A Guide to Design a PLC and SCADA based Industrial Automation System

Manisankar Dhabal[1], Durgesh Lingampalle[2], O P Ullas[3]
[1,2,3]*Hot Lab Utility & Engineering Services Section, NFG, Bhabha Atomic Research Centre*

Abstract **- PLC and SCADA based industrial automation system is the most widely used control system employed in present scenario and its application is increasing very fast. Starting from a small equipment control to a large plant control these systems are used. Manufacturer also finds it very convenient to use PLC in place of embedded control for their flexibility. Although PLC and SCADA system is a generic term the ranges of product available have wide variety. It depends upon the requirement of the system. Very often it is selected based on manipulated suggestion received from the system integrator or a vendor. It may either results into a costly or a compromised product due to lack of basic knowledge about design techniques. This paper describes a very simple method to PLC and SCADA based system. It will be useful for the actual process engineers who gives the whole work to a turnkey vendor or to a consultant. The method helps to design an architecture as well as select seize of major components. While explaining a general building services system has been taken as an example**

Index Terms **- PLC,RIO, IO, SCADA**

Abbreviation: RIO: Remote IO Module, PL: Plant, B1: Building 1, B2: Building 2, FO: Fibre Optics, LAN: Local Area Network, L2: Layer 2, L3: Layer 3, LIU: Live Interface Unit, SFP: small form-factor pluggable

INTRODUCTION

Automation system is used in most of the industries, and they are applied in all sectors. The widely used industrial automation is PLC and SCADA based system. There are industry standards available for PLC, SCADA which defines specification and performance requirements. Online tools are available with various manufacturer to select their package or product. But it does not help to design a complete system. PLC programming is done by a certified engineer only whereas programming in SCADA is also done by an expert only. All plant or industry does not have an in-house expert with them to design a system for their plant. They need to hire a consultancy to design a system who brings a system integrator. [5, p.265]. System integrator executes the overall automation work with the help of other electrical, mechanical contractor. It has been found that if the plant or industry person does not adequate understanding of the design, the finally installed automation platform is not optimally designed. It is necessary to have a knowledge of an automation system design for any plant person who want to purchase and install such system. Online survey and literature study has been done on design of an automation platform with PLC and SCADA system. The available literature are specific to a particular type of a process control design with custom made controller or software. A manufacturer product catalogues explains various hardware configuration and architecture however those require a very depth knowledge in automation system. There are lot of books and documents available PLC programming, SCADA programming however no such literature is therefore for designing overall system which is understandable to a person not much familiar with automation components design. The intent of writing this article is to help any plant or industry to design PLC and SCADA based automation system without need of in-depth knowledge of such components. The paper in a very small article explains how to assess the capacity of automation system and then guide the reader to calculate size of each of the component of the automation system. The calculation method based on few simple approaches which is very obvious but is not found any book or literature. It also gives an idea of the safety aspect which a plant may or may not consider. Very often it has been found that miscellaneous redundancy is considered to make the plant safer but an important aspect is missed out. This document will help a reader to optimally design a PLC

and SCADA based automation system even though he does not have adequate knowledge of such system.

BASIC INDUSTRIAL AUTOMATION SYSTEM

The basic intent of industrial automation system is to monitor and control an equipment from a PC based system from a remote place which is often called as a control room.

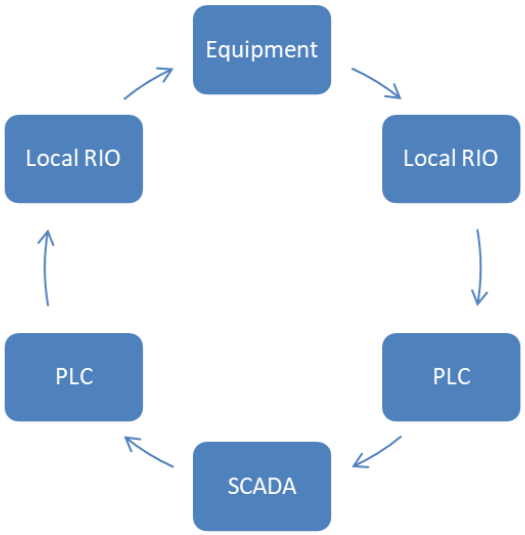

Fig 1 Basic Industrial Automation Scheme

A basic flow diagram is given in Fig 1. This require an equipment needs to be connected one or multiple input output module which is referred as a Remote Input Output Module (RIO). These modules are also referred as RTU [2, p.89] by some vendor. The status of the equipment is given to the RIO panel which send the data to a programmable logic controller (PLC). PLC send the data to a SCADA system which is run in a PC based environment running on windows Operating system. The status of the equipment and process is shown in a graphical environment through various animation and P&I diagram. Buttons are also designed in animated text to send command to the equipment. The command is processed by the PLC which sends back the data to the RIO. The RIO with the help of its various output module changes the equipment and process as directed by SCADA. The connection between RIO, PLC and SCADA is a communication cable whereas the connection between the RIO and the main equipment or process is control cables. This gives the idea of various components of an industrial automation system which is shown in Fig 2.

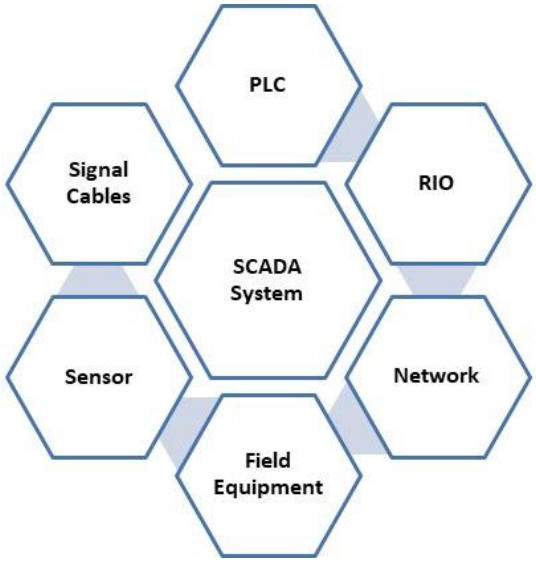

Fig 2: Components of an Industrial Automation System

SCADA System is obviously the heart of the system which is surrounded by PLC, RIO and their interconnecting network, various sensor and equipment pertaining to the process and the signal cables establishing their connection with the RIO.

DESIGN THE CAPACITY OF AN AUTOMATION SYSTEM

Before designing the automation system equipment, it is necessary to design the capacity of the automation system required. In order to design the system first step is to break the overall system of process into smaller process, then break into sub process, subsequently to individual equipment, sub equipment. The process of breaking into smaller process is shown in Fig 3. It may be noted that the abbreviation used in the figure are not standard. It is used solely for explanation purpose.

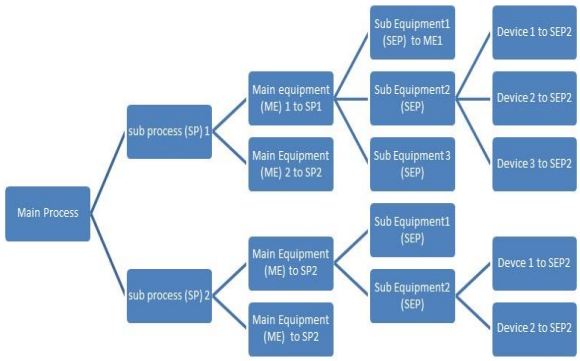

Fig 3: Method to break into small process

The next to be to take a practical example of a large process. The method is explained with a Ventilation and Utility Control plant which is divided into small systems in Fig 4. A Plant Utility Services (PL) is broken into three major process which are Building 1 Services (B1), Building 2 services (B2) and Common services. For explanation only B1 services is broken into small process which are listed as compressed air services, effluent storage system, One through ventilation system, re-circulatory ventilation system , Fire Alarm System (FAS), Power system, Air sampling system. Again for explanation purpose one though ventilation system is broken into 3 major systems which are Fume Hood Exhaust plant (FH) ,exhaust air plant and supply air system. It may be noted that once through ventilation system is used for area where potentially contaminated air is there and materials are handled which may generate toxic gas or contaminated particles. Here one major equipment exhaust system is selected to break into small equipment such as a blower, suction side damper, discharge side damper, a motor driving the blower, a starter for start stop control of the motor and air filtration system. In the same method all major process has to be broken into smallest equipment and make a list all equipment.

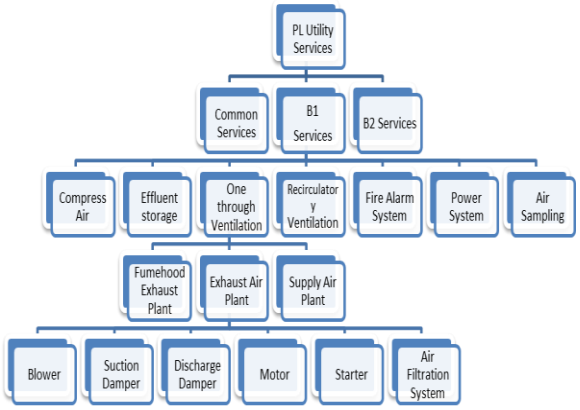

Fig 4: An Utility Plant Services system broken into small equipment

CALCULATION OF IO

As we have broken to the process into small equipment the next step is to calculate the no of input and output parameters (IO). An input parameter is used to read the status of a system where as output parameter is to control the process. For the explanation a suction damper and a starter is taken which will cover all types of input and output parameters used in the industrial automation system. In this process it is required to ask yourself what is the thing you want to monitor for this equipment and what is the thing you to control for this equipment. In the figure 5 the breaking down activity is shown.

ANALOG INPUT AND OUTPUT PARAMETERS

The suction damper is a modulating device which is used to block percentage of air. In this case it is a motorised damper which vary its position depending upon the electrical signal given to it. We may like monitor how much percentage the damper is opened in a running plant. So it is an IO and is called Analog input (AI). Electrical signal given is an Analog output (AO) which is another IO.

SOFT IO PARAMETERS

If the starter is taken it has some other important and distinct equipment as a part of the system. A microprocessor based relay (µP) , a smart meter and the control circuit. In the case shown the microprocessor relay and smart meter has a communicable device inbuilt and it can share data to a third party system vide serial communication [7,p.34]. These devices sometimes available in form of IOT devices [6, p.65] also. In microprocessor based relay the protection setting is required to be monitored from a SCADA system and hence the parameters will be a soft IO parameters.

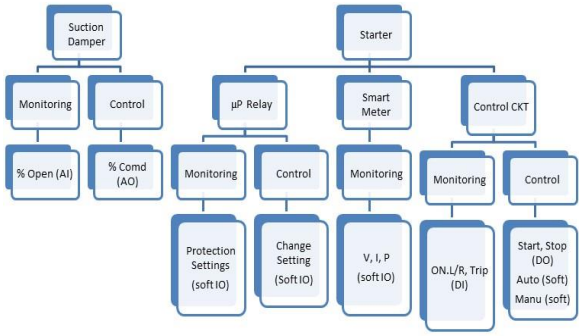

Fig 5: Breaking into IO Parameters

The protection system may be required to change from SCADA and hence control of the setting also are soft IO parameters. Similar is the case of a smart meter

where Voltage, current and power is required to be monitored and hence they will be a part of the soft IO parameter. As in meter there is nothing to controlled hence no control function is listed for the matter.

DIGITAL INPUT AND OUTPUT PARAMETERS

In the starter control circuit there are contactor and relays which gives status of the motor whether running or tripped. Hence for the list of parameters to be monitored are ON Status, Trip Status, Status of Local/Remote hardware selector switch status. This information is digital and hence these are Digital input (DI) parameters. Start and stop command to the blower is given through the starter and hence start and stop will be the control parameter and are Digital output (DO) parameters as these are discrete in value. The blower may be required to keep in auto and manual mode but there is no hardware button required for auto and manual. It can be set from the SCADA or PLC program and hence these will be soft IO parameters discrete in nature.

CAPACITY OF AUTOMATION

The parameters have been divided into DI, DO, AI, AO and soft IO parameter. The way explained above needs to be applied for all the process and a total of all the parameters will be the basis of selection for all the automation equipment.

RIO

An RIO as already discussed is a remote input output module which is in form of a panel. If there are large no of IOs distributed over a large area, it is divided into various RIO.

CONSTRUCTION OF A LOCAL RIO

It is very important to note that IOs are geographically scattered in very large areas. Hence RIOs are used. It is basically a part of PLC distributed in various location. Only the logic part is in PLC. This helps to save wire and has other advantages also and breaking into smaller RIO is a standard practice in distributed IO. We need to geographically separate the IOs and make cluster. In each area total no of different types of IOs needs to be calculated. It may be from various other process. Only a part of the process may be there. In Fig 6 exhaust blower one part is in RIO1 whereas the remaining part is RIO2.

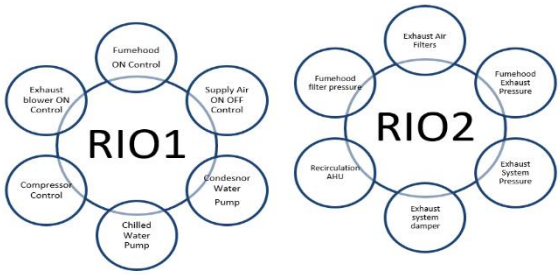

Fig 6: Constructing a Local RIO for IOs located in same geographic location

In RIO1 there are other equipment pertaining to Once through ventilation system as well other common process also. Similar is the case of RIO2. Thus IOs are segregated into various RIO not in form of functional groups but in form of geographical distribution.

MAIN COMPONENTS OF RIO

As per the type of IOs used four cards are used in the RIO for connecting to field equipment and these are DI Module, DO Module, AI module and AO Module. If there are soft IO devices available serial network card is required and a module for appropriate serial communication is required. If the soft IOs are of IOT based and support TCP/IP communication [7, p.14] a TCP/IP card would be necessary. The data from the RIO is sent to PLC with the help of Co-processor where all digital data is processed and converted into a digital and communication platform. The most widely used communication platform is Ethernet communication [3, p.112] works on TCP/IP protocol although there are various other methods available and it may be consulted with the respective vendor for the availability. All these cards are housed in a slotted electronic card based plane which is called back plane. A power supply card is required for the backplane as well as for specific cards. Fig 7 shows the various cards housed in a backplane. The quantity of each type of card will depend on the no of IO and channel density [4] used for the particular card.

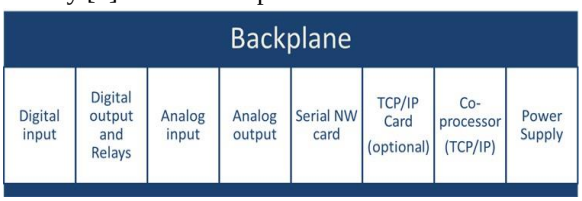

Fig 7: Various Components and their mounting in an RIO

OTHER COMPONENTS INSIDE AN RIO

Other components used in RIO panel are relays for isolation of field equipment from PLC, SMPS for providing power to Analog module, cooling fan for cooling of the panel components, fuses for channel protection.

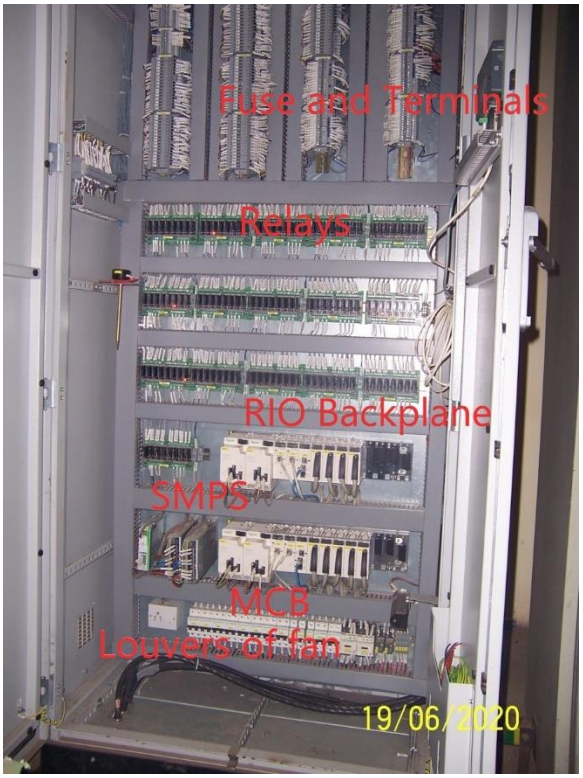

Fig 8: Various Components inside an RIO

REDUNDANCY IN RIO

If we want our control system not to be dependent on a specific equipment some commonly available redundancy needs to be considered. Available redundancies are power level redundancy where multiple power supply cards is used. Communication level redundancy used by providing multiple communication cards as well as considering some other aspects in the network design Card redundancy to perform same task with two card. Say we are measuring static pressure. It can be measured by two instruments giving feedback to two separate IO card. If multiple cards like power, communication and IO cards are used they can be placed in same rack or in different rack. If multiple racks are chosen then it is called backplane redundancy This is to be noted that complicacy in program increases as we go on adding multiple IO cards. Other redundancy does not have much involvement in programming.

RIO TO PLC CONNECTION

In a plant or in a control system there might be a number of RIO and a PLC and SCADA. Connection of RIO to PLC is in a network. This network can be star or ring or bus or a combination of them [1, p.357]. This may be noted that based on the component we select the corresponding networking card type will get changed.

SELECTION OF PLC

There are huge number of PLC available in market and the interesting part is that most of them are capable to carry out a majority of the functions normally used in the control system. Basic selection will be dependent on no of IO handling capacity. However as we go on adding features as per other requirements which are also important the PLC becomes more advanced. Programming becomes easier when software supports real text based IO parameter names. Online changes possible [1, p.199] on higher version is selected. Remote connection, maintenance, downloading capability, local display etc are available in far more advanced version. If safety and security aspects are required in depth further higher version required. As features are added price also increases. So an awareness of these functionality and their use is required. Fig 8 shows that the price increases as the features are added.

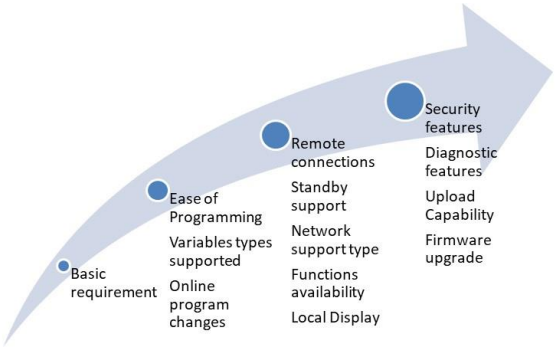

Fig 9: Selection of PLC with various advanced features

COMPONENTS OF A STANDARD PLC RACK

In a standard PLC rack main PLC controller is kept in backplane along with network card for scanning of IOs from RIO panels and another network card for communication with SCADA system. Power supply card is required as usual for any backplane and hence for the PLC rack also. However as there is no IO capacity of power supply card may be chosen less.

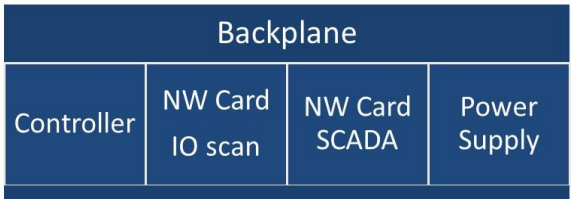

Fig 10: Components of a PLC Rack

REDUNDANCY IN PLC PART

Similar power, communication redundancy is available for the PLC panel also. Interesting part is controller redundancy. Here two controller stays in synch mode with a fibre optics or cat-6 connection. These two controllers can be in same panel, separate panel or at two different building also. While using power and communication redundancy source of power to the PLC can be taken from independent sources to make it further independent of the source availability.

SCADA TAG CALCULATION

Capacity of SCADA system is expressed in terms of SCADA tag. Tags are various variables directly linked and used in PLC as well as in graphical interface of SCADA. Let us take an example of a tank level which is sensed by an AI module and the sensor is used for automatic pumping for a level control. This data is received in voltage or current form and digitally converted in the range of 10000 depending upon the type of ADC [4] used in the AI module. It require a variable to use in SCADA and hence will be one tag. Now we need scaling variable for low- and high-level scaling. We need set points variable for low, high level alarm, set points for auto pumping ON and OFF. On an average 15 variables may be required to use in SCADA and hence 15 tags on average can be taken for SCADA tag calculation. In the same way depending upon the use of the DI, DO, AI, AO no of tags shall be considered. In the Figure 11 for each DI total 4 nos of tags is considered for each DI and total no of tags for 800 nos of DI shall be 3200. IED are intelligent devices [6, p.19] and each device may contain a large no of data. Consider a smart meter where three phase Voltage, current and power is monitored and is used for SCADA system. The no of data used in each system and the useful data may really vary in different system. In the figure average 10 useful data is considered and for each data 5 tags are considered. In this method total no of tags shall be calculated and some spare tags of 10 to 20% must be kept.

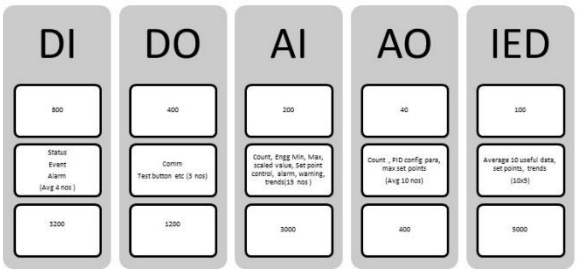

Fig 11: SCADA Tag Calculation

SCADA SYSTEM LICENSE

SCADA software licenses are available in different form. A SCADA system require a server and a client. The server is called an IO Server. Server licenses are available in limited or unlimited license form. Control client license are also available in tag based but it may be a static license where the USB dongle is locally kept on the client computer. A floating license means the client station will be authorised from server and no separate hardware will be attached. Other license are view only client which is only for viewing , web view only client which is only viewing from an web browser and web control client which is control and view from an web browser based application.

HISTORIAN SERVER SELECTION

Historian server is used for generating a report and storing old statistical data as well as carrying out analysis. Its license is also available in tag form. We need not consider all the data or tags for the reports. For a 15000 tag based SCADA it may happen that only 3000 data is required for the report and storage. So Historian will be for 3000 tags only.

In the example given in Fig 12 Exhaust blower all SCADA data is shown. However only 5 data is required for the report as balance data is not so important for checking historical records

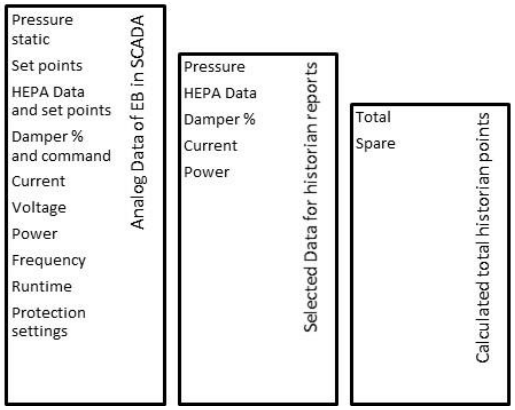

Fig 12: Historian Tag selection example

HARDWARE COMPONENTS OF SCADA

Hardware components of SCADA means various types of computers. Commercial PC is preferable only for viewing station of web view stations. For SCADA client station touch screen industrial PC is the preferred one. Higher grade windows PC are used for the IO server application although Server grade PC is mostly preferable for historian and SCADA IO server. Fig 13 shows different types of PC and their uses in SCADA systems

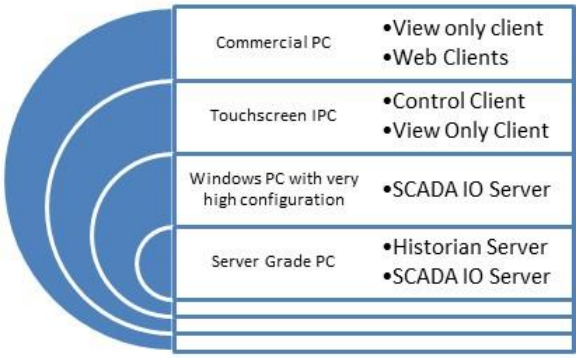

Fig 13: Use of Computers in SCADA system

REDUNDANCY IN SCADA

Redundancy is available in SCADA system also. Fig 14 shows various redundancy available in SCADA. IO Server can be used in hot standby configuration. In each device level hardware level redundancy is given in form of power and communication level. With a server grade PC of very high configuration power and communication redundancy option is available although it can be made externally also by commonly available other methods[15]. A control client can be used in multiple and each device can be provided communication redundancy if IPC is used. Power redundancy requires additional hardware as it is normally not available in COTS [16] products. Redundancy in historian server level is available but not very common to use.

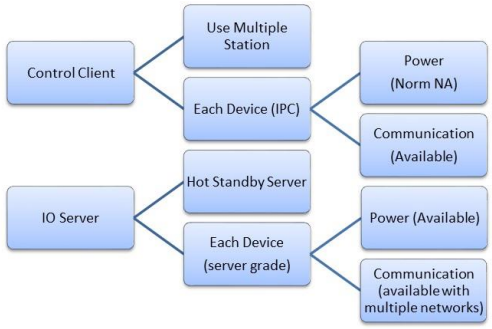

Fig 14: Various Redundancy in SCADA system

OTHER COMPONENTS IN SCADA SYSTEM

Other components of automation systems are various types of cables and networking components, sensors, transmitters etc. as shown in Fig 15. These components are also equally important and a good design require proper selection of these components also.

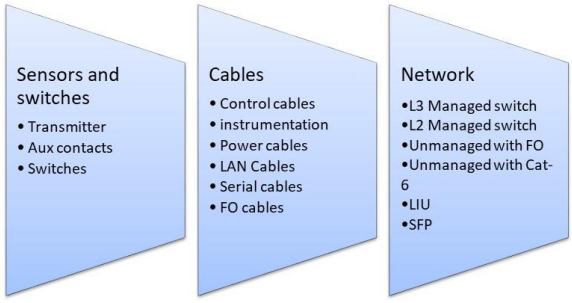

Fig 15 Other Components of SCADA system

SECURITY ASPECTS

Security and safety aspect is vast topic. Security means mostly cyber security for the networking components and the computer-based systems such as SCADA, PLC, RIO etc [6, p.15]. Many components of the automation system are connected in a network. Some components are computer-based system. Those needs to protected for unauthorised access, malicious software etc. especially when the application is of

critical nature. Following are few major security threats

(a) Operating system of the SCADA station gets corrupted. Malicious software is supressing various alarms. As a result of that operator will not come to know about the abnormality.
(b) PLC and RIO logics are once developed does not require any maintenance. If it is accessed by unauthorised person logic can be deliberately changed resulting in unsafe situation.
(c) As a result of attack on the automation components wrong information are displayed and based on that operator may take wrong action
(d) Malicious Software infection causes force shutdown of the complete control system
(e) In chemical industry important recipe is written on the logic which may be stolen by attacker as a result of cyber-attack. This information are intellectual property of the respective industry owner.

COUNTER MEASURES NEEDED FOR SECURITY THREATS

All computer-based stations should have updated antivirus. Plugging of portable USB device must be restricted. PLC and RIO should be kept in a separate network. Which is isolated from any business network or internet. If the data needs to be shared in the internet it should be through multiple firewall. Even though the systems are isolated from internet it may happen that through removable storage device malicious software gets injected in the whole control system. Additional pre-caution needs to be taken during firmware upgradation process Remote access is often allowed for PLC for getting support from vendor over internet. It opens up a path for the hacker. Hence remote access should be avoided. Common network security features are available with major components however smart field devices sometimes lag security features. Again as higher version networking components are selected more layer [8, p.22] of security will be available. But most important is awareness about the security events and threats by all users of the SCADA station. Internal threats due to disgruntled employee of the same organization is also a potential threat which should be combat with access control with multiple layers.

SAFETY ASPECTS

Safety issues arises when the components failed prematurely leading to unsafe incidents. Therefore, redundancy is considered as discussed in each section. However, redundancy in field equipment level also required. As we require more safety more number and level of redundancy would be required. An index called safety Integrity Level [9, p.8] is used automation system for assessing the amount of safety required to be considered. This index is determined both by quantitative and qualitative analysis of any process control. Commonly used techniques are fault tree analysis, consequence analysis, likelihood analysis, event tree analysis, Layer of protection analysis (LOPA) Based on safety requirement selection of components gets changed. A power supply module part number will get changed when it is redundant type although of same rating. Similarly the backplane, network module, IO cards will get changed when those are redundant type or with specific safety integrity level.

IMPLEMENTATION AND COMMISSIONING

Once the design of the scheme and selection of the components are done detailed specification is made and components are procured. PLC, RIO panels are taken up for fabrication and assembling the components. Meanwhile a logic document is required to be prepared so that a programmer can refer them and make the program independently. This is called process control logic document (PCLD) which consists of overall process, equipment and parameters involved with each process, list of set points, details of various modes of operation, special requirements of interlocks and safety. On getting the PCLD programmer starts developing PLC logic and SCADA programmer stars developing graphics in SCADA screen. In parallel to this activity cabling at site is done. Once the PLC and RIO panels are ready it is important to check all input outputs terminals. PLC program and SCADA program developed are required to be vetted in simulation. In this a big logic is tested in small parts. Once logic is checked it is downloaded in PLC. PLC and RIOs are installed at site and all field terminals are connected. A process may have multiple individual equipment controlled by many sub equipment. During commissioning process each of the

small equipment are tested with PLC logic. It may be found that logic is required to be changed multiple times during this process. After all individual equipment are tested the overall process is checked. Again during this stage logic may be required to change further. Once the functionality of the overall system is checked it is tested for various abnormal conditions. System should not develop unsafe incidents in none of the abnormal situation. PLC logic and hardware connections must ensure it.

CONCLUSION

The article explains how capacity of required automation system can be worked out from a list of available process and equipment. Once capacity of automation system is obtained it is very simple to select rest of the components. With this knowledge a plant owner may design his own automation system and directly consult a system integrator for procurement and do not miss out any important aspect. The techniques can be employed for small system containing 5 to 10 equipment's as well as for large systems also. The method is same for any process. The safety and security aspect will get changed depending upon the criticality and vulnerability of the system.The article is expected to be helpful for many people who wants to put PLC and SCADA based automation for their plant. The article has covered only the design part. During execution of the project lot of challenges are faced due to lack understanding of the process required and actual logic made by a programmer. In this paper execution and implementation part is not discussed in details. In future a document will be made which covers a simple method to write a logic document of a very complex process.

REFERENCE

[1] Introduction to Industrial Automation, StamatiosManesis, George Nikolakopolous,
[2] SCADA: Supervisory Control and Data Acquisition , Stuart A. Boyer, ISA, 2004
[3] Understanding TCP/IP: A clear and comprehensive guide to TCP/IP protocols, Libor Dostalek Alena Kabelova, Packet Publishing.
[4] Industrial Digital IO Design Guide, WWW. Maximintegrated.com
[5] Industrial Automation Hands ON, Frank Lamb, McgrawHillEducation,
[6] Cyber-security of SCADA and Other Industrial Control Systems, Edward J. M. Colbert Alexander Kott, Volume 63,
[7] How to Plan, Install, and MaintainTCP/IP Ethernet Networks: The BasicReference Guide for Automation andProcess Control Engineers, Perry S. Marshalland John S. Rinaldi, ISA 2004
[8] Industrial Network Security, Securing Critical Infrastructures for smart Grid , SCADA and other Industrial Control Systems, Eric Knapp, James Broad, Elsevier
[9] Safety Integrity Level Selection, Systematic Methods Including Layer of Protection Analysis, Edward M. Marszal, P.E., C.F.S.E. Dr. Eric W. Scharpf, MIPENZ, ISA