SCADA(Supervisory Control And Data Acquisition)

1.What is SCADA?

1.1 Introduction

SCADA stands for supervisory control and data acquisition. SCADA system is not a specific technology, but a type of application. Any application that gets operating data about a system in order to control and optimize that system is a SCADA application. That application may be a petrochemical distillation process, a water filtration system, a pipeline compressor, or just about anything else For continuous operations we have to provide uninterrupted power supply to the industries. But there are many reasons like breakdown of alternator or increment in load etc. due to which the interruption may be occur in power supply. In this paper we have developed an intelligent system using SCADA which will start spare unit when any one of the running unit will be breakdown or increment in load.

- 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 monitoring 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

1.2 ADVANTAGE OF SCADA SYSTEM

- Saves Time and Money
    - Less traveling for workers (e.g. helicopter ride)
    - Reduces man-power needs
    - Increases production efficiency of a company
    - Cost effective for power systems
    - Saves energy
- Reliable
- Supervisory control over a particular system
- Reduce human resource consumption
- Increase product/project revenue
- Greater accessibility (remotely)
- More security (implementation of user access levels)
- Instantaneous alert on alarms or events
- Organized data records and report generation automatically
- Data analysis (real-time and historical data plotting of graphs, charts, trends, etc.)
- Ensure system availability (implementation of system redundancy)

- Easy user interfaces for interaction (graphical HMI interface with animation for easy understanding)
- Automated calculation

1.3 USES OF THE SCADA

SCADA can be used to manage any kind of equipment. Typically, SCADA systems are used to automate complex industrial processes where human control is difficult. For example in systems where there are more control factors unable to be managed by operators in a control center

- **Electric power generation, transmission and distribution**: Electric utilities use SCADA systems to detect current flow and line voltage, to monitor the operation of circuit breakers, and to take sections of the power grid online or offline.
- **Water, Waste Water Utilities and Sewage**: State and municipal water utilities use SCADA to monitor and regulate water flow, reservoir levels, pipe pressure and other factors.
- **Buildings, facilities and environments**: Facility managers use SCADA to control HVAC, refrigeration units, lighting and entry systems.
- **Oil and Gas Trans & Distributions Wind Power Generation Communication Networks Industrial Plans and Process Control**
- **Manufacturing**: SCADA systems manage parts inventories for just-in-time manufacturing, regulate industrial automation and robots, and monitor process and quality control.
- **Mass transit and Railway Traction**: Transit authorities use SCADA to regulate electricity to subways, trams and trolley buses; to automate traffic signals for rail systems; to track and locate trains and buses; and to control railroad crossing gates.
- **Traffic signals**: SCADA regulates traffic lights, controls traffic flow and detects out-oforder signals.

1.4 Objectives of SCADA

The important objectives of SCADA are to listed below:

- **Monitoring** : Continuous monitoring of the parameters of voltage , current, etc..
- **Measurement**: Measurement of variables for processing.
- **Data Acquisition**: Frequent acquisition of data from RTUs and Data Loggers / Phasor data
  Concentrators (PDC)
- **Data Communication**: Transmission and receiving of large amounts of data from field to control Center
- **Control:** Online real time control for closed loop and open loop processes. **Automation**: Automatic tasks of switching of transmission lines, CBs, etc.

1.5 COMPONENTS

- **Sensors** (either digital or analog) and **control relays** that directly interface with the managed system.
- **Remote telemetry units (RTUs)** These are small computerized units deployed in the field at specific sites and locations. RTUs serve as local collection points for gathering reports from sensors and delivering commands to control relays.
- **SCADA master units (MTU)** These are larger computer consoles that serve as the central processor for the SCADA system. Master units provide a human interface to the system and automatically regulate the managed system in response to sensor inputs.
- **Communications network** that connects the SCADA master unit to the RTUs in the field.
- **IED (intelligent electronic devices**) smart sensors/actuators with intelligence to acquire data, process it, and communicate
- **HMI (human-machine interface)** software to provide for visualization and interaction with SCADA

1.6 ARCHITECHTURE

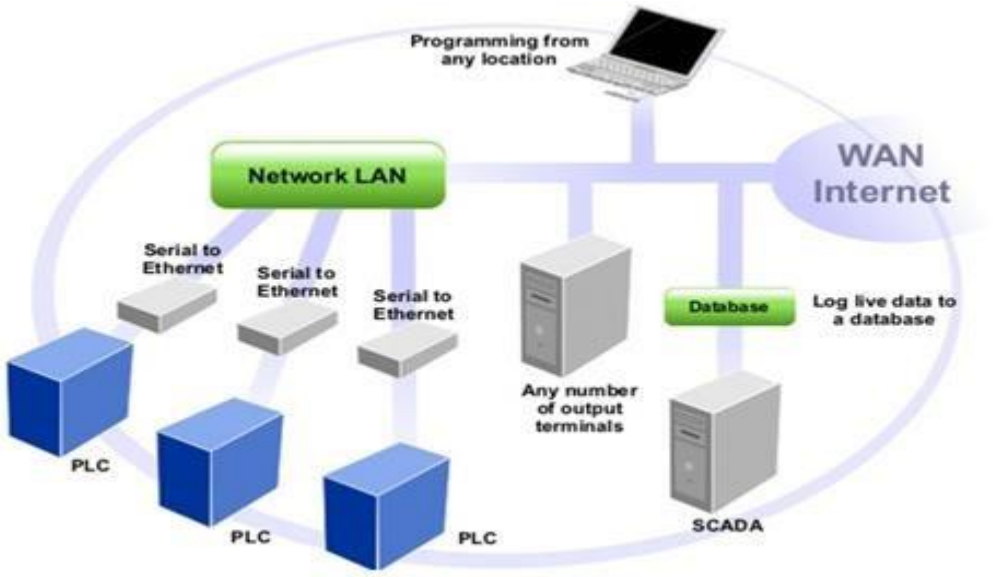
Generally SCADA system is a centralized system which monitors and controls entire area. It is purely software package that is positioned on top of hardware. A supervisory system gathers data on the process and sends the commands control to the process. The SCADA is a remote terminal unit which is also known as RTU. Most control actions are automatically performed by RTUs or PLCs. The RTUs consist of programmable logic converter which can be set to specific requirement. For example, in the thermal power plant the water flow can be set to specific value or it can be changed according to the requirement.

1.6.1 Hardware Architecture:

The generally SCADA system can be classified into two parts:

- **Clint layer-** The Clint layer which caters for the man machine interaction.
- **Data server layer-** The data server layer which handles most of the process data activities

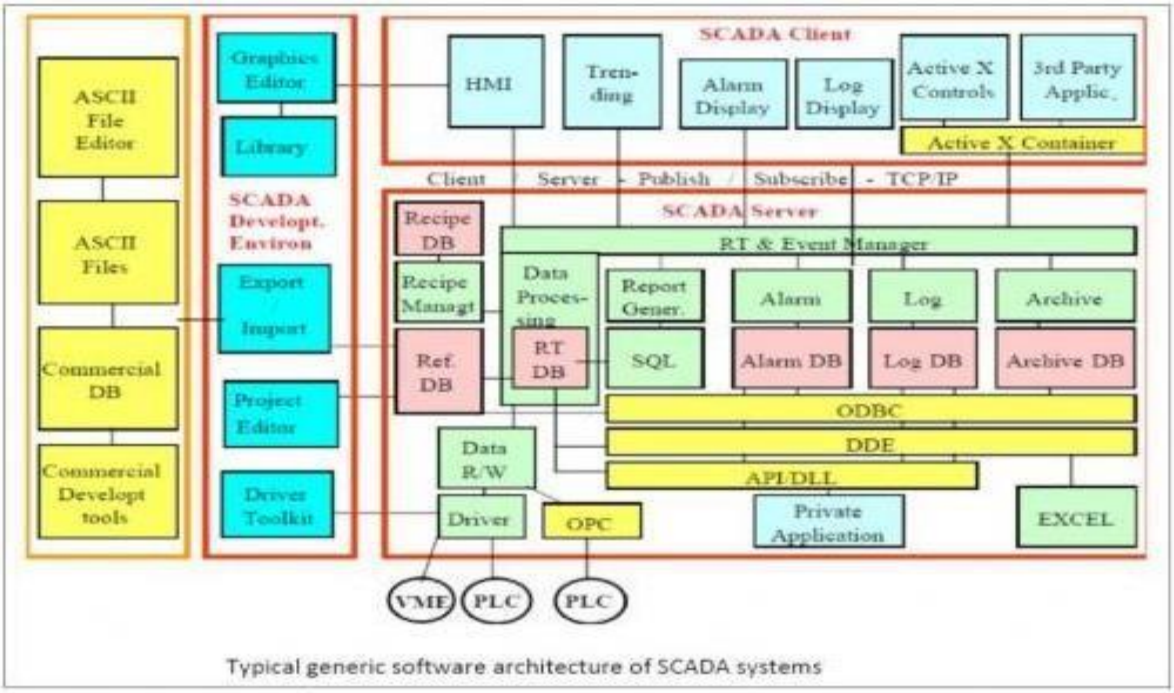
The SCADA station refers to the servers and it is composed of a single PC. The data servers communicate with devices in the field through process controllers like PLCs or RTUs. The PLCs are connected to the data servers either directly or via networks or buses. The SCADA system utilizes a WAN and LAN networks, the WAN and LAN consists of internet protocols used for communication between the master station and devices. The physical equipment like sensors connected to the PLCs or RTUs. The RTUs convert the sensor signals to digital data and sends digital data to master. According to the master feedback received by the RTU, it applies the electrical signal to relays. Most of the monitoring and control operations are performed by RTUs or PLCs as we can see in the figure.



1.6.2 Software Architecture:

Most of the servers are used for multitasking and real time database. The servers are responsible for data gathering and handling. The SCADA system consists of a software program to provide trending, diagnostic data, and manage information such as scheduled maintenance procedure, logistic information, detailed schematics for a particular sensor or machine and expert system troubleshooting guides. This means the operator can see a schematic representation of the plant being controlled.

EX: alarm checking, calculations, logging and archiving; polling controllers on a set of parameter, those are typically connected to the server.



Typical generic software architecture of SCADA systems

1.7 FUNCTIONALITIES OF SCADA

1.7.1 Data Acquisition

First, the systems you need to monitor are much more complex than just one machine with one Output . So a real-life SCADA system needs to monitor hundreds or thousands of sensors. Some sensors measure inputs into the system (for example, water flowing into a reservoir), and some sensors measure outputs (like valve pressure as water is released from the reservoir). Some of those sensors measure simple events that can be detected by a straightforward on/off switch, called a discrete input (or digital input)

1.7.2 Data Communication

In our simple model of the widget fabricator, the “network” is just the wire leading from the switch to the panel light. In real life, you want to be able to monitor multiple systems from a central location, so you need a communications network to transport all the data collected from your sensors. Early SCADA networks communicated over radio, modem or dedicated serial lines. Today the trend is to put SCADA data on Ethernet and IP over SONET. For security reasons, SCADA data should be kept on closed LAN/WANs without exposing sensitive data to the open Internet. Real SCADA systems don’t communicate with just simple electrical signals, either. SCADA data is encoded in protocol format. Older SCADA systems depended on closed proprietary protocols

1.7.3 Data Presentation

The only display element in our model SCADA system is the light that comes on when the switch is activated. A real SCADA system reports to human operators over a specialized computer that is variously called a master station, an HMI (Human-Machine Interface) or an HCI (Human-Computer Interface). The SCADA master station has several different functions. The master continuously monitors all sensors and alerts the operator when there is an "alarm" — that is, when a control factor is operating outside what is defined as its normal operation.

1.7.4 Control

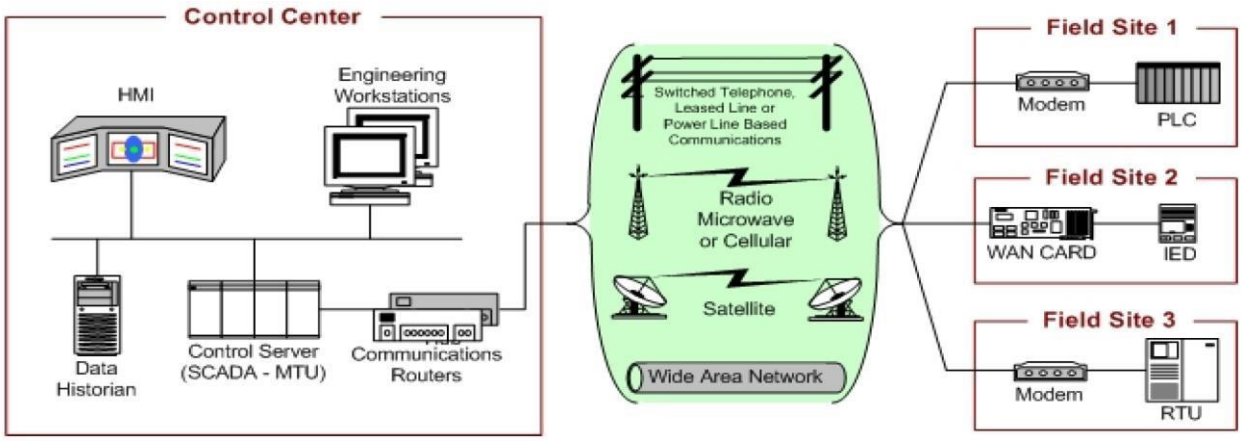
Unfortunately, our miniature SCADA system monitoring the widget fabricator doesn't include any control elements. So let's add one. Let's say the human operator also has a button on his control panel. When he presses the button, it activates a switch on the widget fabricator that brings more widget parts into the fabricator. Now let's add the full computerized control of a SCADA master unit that controls the entire factory. You now have a control system that responds to inputs elsewhere in the system. If the machines that make widget parts break down, you can slow down or stop the widget fabricator. If the part fabricators are running efficiently, you can speed up the widget fabricator.

1.8 WORK FLOW OF SCADA SYTEM

Can be broken down into 3 categories

- NIST representation of SCADA system
    - Control Center
    - Programmable Logic Controllers(PLCs), Remote Terminal Units (RTUs), IEDs
    - Communications Network

The components and general configuration of a SCADA system. The control center houses a control server (MTU) and the communications routers. Other control center components include the HMI, engineering workstations, and the data historian, which are all connected by a LAN. The control center collects and logs information gathered by the field sites, displays information to the HMI, and may generate actions based upon detected events. The control center is also responsible for centralized alarming, trend analyses, and reporting. The field site performs local control of actuators and monitors sensors. Field sites are often equipped with a remote access capability to allow field operators to perform remote diagnostics and repairs usually over a separate dial up or WAN connection. Standard and proprietary communication protocols running over serial communications are used to transport information between the control center and field sites using telemetry techniques such as telephone line, cable, fiber, and radio frequency such as broadcast, microwave and satellite



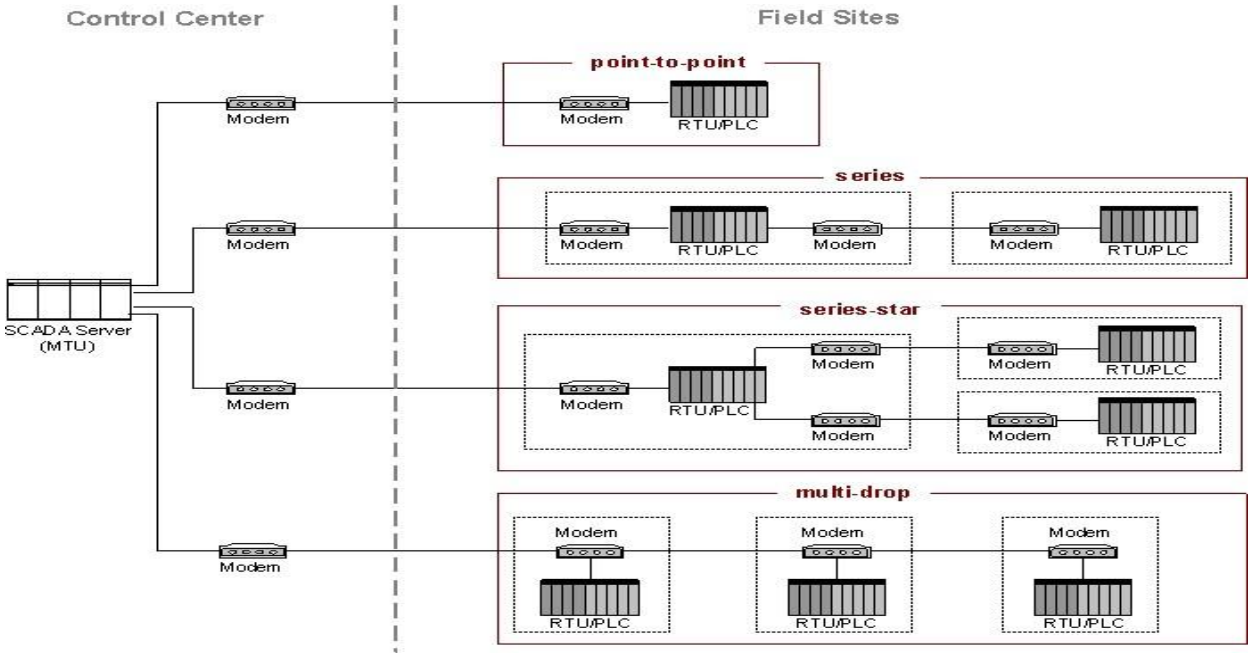
1.9 TYPES OF SCADA SYSTEM

Three types of basic SCADA systems:

- Basic SCADA
  - One machine process
  - One RTU and MTU
- Integrated SCADA
  - Multiple RTUs
  - DCS
- Networked SCADA
  - Multiple SCADA

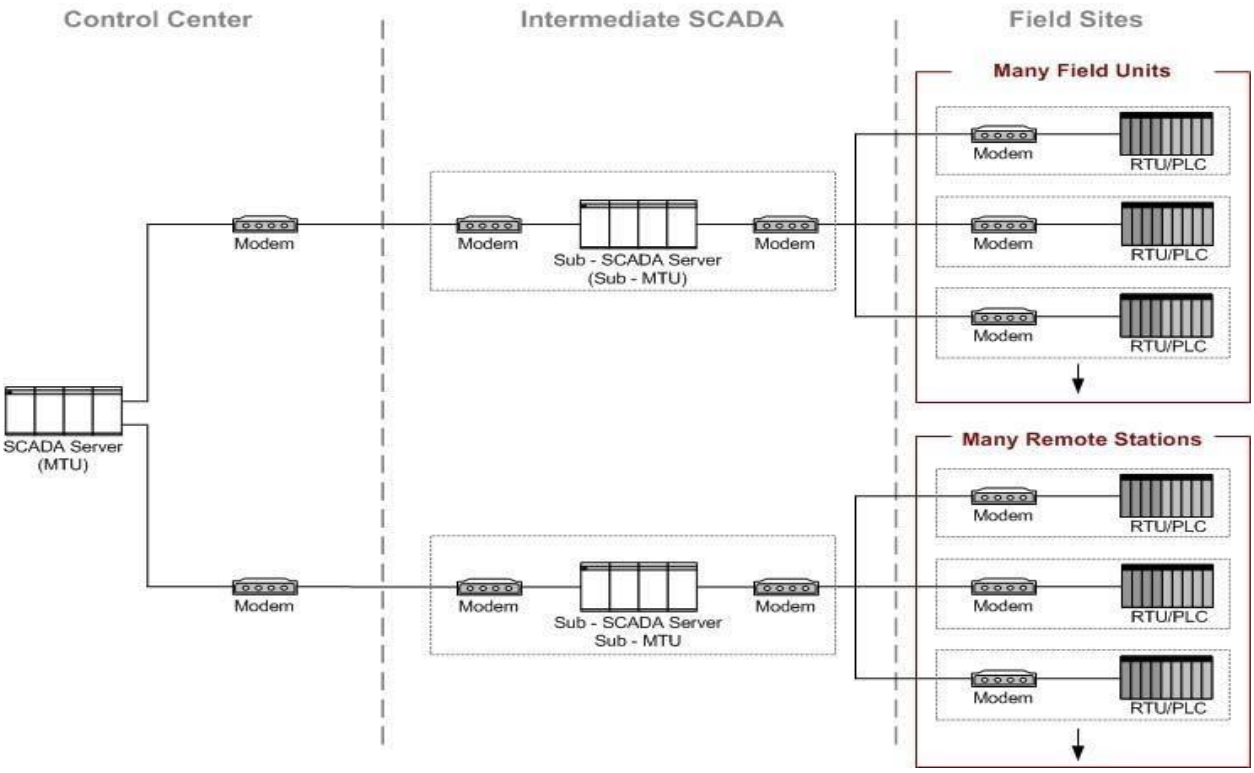
1.9.1 BASIC SCADA System

- Car manufacturing robot
- Room temperature control



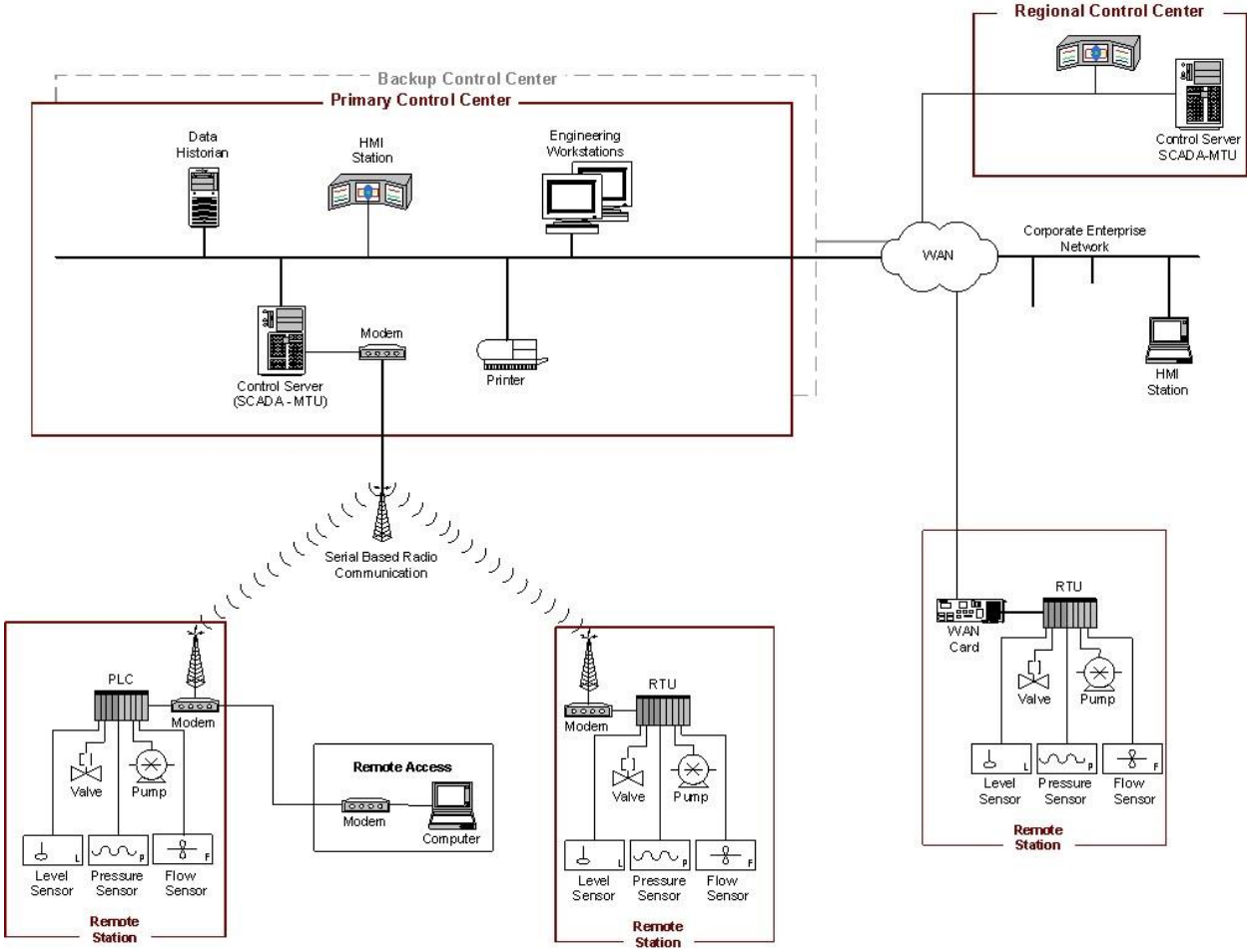
1.9.2 INTEGRATED SCADA System

- Water systems
- Subway systems
- Security systems



1.9.3 Network SCADA System

- Power systems
- Communication systems



2. THREATS and VLUNERABILITIES

2.1 THREATS

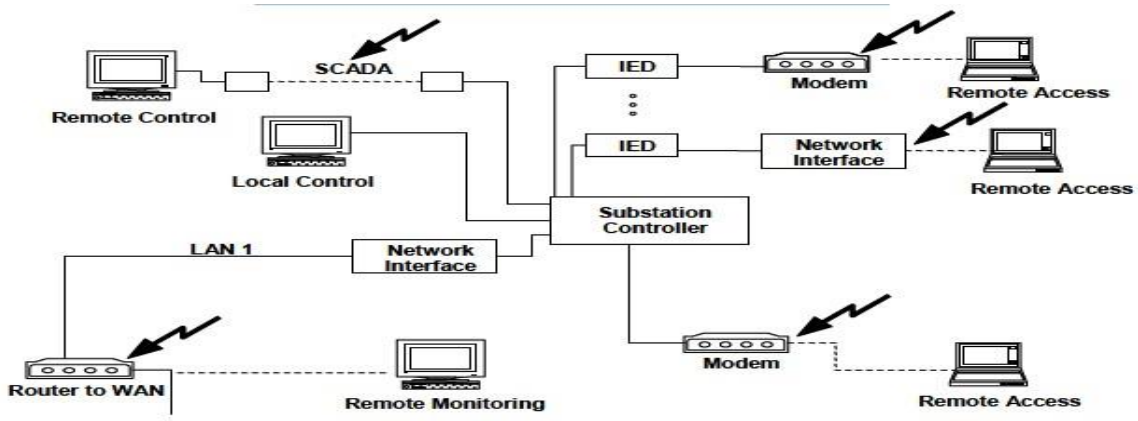
Threats to control systems can come from numerous sources, including adversarial sources such as hostile governments, terrorist groups, industrial spies, disgruntled employees, malicious intruders, and natural sources such as from system complexities, human errors and accidents, equipment failures and natural disasters. To protect against adversarial threats (as well as known natural threats), it is necessary to create a defense-in-depth strategy for the ICS.

2.1.1 Adversarial Threats to ICSs

Threat Agent	Description
Attackers	Attackers break into networks for the thrill of the challenge or for bragging rights in the attacker community. While remote cracking once required a fair amount of skill or computer knowledge, attackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.
Bot-network operators	Bot-network operators are attackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of compromised systems and networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or the use of servers to relay spam or phishing attacks).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the U.S. through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop attacker talent.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrines, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power–impacts that could affect the daily lives of U.S. citizens.
Insiders	The disgruntled insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems. Insiders may be employees, contractors, or business partners. Inadequate policies, procedures, and testing can, and have led to ICS impacts. Impacts have ranged from trivial to significant damage to the ICS and field devices. Unintentional impacts from insiders are some of the highest probability occurrences.
Phishers	Phishers are individuals or small groups that execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Spammers are individuals or organizations that distribute unsolicited e-mail with hidden or false information to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (e.g., DoS).
Spyware/malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.

2.2 VLUNERABILITIES

2.2.1 Vulnerable Points



2.2.2 Policy and Procedure Vulnerabilities

Vulnerabilities are often introduced into ICSs because of incomplete, inappropriate, or nonexistent security documentation, including policy and implementation guides (procedures). Security documentation, along with management support, is the cornerstone of any security program. Corporate security policy can reduce vulnerabilities by mandating conduct such as password usage and maintenance or requirements for connecting modems to ICSs. The policy and procedure vulnerabilities Are given bellow

- Inadequate security policy for the ICS
- No formal ICS security training and awareness program
- Inadequate security architecture and design
- No specific or documented security procedures were developed from the security policy for the ICS
- Absent or deficient ICS equipment implementation guidelines
- Lack of administrative mechanisms for security enforcement
- Few or no security audits on the ICS
- No ICS specific continuity of operations or disaster recovery plan (DRP) Lack of ICS specific configuration change management

2.2.3 Platform Vulnerabilities

Vulnerabilities in ICSs can occur due to flaws, misconfigurations, or poor maintenance of their platforms, including hardware, operating systems, and ICS applications. These vulnerabilities can be mitigated through various security controls, such as OS and application patching, physical access control, and security software (e.g., antivirus software). The tables in this section describe potential platform vulnerabilities
Mainly there are 4 types of platform vulnerabilities

- Platform Configuration Vulnerabilities
- Platform Hardware Vulnerabilities
- Platform Software Vulnerabilities
- Platform Malware Protection Vulnerabilities

2.2.3.1 Platform Configuration Vulnerabilities

- OS and vendor software patches may not be developed until significantly after security vulnerabilities are found
- OS and application security patches are not maintained
- OS and application security patches are implemented without exhaustive testing
- Default configurations are used
- Critical configurations are not stored or backed up
- Data unprotected on portable device
- Lack of adequate password policy
- No password used , disclosure , guessing
- Inadequate access controls applied

2.2.3.2 Platform Hardware Vulnerabilities

- Inadequate testing of security changes
- Inadequate physical protection for critical systems
- Unauthorized personnel have physical access to equipment
- Insecure remote access on ICS components
- Dual network interface cards (NIC) to connect networks
- Undocumented assets
- Radio frequency and electro-magnetic pulse (EMP)
- Lack of backup power
- Loss of environmental control
- Lack of redundancy for critical components

2.2.3.3 Platform Software Vulnerabilities

- Buffer overflow
- Installed security capabilities not enabled by default
- Denial of service (DoS)
- Mishandling of undefined, poorly defined, or “illegal” conditions
- OLE for Process Control (OPC) relies on Remote Procedure Call (RPC) and Distributed Component Object Model (DCOM)
- Use of insecure industry-wide ICS protocols
- Use of clear text
- Unneeded services running
- Use of proprietary software that has been discussed at conferences and in periodicals

- Inadequate authentication and access control for configuration and programming software
- Intrusion detection/prevention software not installed
- Logs not maintained
- Incidents are not detected

2.2.3.4 Platform Malware Protection Vulnerabilities

- Malware protection software not installed
- Malware protection software or definitions not current
- Malware protection software implemented without exhaustive testing

2.2.4 Network Vulnerabilities

Vulnerabilities in ICSs may occur from flaws, misconfigurations, or poor administration of ICS networks and their connections with other networks. These vulnerabilities can be eliminated or mitigated through various security controls, such as defense-in-depth network design, encrypting network communications, restricting network traffic flows, and providing physical access control for network components.

- Network Configuration Vulnerabilities
- Network Hardware Vulnerabilities
- Network Perimeter Vulnerabilities
- Network Monitoring and Logging Vulnerabilities
- Communication Vulnerabilities
- Wireless Connection Vulnerabilities

2.2.4.1 Network Configuration Vulnerabilities

Vulnerability	Description
Weak network security architecture	The network infrastructure environment within the ICS has often been developed and modified based on business and operational requirements, with little consideration for the potential security impacts of the changes. Over time, security gaps may have been inadvertently introduced within particular portions of the infrastructure. Without remediation, these gaps may represent backdoors into the ICS.
Data flow controls not employed	Data flow controls, such as access control lists (ACL), are needed to restrict which systems can directly access network devices. Generally, only network administrators should be able to access such devices directly. Data flow controls should ensure that other systems cannot directly access the devices.
Poorly configured IT security equipment	Using default configurations often leads to insecure and unnecessary open ports and exploitable network services running on hosts. Improperly configured firewall rules and router ACLs can allow unnecessary traffic.
Network device configurations not stored or backed up	Procedures should be available for restoring network device configuration settings in the event of accidental or adversary-initiated configuration changes to maintain system availability and prevent loss of data. Documented procedures should be developed for maintaining network device configuration settings.
Passwords are not encrypted in transit	Passwords transmitted in clear text across transmission media are susceptible to eavesdropping by adversaries, who could reuse them to gain unauthorized access to a network device. Such access could allow an adversary to disrupt ICS operations or to monitor ICS network activity.

Passwords exist indefinitely on network devices	Passwords should be changed regularly so that if one becomes known by an unauthorized party, the party has unauthorized access to the network device only for a short time. Such access could allow an adversary to disrupt ICS operations or monitor ICS network activity.
Inadequate access controls applied	Unauthorized access to network devices and administrative functions could allow a user to disrupt ICS operations or monitor ICS network activity.

2.2.4.2 Network Configuration Vulnerabilities

Vulnerability	Description
Weak network security architecture	The network infrastructure environment within the ICS has often been developed and modified based on business and operational requirements, with little consideration for the potential security impacts of the changes. Over time, security gaps may have been inadvertently introduced within particular portions of the infrastructure. Without remediation, these gaps may represent backdoors into the ICS.
Data flow controls not employed	Data flow controls, such as access control lists (ACL), are needed to restrict which systems can directly access network devices. Generally, only network administrators should be able to access such devices directly. Data flow controls should ensure that other systems cannot directly access the devices.
Poorly configured IT security equipment	Using default configurations often leads to insecure and unnecessary open ports and exploitable network services running on hosts. Improperly configured firewall rules and router ACLs can allow unnecessary traffic.
Network device configurations not stored or backed up	Procedures should be available for restoring network device configuration settings in the event of accidental or adversary-initiated configuration changes to maintain system availability and prevent loss of data. Documented procedures should be developed for maintaining network device configuration settings.
Passwords are not encrypted in transit	Passwords transmitted in clear text across transmission media are susceptible to eavesdropping by adversaries, who could reuse them to gain unauthorized access to a network device. Such access could allow an adversary to disrupt ICS operations or to monitor ICS network activity.
Passwords exist indefinitely on network devices	Passwords should be changed regularly so that if one becomes known by an unauthorized party, the party has unauthorized access to the network device only for a short time. Such access could allow an adversary to disrupt ICS operations or monitor ICS network activity.
Inadequate access controls applied	Unauthorized access to network devices and administrative functions could allow a user to disrupt ICS operations or monitor ICS network activity.

2.2.4.3 Network Hardware Vulnerabilities

Vulnerability	Description
Inadequate physical protection of network equipment	Access to network equipment should be controlled to prevent damage or destruction.
Unsecured physical ports	Unsecured universal serial bus (USB) and PS/2 ports could allow unauthorized connection of thumb drives, keystroke loggers, etc.
Loss of environmental control	Loss of environmental control could lead to processors overheating. Some processors will shut down to protect themselves, and some just melt if they overheat.

Non-critical personnel have access to equipment and network connections	Physical access to network equipment should be restricted to only the necessary personnel. Improper access to network equipment can lead to any of the following: • Physical theft of data and hardware • Physical damage or destruction of data and hardware • Unauthorized changes to the security environment (e.g., altering ACLs to permit attacks to enter a network) • Unauthorized interception and manipulation of network activity • Disconnection of physical data links.
Control network services not within the control network	Where IT services such as DNS, DHCP are used by control networks, they are often implemented in the IT network, causing the ICS network to become dependent on the IT network that may not have the reliability and availability requirements needed by the ICS
Lack of redundancy for critical networks	Lack of redundancy in critical networks could provide single point of failure possibilities

2.2.4.4 Network Perimeter Vulnerabilities

Vulnerability	Description
No security perimeter defined	If the control network does not have a perimeter clearly defined, then it is not possible to ensure that the necessary security controls are deployed and configured properly. This can lead to unauthorized access to systems and data, as well as other problems.
Firewalls nonexistent or improperly configured	A lack of properly configured firewalls could permit unnecessary data to pass between networks, such as control and corporate networks. This could cause several problems, including allowing attacks and malware to spread between networks, making sensitive data susceptible to monitoring/eavesdropping on the other network, and providing individuals with unauthorized access to systems.
Control networks used for non-control traffic	Control and non-control traffic have different requirements, such as determinism and reliability, so having both types of traffic on a single network makes it more difficult to configure the network so that it meets the requirements of the control traffic. For example, non-control traffic could inadvertently consume resources that control traffic needs, causing disruptions in ICS functions.

2.2.4.5 Network Monitoring and Logging Vulnerabilities

Vulnerability	Description
Inadequate firewall and router logs	Without proper and accurate logs, it might be impossible to determine what caused a security incident to occur.
No security monitoring on the ICS network	Without regular security monitoring, incidents might go unnoticed, leading to additional damage and/or disruption. Regular security monitoring is also needed to identify problems with security controls, such as misconfigurations and failures.

2.2.4.6 Communication Vulnerabilities

Vulnerability	Description
Critical monitoring and control paths are not identified	Rogue and/or unknown connections into the ICS can leave a backdoor for attacks.
Standard, well-documented communication protocols are used in plain text	Adversaries that can monitor the ICS network activity can use a protocol analyzer or other utilities to decode the data transferred by protocols such as telnet, FTP, and NFS. The use of such protocols also makes it easier for adversaries to perform attacks against the ICS and manipulate ICS network activity.
Authentication of users, data or devices is substandard or nonexistent	Many ICS protocols have no authentication at any level. Without authentication, there is the potential to replay, modify, or spoof data or to spoof devices such as sensors and user identities.
Lack of integrity checking for communications	There are no integrity checks built into most industrial protocols; adversaries could manipulate communications undetected. To ensure integrity, the ICS can use lowerlayer protocols (e.g., IPsec) that offer data integrity protection.

2.2.4.7 Wireless Connection Vulnerabilities

Vulnerability	Description
Inadequate authentication between clients and access points	Strong mutual authentication between wireless clients and access points is needed to ensure that clients do not connect to a rogue access point deployed by an adversary, and also to ensure that adversaries do not connect to any of the ICS's wireless networks.
Inadequate data protection between clients and access points	Sensitive data between wireless clients and access points should be protected using strong encryption to ensure that adversaries cannot gain unauthorized access to the unencrypted data.

2.2.5 Possible Incident Scenarios

- Control systems operation disrupted by delaying or blocking the flow of information through corporate or control networks, thereby denying availability of the networks to control system operators or causing information transfer bottlenecks or denial of service by IT-resident services (such as DNS)
- Unauthorized changes made to programmed instructions in PLCs, RTUs, DCSs, or SCADA controllers, change alarm thresholds, or issue unauthorized commands to control equipment, which could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of

processes (such as prematurely shutting down transmission lines), causing environmental incident, or even disabling of control equipment

- False information sent to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators
- Control system software or configuration settings modified, producing unpredictable results
- Safety systems operation interfered with
- Malicious software (e.g., virus, worm, Trojan horse) introduced into the system.

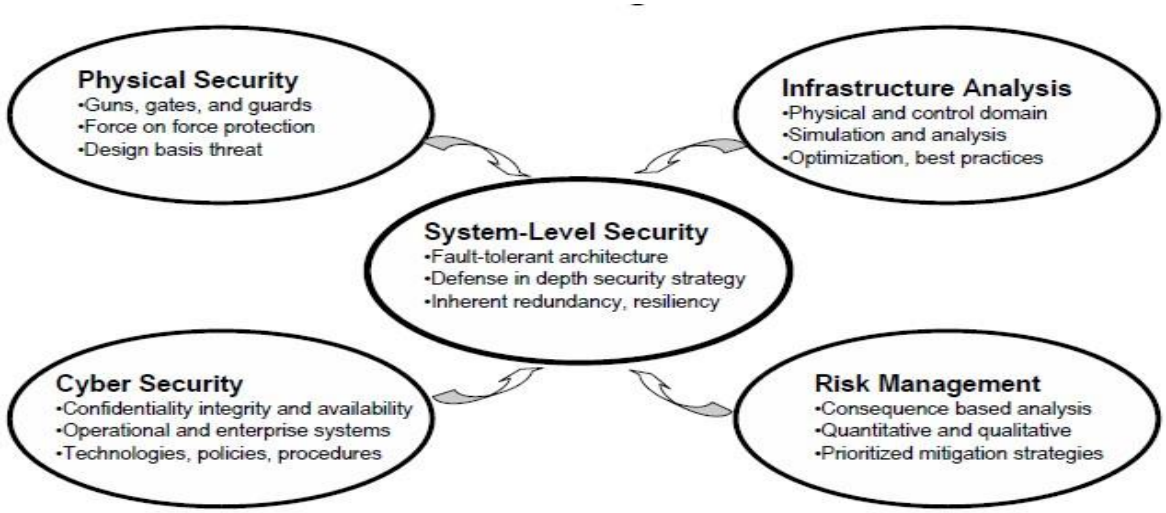
- Recipes (i.e., the materials and directions for creating a product) or work instructions modified in order to bring about damage to products, equipment, or personnel

In addition, in control systems that cover a wide geographic area, the remote sites are often unstaffed and may not be physically monitored. If such remote systems are physically breached, the adversaries could establish a connection back to the control network.

3. Security Controls

Security controls are the management, operational, and technical controls prescribed for an informational system to protect the confidentiality, integrity, and availability of the system and its information. A single security product or technology cannot adequately protect an ICS. Securing an ICS is based on a combination of effective security policies and a properly configured set of security controls. An effective cyber security strategy for an ICS should apply defense-in-depth, a technique of layering security mechanisms so that the impact of a failure in any one mechanism is minimized.

3.1 System-Level Security Should Be Built on a Strong Foundation



3.2 Management Controls

Management controls are the security countermeasures for an ICS that focus on the management of risk and the management of information security. NIST SP 800-53 defines four families of controls within the Management controls class:

Risk Assessment (RA): the process of identifying risks to operations, assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact

- System characterization – produces a picture of the information system environment, and delineation of system boundaries
- Threat identification – produces a threat statement containing a list of threat-sources that could exploit system vulnerabilities
- Vulnerability identification – produces a list of the system vulnerabilities that could be exercised by the potential threat sources
- Control analysis – produces a list of the planned controls used for the information system to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event.
- Likelihood determination – produces a likelihood rating (High, Medium, or Low) that indicates the probability that a potential vulnerability may be exercised
- Impact analysis – produces a magnitude of impact (High, Medium, or Low) resulting from the exploitation of a vulnerability.
- Risk determination – produces measurement for risk based on a scale of high, medium, or low
- Control recommendations – produces recommendations of security controls and alternative solutions to mitigate risk
- Results documentation – produces a risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.

Planning (PL): development and maintenance of a plan to address information system security by performing assessments, specifying and implementing security controls, assigning security levels, and responding to incidents

System and Services Acquisition (SA): allocation of resources for information system security to be maintained throughout the systems life cycle and the development of acquisition policies based on risk assessment results including requirements, design criteria, test procedures, and associated documentation

Certification, Accreditation, and Security Assessments (CA): assurance that the specified controls are implemented correctly, operating as intended, and producing the desired outcome.

3.3 Operational Controls

Operational controls are the security countermeasures for an ICS that are primarily implemented and executed by people as opposed to systems. NIST SP 800-53 defines nine families of controls within the Operational controls class:

Personnel Security (PS): policy and procedures for personnel position categorization, screening, transfer, penalty, and termination; also addresses third-party personnel security.

- Hiring policies

- Organization policies and practices
- Terms and conditions of employment.

Physical and Environmental Protection (PE): policy addressing physical, transmission, and display access control as well as environmental controls for conditioning (e.g., temperature, humidity) and emergency provisions (e.g., shutdown, power, lighting, fire protection).

- Protection of Physical Locations
- Access Control
- Access Monitoring System
- Access Limiting Systems
- Environmental Control Systems
- Control Center/Control Room
- Portable Devices
- Cabling

Contingency Planning (CP): policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

- Business Continuity Planning
- Disaster Recovery Planning

Configuration Management (CM): policy and procedures for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.

Maintenance (MA): policies and procedures to manage all maintenance aspects of an information system.

System and Information Integrity (SI): policy and procedures to protect information systems and their data from design flaws and data modification using functionality verification, data integrity checking, intrusion detection, malicious code detection, and security alert and advisory controls.

- Malicious Code Detection
- Intrusion Detection and Prevention
- Patch Management

Media Protection (MP): policy and procedures to ensure secure handling of media. Controls cover access, labeling, storage, transport, sanitization, destruction, and disposal.

Incident Response (IR): policy and procedures pertaining to incident response training, testing, handling, monitoring, reporting, and support services.

Awareness and Training (AT): policies and procedures to ensure that all information system users are given appropriate security training relative to their usage of the system and that accurate training records are maintained.

3.4 Technical Controls

Technical controls are the security countermeasures for an ICS that are primarily implemented and executed by the system through mechanisms contained in the hardware, software, or firmware components of the system. As discussed in detail in the following subsections, NIST SP 800-53 defines four families of controls within the Technical controls class:

Identification and Authentication (IA): the process of verifying the identity of a user, process, or device, as a prerequisite for granting access to resources in an IT system.

- Password Authentication
- Challenge/response Authentication
- Physical Token Authentication
- Biometric Authentication

Access Control (AC): the process of granting or denying specific requests for obtaining and using information and related information processing services for physical access to areas within the information system environment.

- Role-based Access Control (RBAC)
- Web Servers
- Virtual Local Area Network (VLAN)
- Dial-up Modems
- Wireless

Audit and Accountability (AU): independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

System and Communications Protection (SC): mechanisms for protecting both system and data transmission components.

- Encryption
- Virtual Private Network (VPN)

REFERENCE:-

1. https://nptel.ac.in/courses/108106022/LECTURE%2012.pdf
2. https://onupkeep.com/blog/advantages-scada-system/
3. https://www.elprocus.com/scada-systems-work/
4. SCADA Presentation.pptx
5. 2005_09_15_Jeff_Dagle.pdf By Jeff Dagle, PEPacific Northwest National Laboratory Grainger Lecture Series for the University of Illinois at Urbana-Champaign
6. Intelligent_SCADA_System.pdf By Rajeev Kumar Chauhan, Mohan Lal Dewal
7. https://www.doc-txt.net/Guide-to-Supervisory-Control-and-Data-Acquisition.pdf
8. https://www.doc-txt.net/Guide-to-Supervisory-Control-and-Data-Acquisition.pdf
9. https://www.controlglobal.com/assets/Media/MediaManager/wp_071204_Semaphore_SCADA.pdf
10. https://www.slideshare.net/sebaii/scada-classification