ENGINEERING
PROJECT: [illegible] PIPELINE PROJECT
LOCATION: MSEB URAN
DOC NO. 7354-03-03-02-01
SHEET No. 03 OF 38
REV. 1

1	[illegible]	COMMENTS INCORPORATED
0	[illegible]	ISSUED FOR APPROVAL
REV	DATE	DESCRIPTION


SKID BATTERY LIMIT
Z-109A
DIGITAL
ANALOG
12" INLET FROM
GAIL
12" OUTLET TO METERING
FILTER
FILTER
12" FUTURE CONN.
FUTURE CONN.
MSEB URAN - 12"
FILTRATION SKID
TABLE 01
OPERATING PARAMETER
MIN.
MAX.
DESIGN
UNITS
FLOW
PRESSURE
TEMPERATURE
PRESSURE CLASS
FIELD AREA ZONE II, GROUP IIA, IIB, T3
INLET LINE SIZE 12"
OUTLET LINE SIZE 12"
PIPE SCHEDULE : SCH 80
NOTES
1) INLET & OUTLET MATCHING FLANGES OR BLIND, STUDS, NUT & GASKETS NOT IN CUSTOMER SCOPE
2) VENT WILL BE MIN. 3.0 MTR. HEIGHT FROM SKID BASE
3) COPPER JUMPER WILL BE PROVIDED AT EACH FLANGES CONNECTIONS.
4) DRAIN WILL RUN UP TO EDGE OF THE SKID.
5) DANIEL WILL PROVIDE TIE OFF POINT FOR EACH DRAIN FLANGES CONNECTIONS.
REFER DOCUMENT NO. :
SYSTEM ARCHITECTURE DRAWING NO. 7054-03-03-03-01
Engineering
A.
B. APPROVED SUBJECT TO INCORPORATION OF COMMENTS
C. NOT APPROVED
D. FOR INFORMATION
THIS APPROVAL DOES NOT ABSOLVE THE CONTRACTOR OF CONTRACTUAL OBLIGATIONS
DATE:
SIGNATURE
A
DANIEL
DANIEL MEASUREMENT AND CONTROL (INDIA) PVT. LTD.
NAME
DATE
P & ID FOR FILTRATION SKID 12" MSEB URAN
SUPPLIER
CLIENT
CONSULTANT
PROJECT
SCALE
LOCATION
MSEB URAN
1
COMMENTS INCORPORATED
0
ISSUED FOR APPROVAL
REV
DATE
DESCRIPTION
PREP
CHKD
APPD
DOC. NO
7054-03-03-02-01
SHEET No
04 OF 05
REV
7054

SYMBOLS



MANUAL BALL VALVE
MANUAL GLOBE VALVE
CHECK VALVE
PRESSURE OR THERMAL RELIEF VALVE (FLANGE)
FILTER
3 WAY MANIFOLD
5 WAY MANIFOLD
CHANGE OF PIPING CLASS
ON-OFF VALVE (SOLENOID ACTUATOR)
ISOLATION VALVE WITHOUT HANDWHEEL (GAS ACTUATED)
REDUCER CONCENTRIC
ULTRASONIC METER
SOCKET WELD END
BLIND FLANGE
FLANGED CONNECTION
PIPE CAP
SLAM SHUT VALVE
PRESSURE REDUCING VALVE (FLANGE)
PROCESS CONTROL/SHARED DISPLAY INSTRUMENT
INDICATING LAMP ON LOCAL PANEL
FIELD MOUNT INSTRUMENTS.
INSTRUMENT MOUNTED ON LOCAL PANEL
IB/R ISOLATING BARRIER/REPEATER
DOUBLE STAGE 2S316 REGULATOR

LINE NOMENCLATURE

0001 - PL - XXX - 6C1 - I1

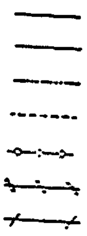
INSULATION (SEE INSULATION CLASS)
CLASS (SEE PIPING CLASS)
LINE SIZE
NG
LINE NO.

INSTRUMENT TAGGING PHILOSOPHY

YYY - 11 XXX

INSTRUMENT NO
STATION NO
INSTRUMENT INDETIFICATION

LINE SYMBOLS



MAIN PROCESS LINE
SECONDARY PROCESS LINE & UTILITIES
BATTERY LIMIT
ELECTRIC SIGNAL
RS 232/485 SERIAL LINK
ACTUATION GAS
TCP/IP ETHERNET LINK

ABBREVIATIONS

PT	: PRESSURE TRANSMITTER
PI	: PRESSURE INDICATOR
TI	: TEMPERATURE INDICATOR
ZSO	: LIMIT SWITCH FOR VALVE OPEN STATUS
ZSC	: LIMIT SWITCH FOR VALVE CLOSE STATUS
PSV	: PRESSURE SAFETY VALVE
RO	: RESTRICTION ORIFICE
LG	: LEVEL GAUGE
DPT	: DIFF. PRESSURE TRANSMITTER
IDB	: INTEGRATED DOUBLE BLOCK & BLEED
XSC	: SOLENOID VALVE CLOSE COMMAND
XSO	: SOLENOID VALVE OPEN COMMAND
DPS	: DIFF. PRESSURE SWITCH
FT	: FLOW TRANSMITTER
AT	: GAS CHROMATOGRAPH ANALYZER
FCIC	: FLOW TOTALIZER / INDICATOR COMPUTER

ABBREVIATIONS

TT	: TEMPERATURE TRANSMITTER
TW	: TEST THERMOWELL 1
SV	: SOLENOID VALVE

Tractebel Engineering APPROVED

[illegible] Engineering
A APPROVED
B APPROVED SUBJECT TO INCORPORATION OF COMMENTS
C NOT APPROVED
D FOR INFORMATION
This approval does not absolve the contractor/vendor of his contractual obligations
DATE:
SIGNATURE

A

DANIEL
DANIEL MEASUREMENT AND CONTROL (INDIA) PVT. LTD.

	NAME	DATE	
DGN.	BRP	25.08.2008	P & ID SYMBOLS & ABBREVIATION, MSEB URAN
CHD	MK/SS	25.08.2008	SUPPLIER : DANIEL MEASUREMENT & CONTROL (INDIA) PVT. LTD.
APD.	AS/AN	25.08.2008	CLIENT : GAIL (INDIA) LIMITED.
SCALE	-		CONSULTANT : TRACTEBEL ENGINEERING
LOCATION : MSEB, URAN			PROJECT : DAHEJ-URAN PIPELINE PROJECT
JOB NO. 7854			P.O. NO. : FOI NO : GAIL/ND/C&P/PROJ/01042/DUPL/25 Dt.21.03/06
			DOC. NO. 7854-03-03-02-01
			SHEET No. 03 OF 08
			REV. 1

REV	DATE	DESCRIPTION	PRP.	CHD.	APD.
1	29.09.2008	COMMENTS INCORPORATED	[illegible]	[illegible]	[illegible]
0	14.09.2008	ISSUED FOR APPROVAL	MAS	MK/SS	AS/AN

A3 - 420x297 SHEET

REFERENCE:-

- SCADA techr.ical information bulletin 2004.
- Digital flow c›mputer manual.
- Implementatic›n procedure by Emerson industries.
- Senior sonic gas flow meter manual.
- **Process contı ol** handbook 3 –Bela G liptak.
- Curtis, Ken, A., DNP3 Protocol Primer, DNP Users Group, 1 June 2000
- *McClanahan, R.H.,* **The Benefits of Networked SCADA Systems Utilizing IPEnabled Networks,** Rural Electric Power Conference, 2002. 2002 IEEE, 5-7 May 2002 Pages: C5 - C5_7.