PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

Ministry of Higher Education and Scientific Research

University of Amar Telidji - Laghouat

Faculty of Technology

Department of Electronics

Lecture Notes

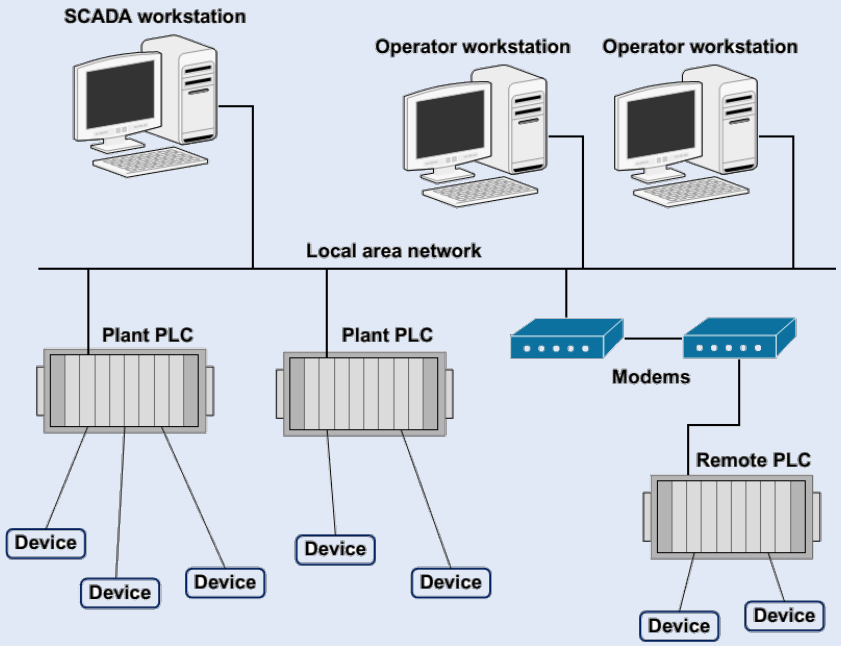
DOMAIN: Science & Technology

FIELD: Automatics

SPECIALTY: Master 2 Automation & Industrial Computing

Dr. Aboubakeur HADJAISSA

INDUSTRIAL SUPERVISION SCADA



2023 / 2024

Abstract

This manual is intended to give students a solid grasp of SCADA systems' foundational ideas and real-world problems. At their most basic level, SCADA systems are industrial control systems. They are computer-based control systems that keep track of and manage industrial operations carried out in the real world. Manufacturing facilities, oil production and processing, pharmaceuticals, energy, water treatment and distribution, and a host of other industries use SCADA systems. They are the ideal control approach for operations that require vital control in quick-paced processes, have vast amounts of data that must be gathered and analyzed, or are dispersed across large distances.

This cours enable students to gain hands-on experience with real-time monitoring and control of industrial processes. This includes understanding and working with hardware like PLCs (Programmable Logic Controllers) and software used in SCADA systems, also, the students can engage in research and development projects related to SCADA systems, contributing to innovations in industrial automation and control technologies.

According to the program of study established by CPND, this course is designed for second-year master's students in automation and industrial computing.

Contents

List of Figures

List of Tables

Abbreviations

Here is the sorted list of abbreviations in alphabetical order:

- **CP**: **C**ontrol **P**art.
- **CPU**: **C**entral **P**rocessing **U**nit.
- **EMF**: **E**lectromotive **F**orce.
- **FBD**: **F**unction **B**lock **D**iagram.
- **FC**: **F**unction **C**all.
- **HMI**: **H**uman **M**achine **I**nterface.
- **IEC**: The **I**nternational **E**lectrotechnical **C**ommission.
- **IL**: **I**nstruction **L**ist.
- **I/O**: **I**nput and **O**utput.
- **LAN**: **L**ocal **A**rea **N**etwork.
- **MPI**: **M**ulti **P**oint **I**nterface.
- **OB**: **O**rganization **B**lock.
- **OP**: **O**perative **P**art.
- **PC**: **P**rogrammable **C**omputer.

- **PID control**: **P**roportional, **I**ntegral, **D**erivative control.
- **PLC**: **P**rogrammable **L**ogic **C**ontroller.
- **PN/IE**: **P**rofinet/**I**ndustrial **E**thernet.
- **PWM**: **P**ulse **W**idth **M**odulation.
- **SFC**: **S**equential **F**unction **C**hart.
- **SP**: **S**upervision **P**art.
- **ST**: **S**tructured **T**ext.
- **TCP/IP**: **T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol.
- **TIA portal**: **T**otally **I**ntegrated **A**utomation **P**ortal.

General Introduction

"Supervisory Control and Data Acquisition" stands for SCADA. Industrial equipment such as motors, valves, pumps, relays, sensors, and other items are centrally monitored and controlled by real-time industrial process control systems. Previously, industrial processes were totally managed by PLC, CNC, PID, and micro controllers that had been coded in specific languages or codes. These routines lacked any real animation that would have explained how the operation was being carried out and were either written in relay logic or assembly language. If the status of the process is displayed using some animations rather than plain codes, it is always simple to understand. Thus, SCADA software was created and, thanks to some unique qualities, it was integrated into the automation system.

SCADA consists of both hardware and software. It's a notion. It is a system made up of unique software, hardware, and protocols. SCADA is used to manage operations in chemical plants, oil and gas pipelines, manufacturing facilities, infrastructure for water purification and distribution, and other systems. As an illustration, a PLC can be utilized in a SCADA system to regulate the flow of cooling water as part of an industrial operation. The supervisor can also utilize the Host control feature to adjust the temperature of the water flow at the same time. The distributed database used by SCADA systems is frequently referred to as a tag database and comprises data components called tags or points. A point is an individual input or output value that the system is monitoring or controlling. You can have "hard" or "soft" points. A soft point is the outcome of applying logic and math to other hard and soft points, whereas a hard point is a representation of a genuine input or output connected to the system.

The majority of implementations conceptually eliminate this distinction by making each property a "soft" point (expression) that, in the simplest scenario, can equal a single "hard" point. In most cases, point values are saved as value-timestamp combinations, which include both the value and the time at which the value was calculated or recorded. The history of that point is a set of value-timestamp pairs. Additional metadata, such as the path to a field device and a PLC register, design time comments, and even warning information, are frequently stored with tags.

This manual is divided into five chapters:

- In chapter One, an overview of SCADA systems is presented, including discussions on SCADA , history and applications
- The second chapter discussed the existing architectures of SCADA system
- One of the important elements of SCADA systems is the HMI element , this important element will be discussed in details in the third chapter
- The fourth chapter of this manuscript talk on the security of SCADA system
- In the last part of this course, we present six specifications of laboratory works.

This thesis equips readers with the knowledge and skills to design and implement industrial automation and control systems. By examining hardware, software, and practical application on a test bench, it advances automation technology in various industries.

Chapter 1

SCADA system overview

Contents

1.1 Introduction

SCADA is the technology that enables a user to gather information from one or more remote facilities and to transmit them a limited set of control instructions. When remote facilities are running smoothly, SCADA eliminates the need for an operator to be stationed there or to travel there frequently. SCADA includes—but is not limited to—the operator interface and the manipulation of data connected to applications. Although some manufacturers are creating software packages they refer to as SCADA, they are not full SCADA systems since they lack communications links and other necessary hardware, even if they are frequently well suited to function as elements of a SCADA system.

This chapter presents the fundamental components of the SCADA system, covers some of the processes that can profit from its implementation, and lists some of the advantages that the system can offer.

1.2 Definition of SCADA

SCADA is an acronym made up of the first letters of the phrase "supervisory control and data acquisition." The acronym SCADA is a suitable one, aside from the fact that the root term does not allude to the element of distance, which is typical of most SCADA systems. A SCADA system enables an operator to change set points on distant process controllers, open or close valves or switches, monitor alarms, and gather measurement data from a location central to a widely distributed process, such as an oil or gas field, pipeline system, irrigation system, or hydroelectric generating complex. One may understand the benefits SCADA offers in terms of minimizing the cost of routine visits to monitor facility functioning when the process's dimensions become very large—hundreds or even thousands of kilometers from one end to the other. If the facilities are extremely far away and require a lot of work (like a helicopter flight), the value of these perks will increase even further [1].

1.2.1 Industrial Automation Pyramid

In the industrial automation pyramid, the SCADA system resides above the plant floor PLCs layer and below the ERP layer, Figure 1.1 [2]:

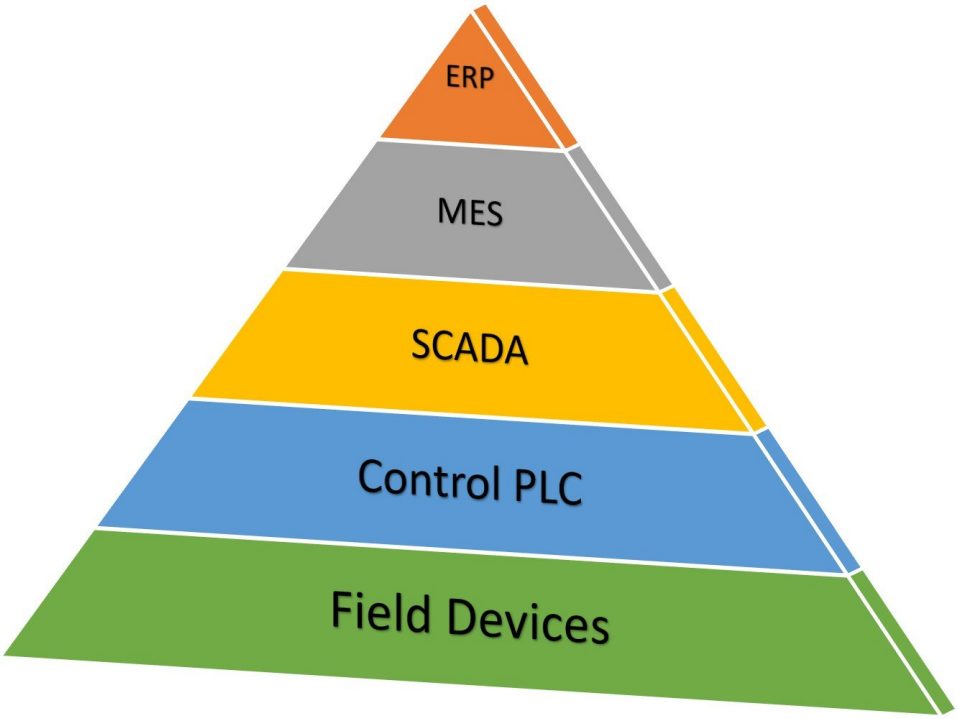


Figure 1.1: Industrial Automation Pyramid

1.2.1.1 FIELD DEVICES

Automation begins at the field device level.

Few examples of field devices: Photoelectric digital sensors that detect a change in light intensity to sense objects within a field of view. Level analog sensors such as those with radar can detect the chemical level in a tank by emitting a frequency and measuring the return wave. Field devices also include industrial AC or DC motors that can vary in speed to accommodate different machine or process requirements. These motors can have Variable Speed Drives – VFDs that can modulate and control the speed of the motor. How do all of these field devices work cohesively in order to automate a machine? What processes this information, and how does it know what functions to perform?

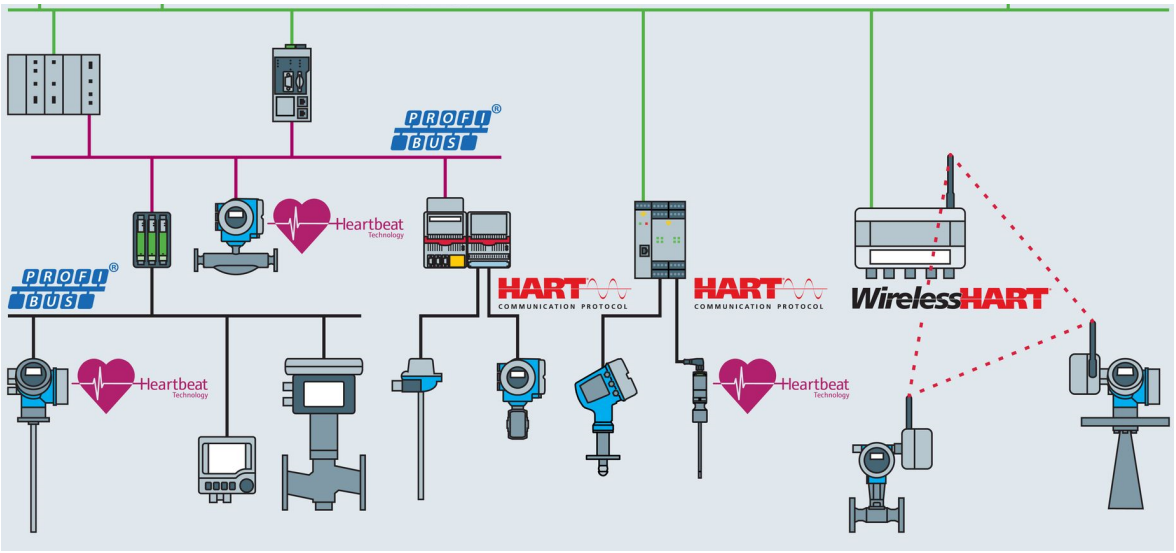


Figure 1.2: Field Devices

1.2.1.2 CONTROL LEVEL

An industrial computer, also known as a programmable logic controller or "PLC," comprises different modules, including a processor, digital input, analog input, high-speed counters, and various industrial communication protocol adapters.

Figure 1.3: Control level based PLC

The PLC is on the next tier, known as the control level of the pyramid. With this controller, we can execute functions based on inputs in the form of electrical signals

translated in binary form of a 1 for on or 0 for off. Outputs such as a motor, pneumatic actuator, or any mechanical actuator.

Human intervention is reduced nowadays when the PLC controls the equipment and can complete the tasks more precisely.

Programs written by control system engineers are stored in the PLC's memory in a language it understands. These languages include ladder logic, sequential function charts, or structured text.

A Human Machine Interface (HMI) runs a computerized application at the "machine level" so that the operator can directly interface with the equipment without needing to edit any of the PLC code.

PLCs have become the workhorse of the industrial automation field and have become more powerful in manipulating data.

- ***Communications*** The automated industrial facility relies heavily on communication protocols to facilitate the interaction of various types of remote input or output devices.

  At the field device level, we have protocols such as IO-Link or Modbus RTU that give sensors and the PLC a means of communicating. The PLC acts as the master, assigns the sensor its parameters, and accesses its process values such as temperature, pressure, conductivity, and level.

  Modules transfer the data to the PLC using protocols such as EthernetIP or Profinet. EthernetIP has almost eliminated the need for field device wiring, reducing installation costs.

  Through EthernetIP, we can communicate with modules or "gateways" where multiple sensors can be connected. This data is then transmitted through an Ethernet cable to the PLC for use in the program or code to perform the desired operation.

  Next, we will examine the two types of industrial automation.

- ***Machine Control*** Industrial manufacturing facilities use equipment to perform a task repetitively, for instance, a machine that folds a carton to hold a finished

product. Therefore, the flaps must be in the same place every cycle to mitigate any downstream or quality issues.

This machine uses a photoelectric sensor to detect when the carton has entered the area to be folded.

The PLC then runs the program to glue, seal, and close the carton.

This is an example of fixed processes that were once done without automation.

- ***Process Control*** Batching processes were once done by humans and were prone to inaccuracies. A simple diagram below shows the essential components needed to automate a mixing or batching process.

  With industrial automation, we can eliminate or reduce human intervention by controlling the addition of ingredients.

1.2.1.3 SUPERVISORY CONTROL AND DATA ACQUISITION - SCADA LEVEL

The last tier of the industrial automation hierarchy we will discuss is the supervisory level. This is one of the most powerful as it can bind both the operations and information systems. "SCADA," which stands for Supervisory Control and Data Acquisition, encompasses the entire facility or processes and not only at the control or field device level.

SCADA software is commonly installed on a server computer and is accessed by computers or clients within the same network.

A user can access pre-configured and customizable screens that allow control of components on the ground floor, such as valves, motors, actuators, etc.

SCADA systems can automate the data acquisition process by recording values from instrumentation or electronic sensors in the field. This function can be executed by linking the software to a PLC where the values are read and written.

Once a change in values is detected, information is passed into a database on the server and stored for retrieval at any time.

Historically data was recorded manually by an operator, on software, or by paper. SCADA systems can run reports to track downtime and equipment efficiencies to

Figure 1.4: SCADA

increase productivity.

The automated process of storing and retrieving data allows for greater visibility of equipment efficiency. In addition, machine learning capabilities are on the rise and further push the automated plant to become more and more productive.

1.2.1.4 Manufacturing Execution Systems (MES) Level

The MES level in the Industrial Automation Pyramid is responsible for managing and monitoring production processes on the factory floor.

It operates in real-time to control and optimize manufacturing operations, providing feedback to both the enterprise level (ERP) and the control level (SCADA and PLCs). MES covers a range of functions, including:

- Production Scheduling: Ensuring that production plans are executed efficiently.
- Resource Management: Managing materials, equipment, and labor resources.
- Quality Management: Monitoring and controlling product quality during the manufacturing process.

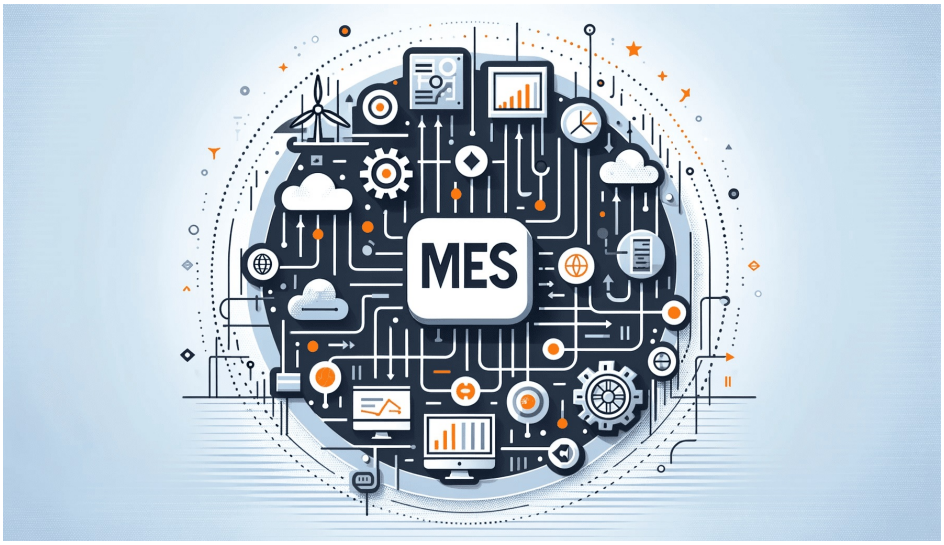


Figure 1.5: Manufacturing Execution Systems (MES)

- Performance Analysis: Tracking and analyzing production performance to identify bottlenecks and areas for improvement.
- Data Collection and Management: Gathering real-time data from the shop floor and making it available for analysis and reporting.

The MES level helps in enhancing productivity, reducing production costs, improving product quality, and ensuring compliance with regulatory requirements.

1.2.1.5 Enterprise Resource Planning (ERP) Level

The ERP level is the highest tier in the Industrial Automation Pyramid, focusing on the comprehensive management of business processes across an organization. ERP systems integrate various functions and departments, ensuring that information flows seamlessly throughout the enterprise.

The key roles and features of the ERP level include:

- Resource Planning: Managing and allocating resources such as raw materials, workforce, and financial assets efficiently.
- Business Process Integration: Coordinating processes across departments like finance, human resources, procurement, sales, and manufacturing.

Figure 1.6: Enterprise Resource Planning (ERP) Level

- Data Management: Centralizing data storage and ensuring data consistency across the organization.
- Strategic Planning and Decision-Making: Providing tools for forecasting, budgeting, and strategic decision-making based on real-time data.
- Customer Relationship Management (CRM): Enhancing customer interactions and relationship management. Supply Chain Management (SCM): Managing supply chain activities to optimize the flow of goods and services.

The ERP system acts as the backbone of an organization's information system, connecting all aspects of the business and providing a unified view of operations. This level is critical for ensuring that strategic objectives are met and that the organization operates efficiently and effectively.

1.3 Applications of SCADA

Supervisory Control and Data Acquisition (SCADA) systems find applications in a wide range of industries, providing real-time monitoring, control, and automation capabilities [3].

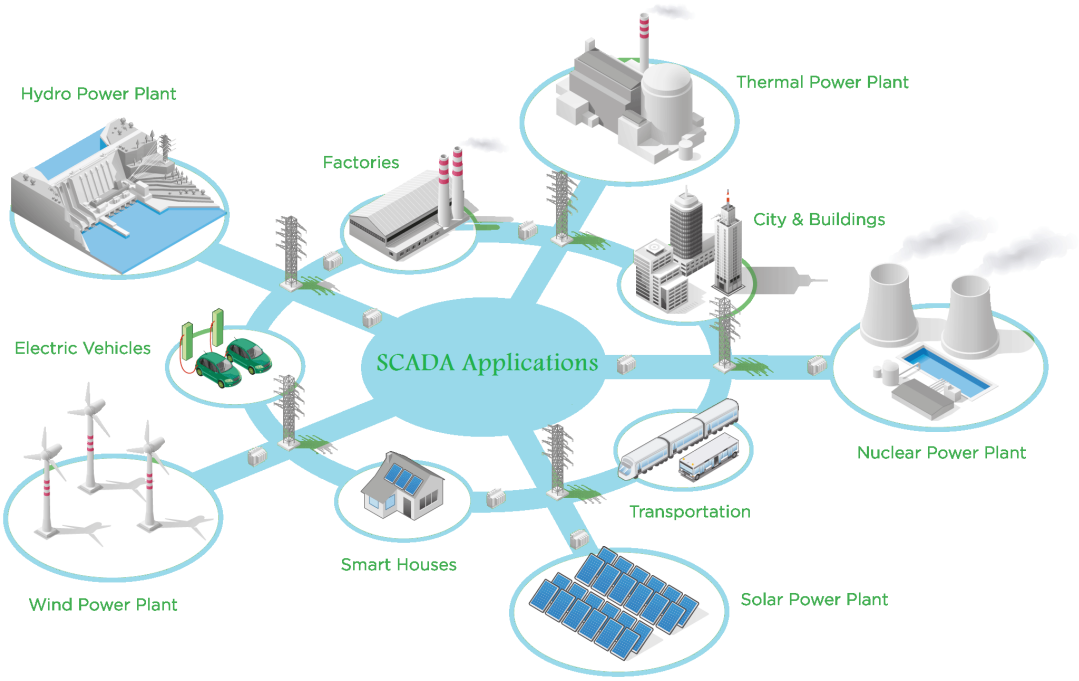


Figure 1.7: SCADA Application Areas

Here are some key applications of SCADA across various sectors:

1. **Energy Management:**
   - **Power Generation:** SCADA systems monitor and control power plants, optimizing the generation process, and ensuring efficient energy production.
   - **Transmission and Distribution:** SCADA helps manage the transmission and distribution of electricity, ensuring a reliable supply and quick response to faults.
2. **Manufacturing and Industrial Processes:**

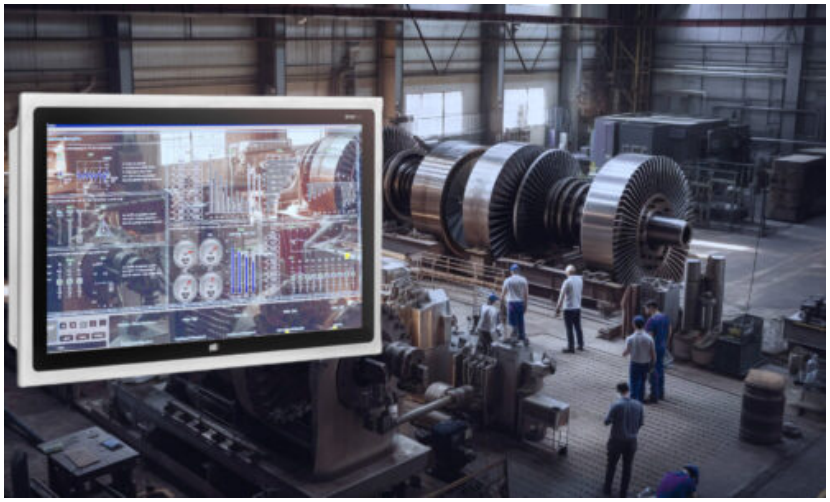


Figure 1.8: SCADA Manufacturing

- **Process Automation:** SCADA is used to automate and control manufacturing processes, enhancing efficiency, reducing errors, and improving product quality.
- **Quality Control:** SCADA systems monitor parameters such as temperature, pressure, and flow, ensuring products meet quality standards.

3. **Water and Wastewater Treatment:**

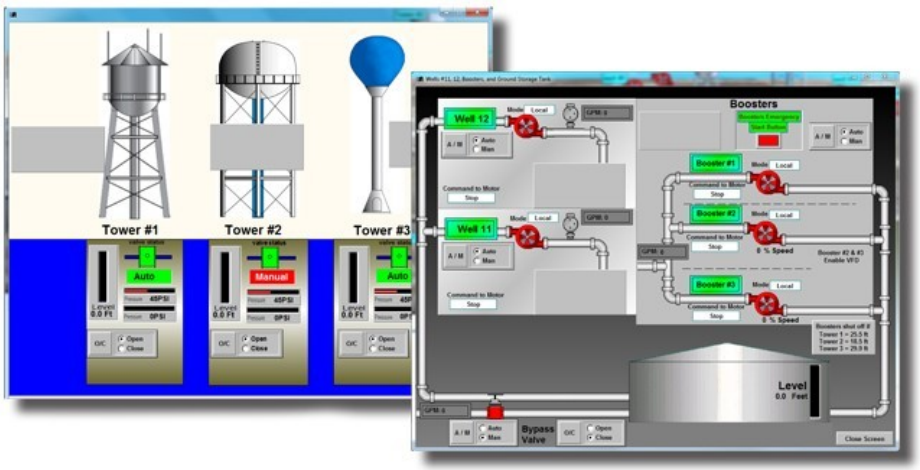


Figure 1.9: Water and Wastewater Treatment using SCADA

- **Water Distribution:** SCADA manages the distribution of water in municipal systems, optimizing pumping and ensuring consistent water supply.

- **Wastewater Treatment:** SCADA monitors and controls wastewater treatment processes, optimizing the use of resources and minimizing environmental impact.

4. **Oil and Gas Industry:**

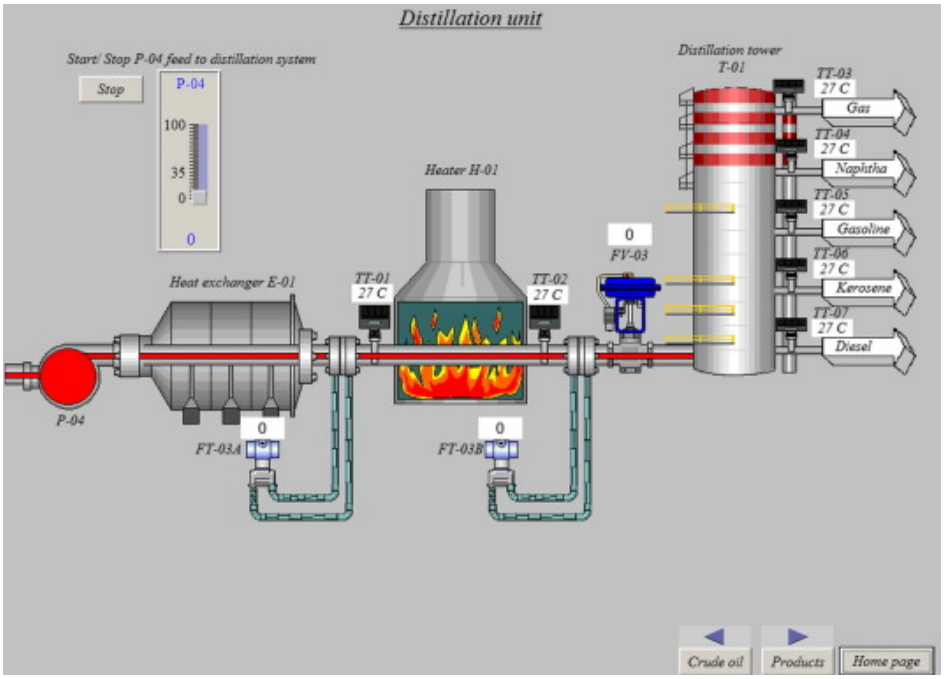


Figure 1.10: SCADA in Oil & Gas field

- **Extraction and Refining:** SCADA systems oversee oil and gas extraction processes, as well as refining operations, ensuring safety and efficiency.
- **Pipeline Monitoring:** SCADA is employed for monitoring pipelines, detecting leaks, and controlling the flow of oil and gas.

5. **Transportation Systems:**

- **Traffic Control:** SCADA is used in intelligent transportation systems for traffic monitoring, signal control, and incident management.
- **Railway Systems:** SCADA ensures the safe and efficient operation of railway systems, including track switching and train control.

6. **Building Automation:**

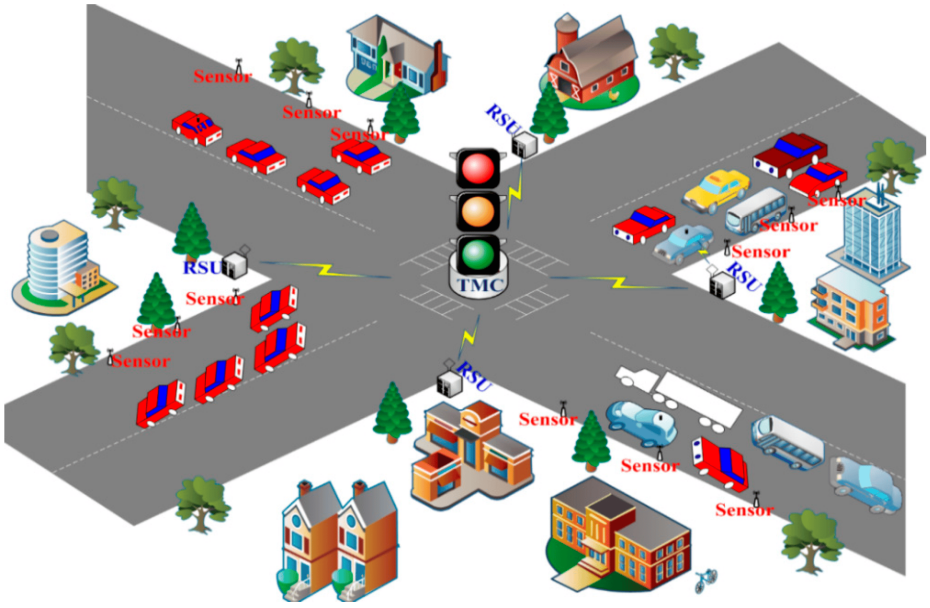


Figure 1.11: Transportation Systems

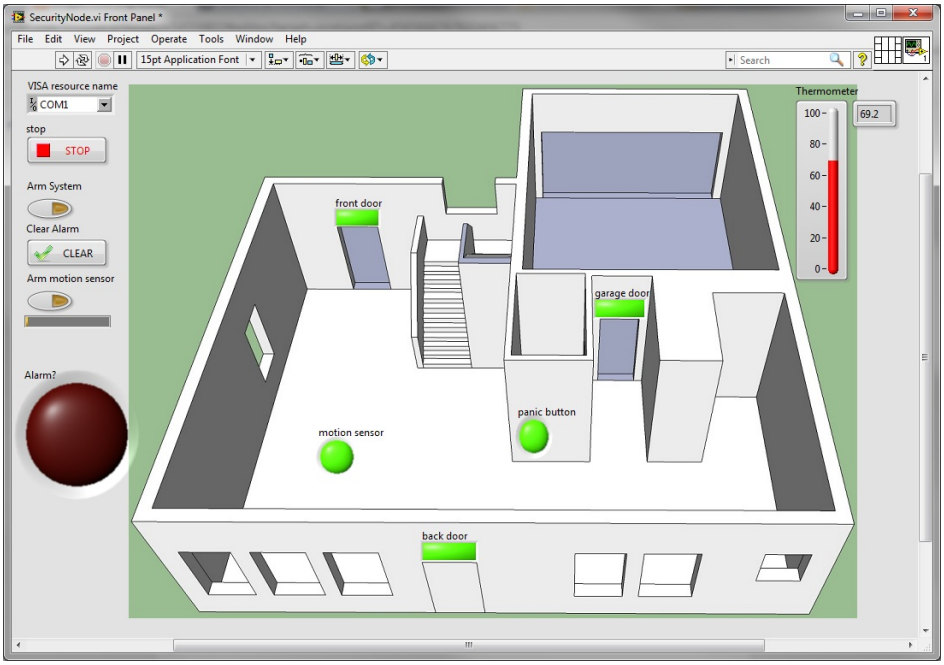


Figure 1.12: building automation using SCADA system

- **HVAC Systems:** SCADA systems control heating, ventilation, and air conditioning (HVAC) systems in commercial and industrial buildings for energy efficiency.
- **Security Systems:** SCADA integrates with security systems, providing surveillance and access control.

7. **Telecommunications:**

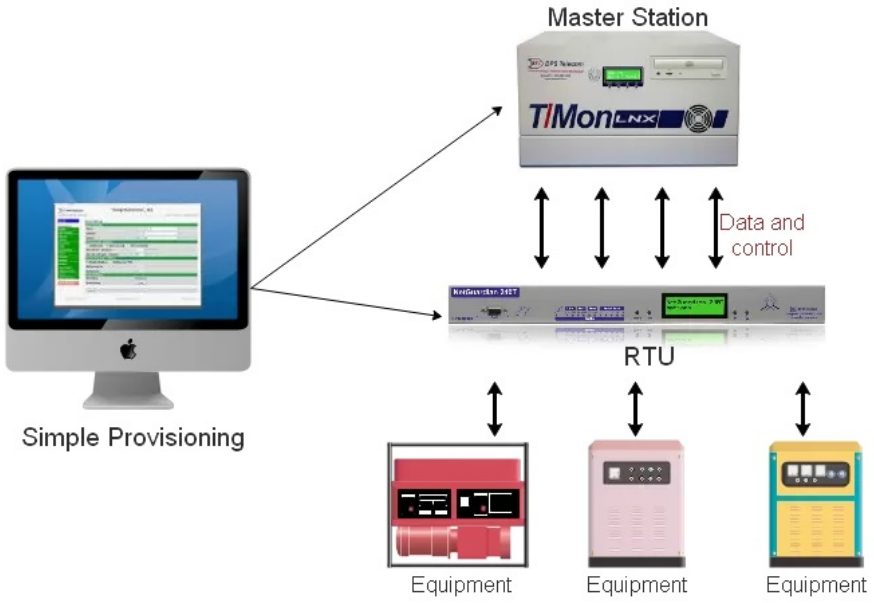


Figure 1.13: Telecommunications using SCADA system

- **Network Monitoring:** SCADA monitors telecommunications networks, ensuring reliability and identifying issues for quick resolution.
- **Tower and Antenna Control:** SCADA is used for the remote control and monitoring of communication towers and antennas.

8. **Environmental Monitoring:**

- **Air and Water Quality Monitoring:** SCADA systems are employed to monitor environmental parameters, ensuring compliance with regulatory standards.
- **Weather Stations:** SCADA integrates with weather monitoring stations for real-time data collection and analysis.

9. **Healthcare Facilities:**

- **Facility Management:** SCADA helps manage critical systems in healthcare facilities, such as power distribution, HVAC, and emergency response.

10. **Agriculture:**

    Precision Farming: SCADA is used in agriculture for monitoring and controlling irrigation systems, climate conditions, and the overall farm operation.

These applications highlight the versatility of SCADA systems, showcasing their ability to enhance efficiency, reduce downtime, and ensure the optimal functioning of critical processes across diverse industries.

1.4 History of SCADA

Supervisory Control and Data Acquisition (SCADA) systems have a rich history, evolving from humble beginnings to becoming a critical component in the management and control of industrial processes. Here's a chronological overview of key milestones in the development of SCADA systems:

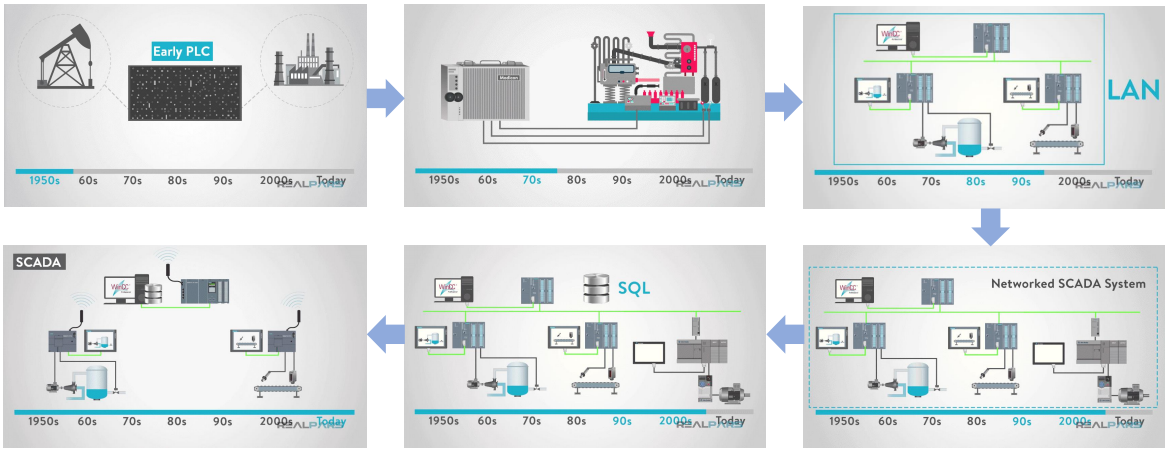


Figure 1.14: SCADA History

1. Early 20th Century: Telegraph and Telemetry

   The roots of SCADA can be traced back to the early 20th century when telegraph systems were used to transmit simple messages over long distances. This basic form of telemetry laid the groundwork for the remote monitoring of equipment and processes.

2. World War II: Development of Remote Control

   During World War II, the military extensively used remote control technology to operate unmanned vehicles and weaponry. This wartime innovation spurred interest in remote monitoring and control applications for civilian purposes.

3. 1960s: Introduction of SCADA Concepts

   The term "SCADA" began to emerge in the 1960s. The focus was on developing systems that could monitor and control industrial processes remotely. Early SCADA systems utilized analog and digital technology for data acquisition.

4. 1970s: Digital Revolution and PLCs

   Advancements in digital technology during the 1970s facilitated the transition from analog to digital SCADA systems. Programmable Logic Controllers (PLCs) became integral to SCADA, offering improved control and automation capabilities.

5. 1980s: Integration of Computers and SCADA

   The widespread adoption of personal computers in the 1980s revolutionized SCADA systems. The integration of computers allowed for more sophisticated data processing, visualization, and control. Human-Machine Interfaces (HMIs) became standard components of SCADA systems.

6. 1990s: Standardization and Interoperability

   The 1990s saw efforts to standardize SCADA protocols to enhance interoperability between different systems and devices. Protocols such as Modbus, DNP3, and OPC (OLE for Process Control) gained prominence, fostering compatibility in the industry.

7. Late 1990s to Early 2000s: Internet Connectivity and Cybersecurity Challenges

   As the internet became more prevalent, SCADA systems started leveraging online connectivity for remote monitoring and control. However, this connectivity

introduced new challenges, particularly in terms of cybersecurity. The susceptibility of SCADA systems to cyber threats became a significant concern during this period.

8. 2010s: IoT Integration and Cloud Computing

   The 2010s marked a shift towards integrating SCADA systems with the Internet of Things (IoT). This allowed for enhanced data collection, analysis, and connectivity. Cloud computing also gained traction, enabling the storage and processing of vast amounts of SCADA data.

9. Present and Future: Smart SCADA Systems

   In the present day, SCADA systems continue to evolve into "smart" systems. The integration of artificial intelligence, machine learning, and advanced analytics promises to further enhance the capabilities of SCADA, enabling predictive maintenance, optimization, and improved decision-making.

Throughout its history, SCADA has undergone a remarkable transformation, evolving from rudimentary telemetry systems to sophisticated, interconnected platforms that play a crucial role in managing the complex processes of various industries.

1.5 SCADA components

In industrial automation, when you use various devices, it is necessary to understand the architecture designed in them. The SCADA devices communicate with each other in various ways – either through hardware or through communication to share the data between the field and control room. Which link goes in which connection, is necessary to define and work out, Once we understand the architecture, then we can work in the system easily.

Here's an overview of the common elements in SCADA architecture:

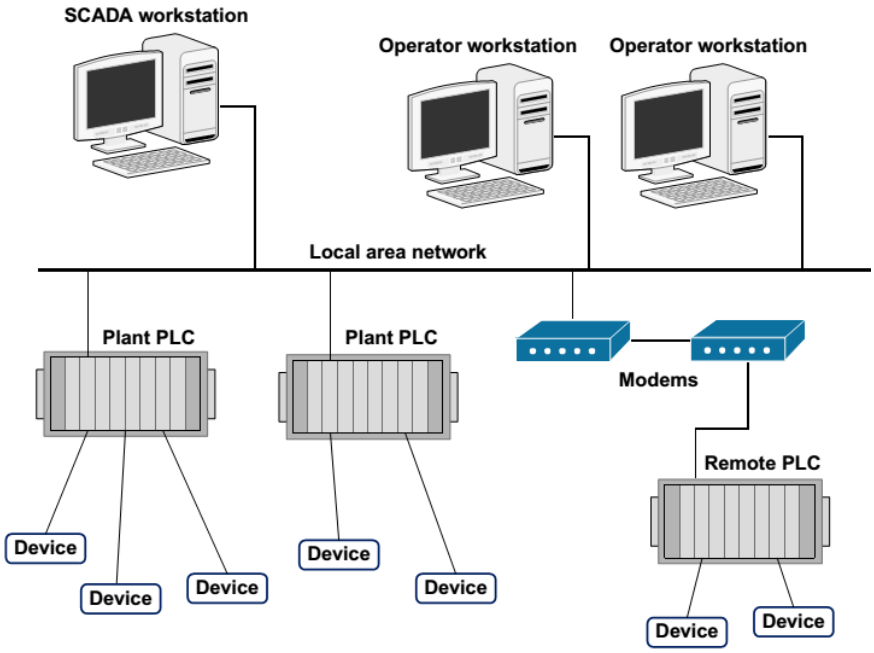


Figure 1.15: Typical SCADA system architecture

1.5.1 Supervisory Computers (SCs):

These are the central components responsible for processing and displaying information to the human operator. SCs are often equipped with Human Machine Interface (HMI) software that provides a graphical representation of the industrial processes being monitored. Operators use these interfaces to interact with the system, view real-time data, and issue commands.

Figure 1.16: Human Machine Interface (HMI)

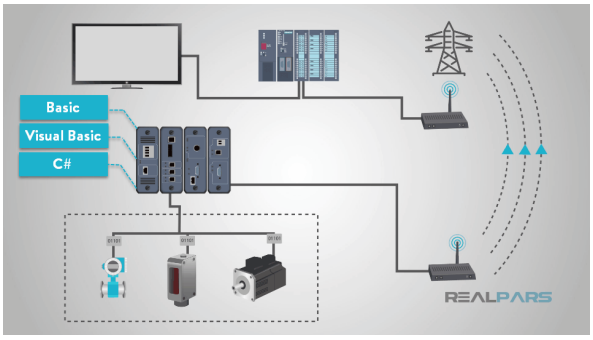


Figure 1.17: Remote Terminal Units (RTUs)

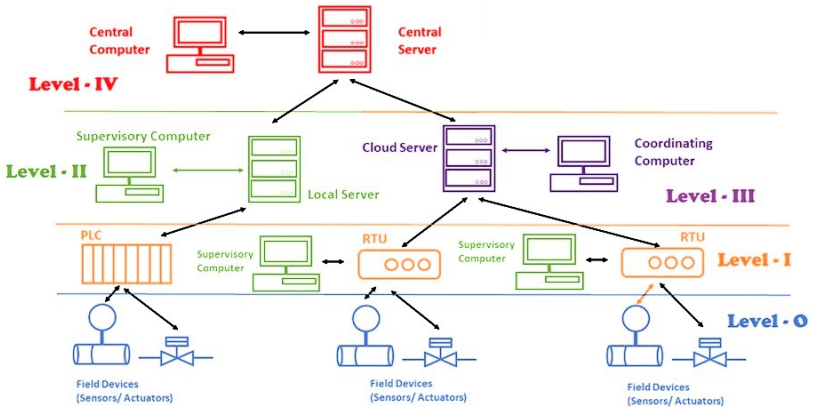


Figure 1.18: SCADA Architecture

1.5.2 Remote Terminal Units (RTUs) :

RTU, which stands for Remote Terminal Unit, is occasionally referred to as Remote Telemetry Unit or Remote Telecontrol Unit. RTUs are field devices that interface with sensors and actuators to collect data from the physical processes. They are responsible for monitoring the status of equipment and processes, as well as executing control commands issued by the SCADA system. RTUs are critical for the integration of field devices into the SCADA network. An RTU is a microprocessor-based device responsible for monitoring and controlling field devices. It subsequently connects to plant control or SCADA (supervisory control and data acquisition) systems.

1.5.3 Communication Infrastructure:

SCADA systems rely on a communication network to facilitate data exchange between SCs and field devices.

The communication infrastructure can include various technologies such as Ethernet, radio, satellite, or other wired and wireless protocols. The selection of the communication technology depends on the specific requirements and constraints of the industrial environment.

1.5.4 Data Acquisition System:

This subsystem is responsible for collecting data from sensors and instruments distributed across the monitored processes. The collected data is then transmitted to the SC for processing and analysis. The data acquisition system ensures that real-time and accurate information is available for monitoring and control.

1.5.5 SCADA Master Station:

The SCADA master station, often located in a centralized control room, is where the SCADA software runs. It is responsible for processing data received from RTUs or PLCs, providing a user interface for operators, and executing control actions based on the received information.

1.5.6 Historian:

The historian component of SCADA systems is responsible for storing and archiving historical data. This data can be valuable for trend analysis, performance monitoring, and compliance reporting. It helps operators and management make informed decisions based on past performance and trends.

1.5.7 Security Infrastructure:

Given the critical nature of SCADA systems and the potential impact of unauthorized access or cyber-attacks, security is a crucial consideration. Security measures include firewalls, encryption, authentication mechanisms, and other measures to protect the integrity and confidentiality of the SCADA network.

SCADA architectures can vary based on the specific requirements of the industrial processes they monitor and control. Additionally, advancements in technology, such

as the integration of cloud computing and edge computing, continue to influence the evolution of SCADA architectures.

1.6 Conclusion

In conclusion, a SCADA (Supervisory Control and Data Acquisition) system serves as a vital tool for monitoring and controlling industrial processes and infrastructure. It integrates data acquisition, networked communication, and user interface capabilities to provide real-time control and monitoring. With its ability to enhance operational efficiency, improve decision-making, and ensure system reliability, SCADA systems play a crucial role in various industries, from energy and water management to manufacturing and transportation. As technology continues to advance, the role and capabilities of SCADA systems are expected to evolve, offering even more sophisticated solutions for complex and interconnected systems.

Chapter 2

Architecture of SCADA system

Contents

2.1 Introduction

In this chapter, we will delve into the various architectures that underpin SCADA (Supervisory Control and Data Acquisition) systems. Understanding these architectures is crucial as they dictate the system's functionality, scalability, and reliability. We will explore the evolution from monolithic to distributed and networked architectures, highlighting their unique characteristics, advantages, and applications. By the end of this chapter, readers will gain a comprehensive understanding of the diverse SCADA architectures and their significance in modern industrial automation.

2.2 SCADA Architectures

SCADA systems have advanced alongside the development and complexity of contemporary computing technology. The subsequent sections will outline the three generations of SCADA systems as follows:

1. First Generation – Monolithic
2. Second Generation – Distributed
3. Third Generation – Networked
4. Fourth Generation – Industry 4.0

2.2.1 Monolithic SCADA Systems

This describes systems operating in isolation without connectivity to other systems, designed to function independently. Early SCADA systems used large minicomputers for computing tasks, with the PDP-11 series from Digital Equipment Corporation serving as a prime example of a first-generation SCADA system. In this architecture, RTUs communicated with the MTU via Wide Area Networks (WAN), as illustrated in Fig. 2.1.

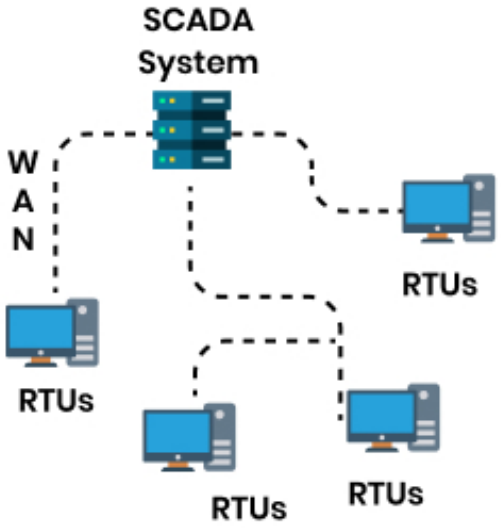


Figure 2.1: Monolithic SCADA Systems

However, the WAN protocols utilized at that time were in their nascent stages. Communication protocols were proprietary, compatible only with the vendor-specific MTU. These protocols were restricted to scanning, control, and data exchange between the MTU and RTUs, with interconnections occurring at the bus level [9]. Integrating RTUs from different vendors with the MTU posed significant challenges, underscoring the need for open standards. In some instances, to enhance SCADA system redundancy, an equally equipped backup system was linked to the primary system.

2.2.2 Distributed SCADA Systems

These systems were interconnected within a limited network range, such as Local Area Networks (LAN), as depicted in 2.2. This generation distributes computing tasks across remotely located systems via LAN, with some systems functioning as communication processors, others as operator interfaces, and some as database servers, among other roles [9]. This approach results in enhanced processing power, redundancy, and system reliability. Distributed architectures are employed in scenarios involving multiple clients and stations.

Like their monolithic counterparts, distributed SCADA systems were also restricted to vendor-specific hardware, software, network protocols, and peripheral devices [10, 11]. Security considerations for SCADA systems were minimal, with information being

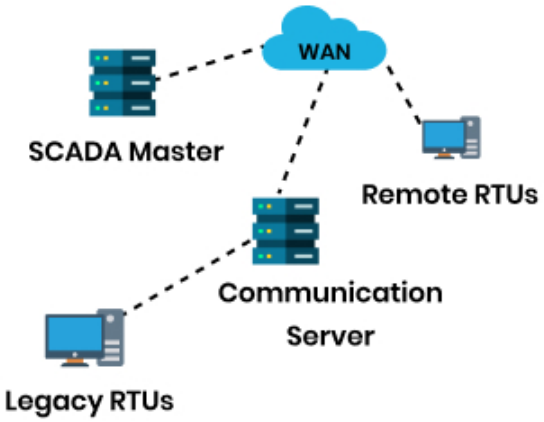


Figure 2.2: Distributed SCADA Systems

shared over LANs. However, the use of proprietary LAN protocols limited the systems that could be connected to function as a distributed MTU. WAN was utilized for communication between RTUs and the MTU.

2.2.3 Networked SCADA Systems:

These systems leverage networks and the web extensively, benefiting from standardization and cost-effective solutions tailored for large-scale applications. Often considered a modern SCADA system [8], this design allows SCADA systems to be geographically dispersed. While Networked SCADA shares similarities with Distributed SCADA, a key distinction lies in the use of open protocols and standards for communication instead of proprietary ones. This facilitates the distribution of MTU functionality across a WAN, as depicted in Fig. 2.3.

The adoption of open standards also enables the connection of third-party peripheral devices to the network. A pivotal advancement in Networked SCADA was the implementation of the Internet Protocol for communication between MTU and RTUs, enhancing disaster resilience.

2.2.4 Fourth Generation - Industry 4.0

Industries have harnessed technology's capabilities to design, monitor, and control systems more efficiently. The integration of Internet of Things (IoT) advancements

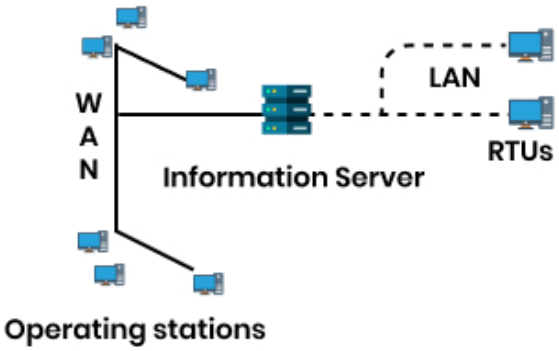


Figure 2.3: Networked SCADA Systems

and cost-effective cloud computing with SCADA systems has significantly reduced infrastructure and deployment costs. Additionally, integration and maintenance have become more straightforward compared to previous generations [12]. Industry 4.0 serves as an exemplar of a fourth-generation SCADA system, as depicted in Fig. 2.4, incorporating distributed cognitive computing, Cyber-Physical Systems (CPS), IoT, and cloud computing [4].

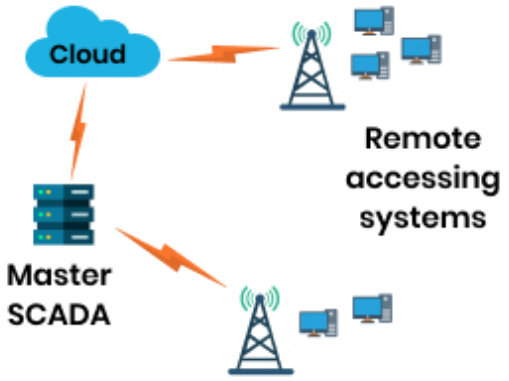


Figure 2.4: Fourth Generation - Industry 4.0

While SCADA systems already exhibit some IoT characteristics, such as data access, manipulation, and visualization, IoT distinguishes itself through interoperability, scalability, and advanced big data analytics capabilities. Data collection and management in these systems rely on open communication standards, with data stored in the cloud for extracting valuable insights. The Industrial Internet of Things (IIoT) or Industry 4.0 represents advancements in fourth-generation SCADA systems, essentially

describing IoT applications in industries. It constitutes a network of devices primarily focused on transmitting and controlling critical information and deriving insights from extensive data sets.

To integrate IIoT into SCADA, various devices and protocols must be incorporated into the existing system. IIoT has also bolstered its resilience by leveraging data-driven techniques to identify anomalous behavior [14, 15, 16]. Additionally, Continuous Improvement (CI) systems prioritize minimizing losses due to downtime. However, predictive maintenance strategies can mitigate these downtimes, thereby enhancing system productivity [17].

2.3 SCADA Communication Protocols

Communication protocols serve as guidelines for data representation and exchange across communication links [18]. In the realm of SCADA, these protocols are integral to MTU-RTU interactions. Initially, remote communications were facilitated through instruments and protective relays using local RS232 connections or dial-up modem interfaces. However, scalability concerns prompted a shift towards more sophisticated protocols [19].

Given that a SCADA system comprises multiple components, using vendor-specific protocols for each component can hinder inter-component communication. Vendor-specific SCADA protocols come with their unique communication rules and procedures, encompassing data presentation, conversion, address assignment, command generation, and status information. To foster interoperability and cost-effectiveness, open standards have been introduced.

The introduction of the Open System Interconnection (OSI) Model in 1984 aimed to promote open protocols [20]. This model delineates the data communication process into seven distinct layers, each detailing how data is managed at various transmission stages. Open protocols enhance device availability, interoperability, vendor independence, cost optimization, and facilitate easier technical support.

A comprehensive analysis of various communication protocols is provided below.

2.3.1 Modbus

The Modbus transmission protocol, an application layer messaging protocol, was introduced by Gould Modicon for their Modicon programmable controller [21]. It stands out as the most widely adopted protocol for electronic device connections, thanks to its openly published nature and user-friendly design. Additionally, it serves as a communication link between MTUs and RTUs. A standard Modbus network accommodates

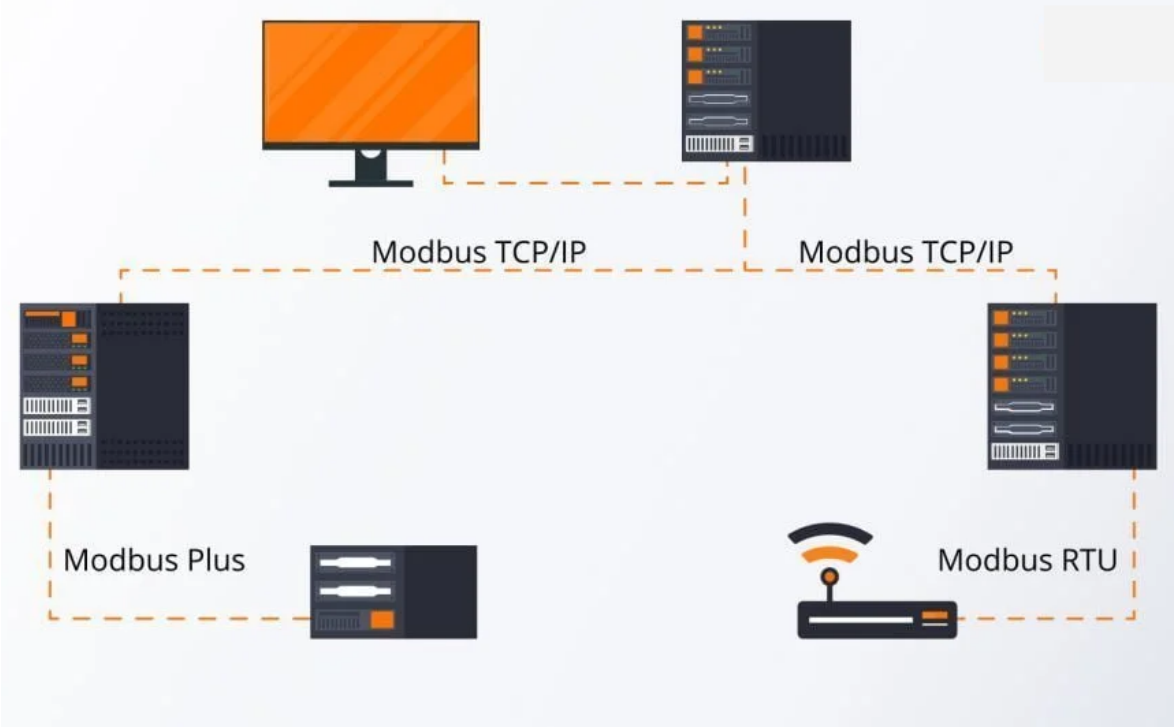


Figure 2.5: Modbus protocol

one master and up to two hundred forty-seven slaves. RTUs respond solely to targeted messages while disregarding broadcasts [22]. The protocol employs four communication message types: request/response messages to/from MTUs, acknowledgement messages confirming successful message delivery to both MTUs and RTUs. MTUs can communicate with slaves and allocate individual addresses ranging from 1 to 247 to each slave. An enhanced variant, Modbus/TCP, prioritizes reliable communication over the Internet and Intranet, leveraging TCP/IP's error detection mechanisms.

Introduced to address vulnerabilities in master terminals, the Modbus Plus protocol operates on a token-based system, Fig.2.6

The Modbus protocol compiles the request messages sent from the remote terminal

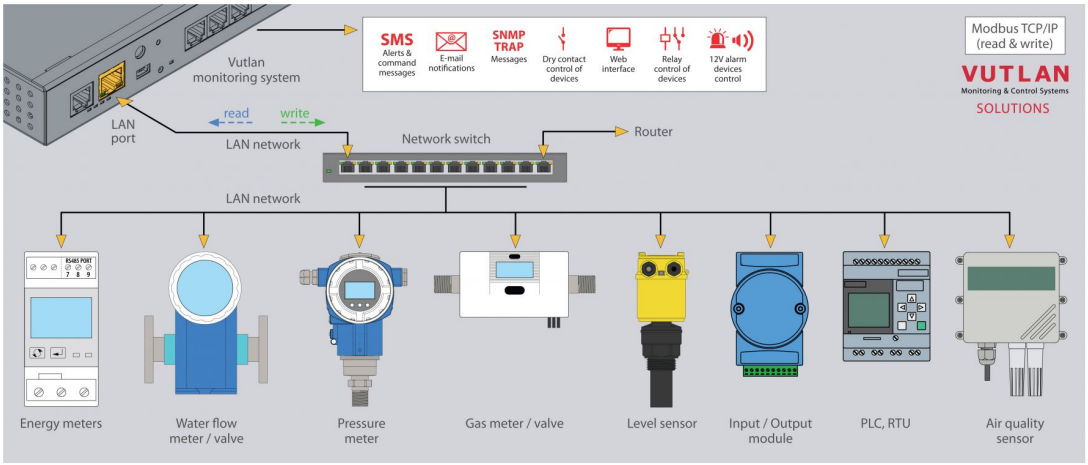


Figure 2.6: Modbus

to the master terminal into a Protocol Data Unit (PDU), combining data requests and function codes. The PDU transforms into an application data unit by incorporating function code fields at the OSI layer. Conversely, the master terminal responds to the remote terminal. However, due to additional cabling and communication challenges, it isn't the preferred choice for real-time communication.

2.3.2 Distributed Network Protocol(DNP3)

The Distributed Network Protocol (DNP) ,also known as IEEE Std 1815, is grounded on the Enhanced Performance Architecture (EPA) model, a more streamlined version of the OSI layer architecture. Developed by Harris, Distributed Automation Products [7], DNP3 was created to achieve open and standard-based interoperability among RTUs, MTUs, and Programmable Logic Controllers (PLCs).

The DNP3 protocol accommodates various network setups, with three primary configurations illustrated in Figure 2.7 [2]. In the "one-on-one" configuration, a single master and one outstation device communicate over a dedicated link, like a dial-up phone line. The "multi-drop" setup features one master communicating with multiple outstations. While each outstation receives all requests from the master, they only respond to messages specifically directed at them. In the "hierarchical" configuration, a device serves as an outstation in one segment and a master in another, earning it the title of a "sub-master" due to its dual functionality.

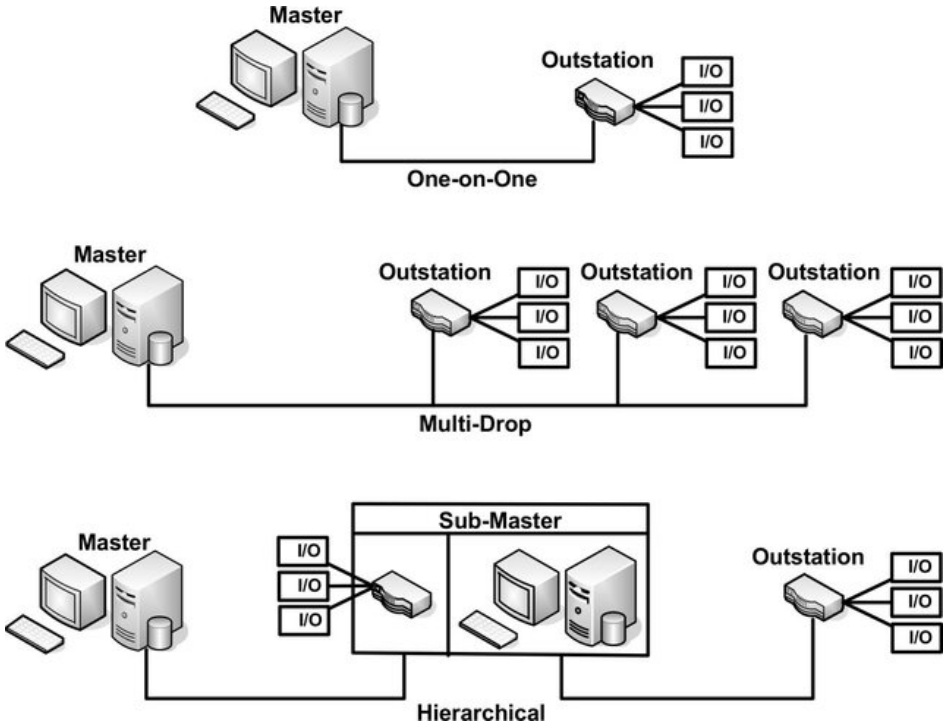


Figure 2.7: Different DNP3 configurations

The DNP3 protocol comprises core components like the data link layer convention, transport functions, application conventions, and a data link library. An additional user layer is integrated into the EPA architecture, responsible for tasks like multiplexing, data fragmentation, prioritization, and error checking. Within the DNP3 protocol's layered architecture, the application layer defines packet design, services, and procedures specific to its layer. This data is then directed to the pseudo-transport layer, which segments the data unit before passing it to the data link layer [19], which subsequently sends it to the physical layer [23]. The protocol facilitates multi-slave, peer-to-peer (P2P), and multi-master communication.

2.3.3 IEC 60870-5 Protocol

The International Electro-Technical Commission (IEC) 60870-5 protocol is also structured on the EPA model. An application layer is incorporated as an extra top layer in the EPA architecture, detailing functions relevant to the telecontrol framework, Fig.2.8. Variants of the telecontrol framework, such as T101, T102, T103, and T104, define distinct specifications, data objects, and function codes at the application proto-

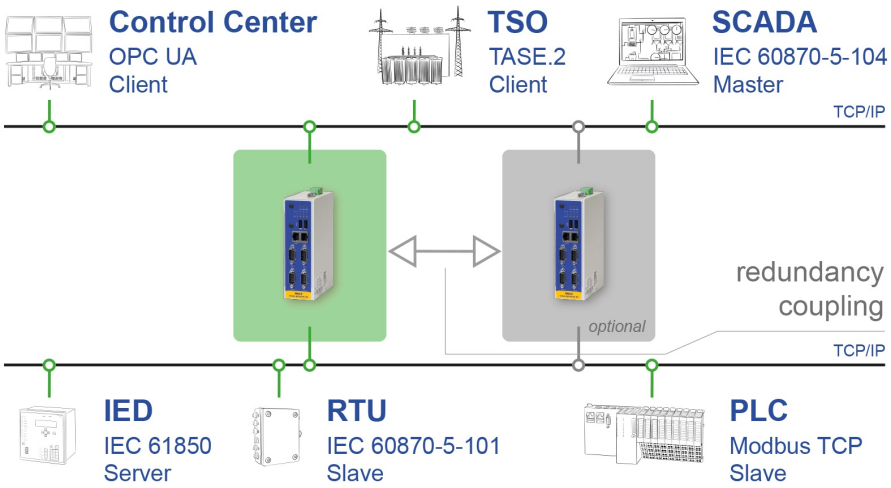


Figure 2.8: IEC 60870-5 Protocol

col level [24]. While the DNP3 layer stack includes a pseudo-transport layer for efficient transmission, this is not utilized in the IEC 60870-5 protocol.

2.3.4 Foundation Fieldbus Protocol

This protocole introduced by the FieldComm Group [25], the Foundation Fieldbus protocol employs a four-layer stack comprising the user, application, data link, and physical layers. Following the OSI layer model, the architecture of Foundation Fieldbus incorporates the user layer as an additional top layer above the application layer, Figure 2.9. This user layer serves as a bridge between software applications and field devices.

Its advantages include seamless process integration, multifunctional devices, adherence to open standards, and reduced costs associated with extensive wiring, setting it apart from other protocols.

2.3.5 Profibus Protocol

The Process Field Bus (Profibus) protocol was championed by BMBF in Germany. The data communication between MTU and RTUs operates in a cyclic manner, with the MTU reading input data from the RTUs and writing output data to them. The protocol has three versions: Field Bus Message Specification (FMS), Distributed Peripheral

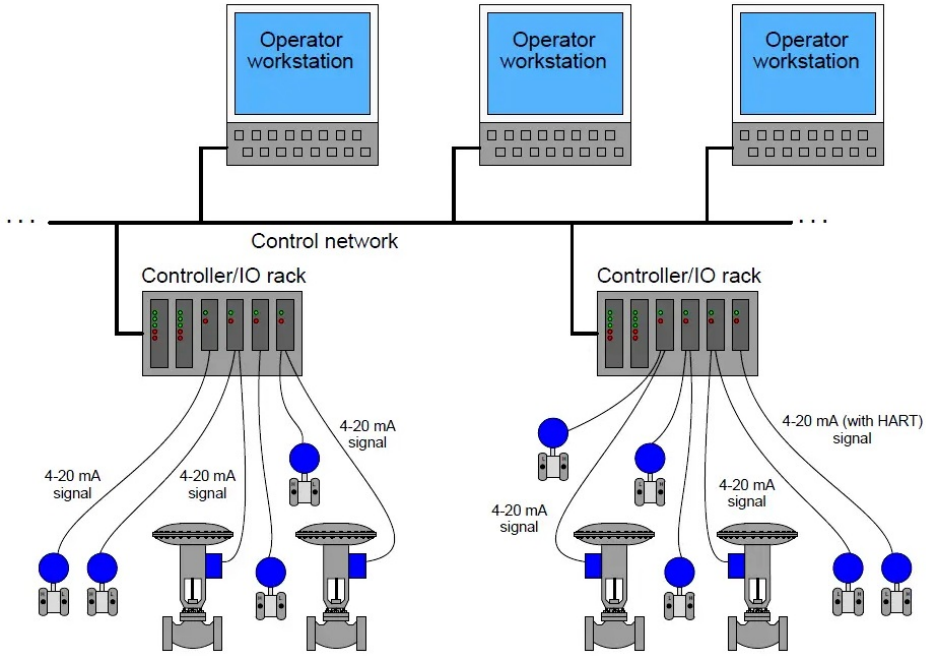


Figure 2.9: Foundation Fieldbus Protocol

(DP), and Profibus Variations (PA). Profibus is predominantly utilized in discrete manufacturing and process control [7].

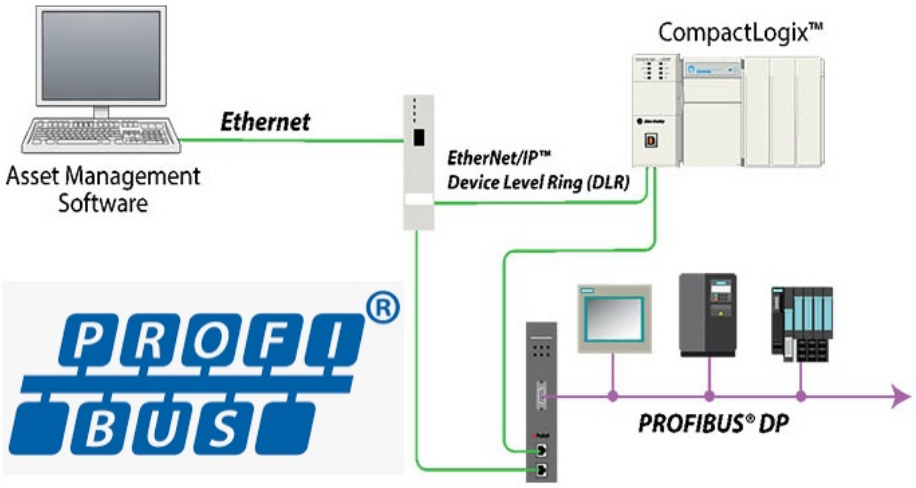


Figure 2.10: PROFIBUS Protocol

2.3.6 IEC 61850 Protocol

The International Electro-Technical Commission (IEC) 61850 protocol was formulated by the IEC Technical Committee 57 [26]. A consortium of manufacturers including ABB, Alstom, Schneider, SEL, Siemens, and Toshiba proposed this protocol to enhance equipment interoperability [27]. What sets this protocol apart from other OSI reference models is its comprehensive coverage, detailing not just data transmission but also execution and storage. Both the source and destination addresses consist of 48 bits each [28].

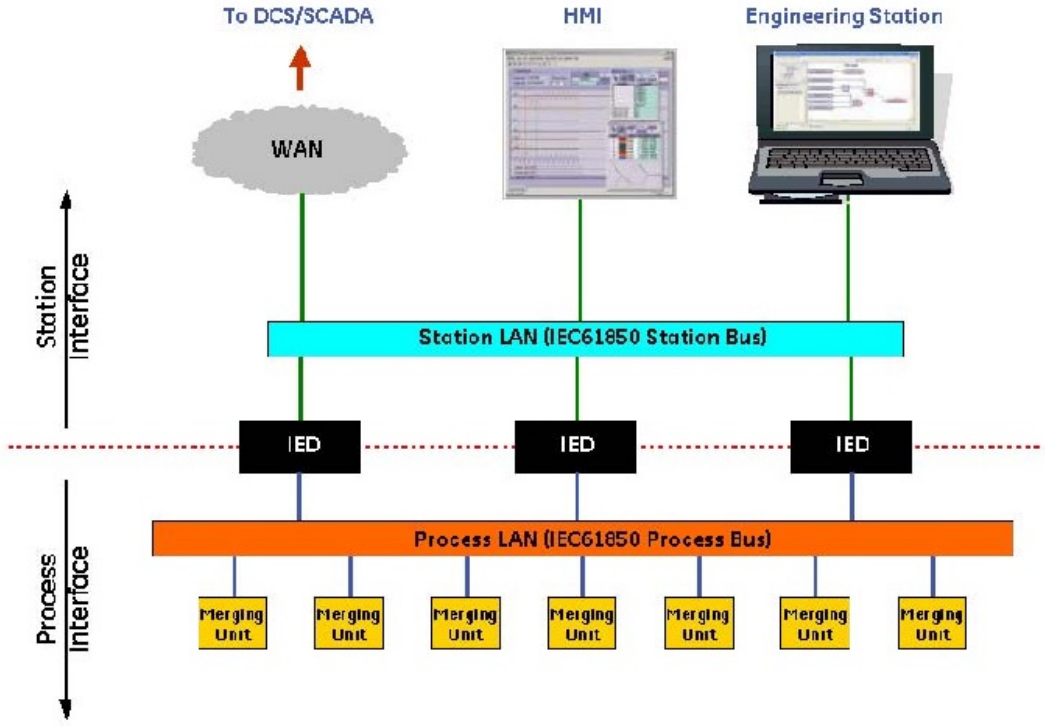


Figure 2.11: iec61850

Widely adopted in electrical substations, IEC 61850 facilitates communication among intelligent electronic devices [26]. Additionally, its abstract data models can be adapted to various other protocols like MMS, GOOSE, and SMV [29].

2.4 Evolution of SCADA Communication Protocols

Consequently, SCADA communication standards have evolved from proprietary to commercial/open-source standards. The reliability of a SCADA system hinges on its communication protocols. Based on previous studies and comparative analysis of the communication protocols suitable for SCADA. Given that DNP3, IEC 60870-5-101, and Foundation Fieldbus are open standards [30], they see broader adoption. Both DNP3 and IEC 60870-5-101 primarily address Data Acquisition Interoperability at the initial level, essential for external substation communication [23]. DNP3 facilitates varied polling frequencies in SCADA systems, while IEC 60870-5-101 maintains consistent polling rates, making it suitable for limited bandwidth scenarios. DNP3's packet size surpasses that of IEC 60870-5-101, making DNP3 preferable for longer distances. Modbus is predominantly used in low-volume data exchange applications [19]. It operates as a swift and secure protocol, capable of transmitting substantial data in a single message [18].

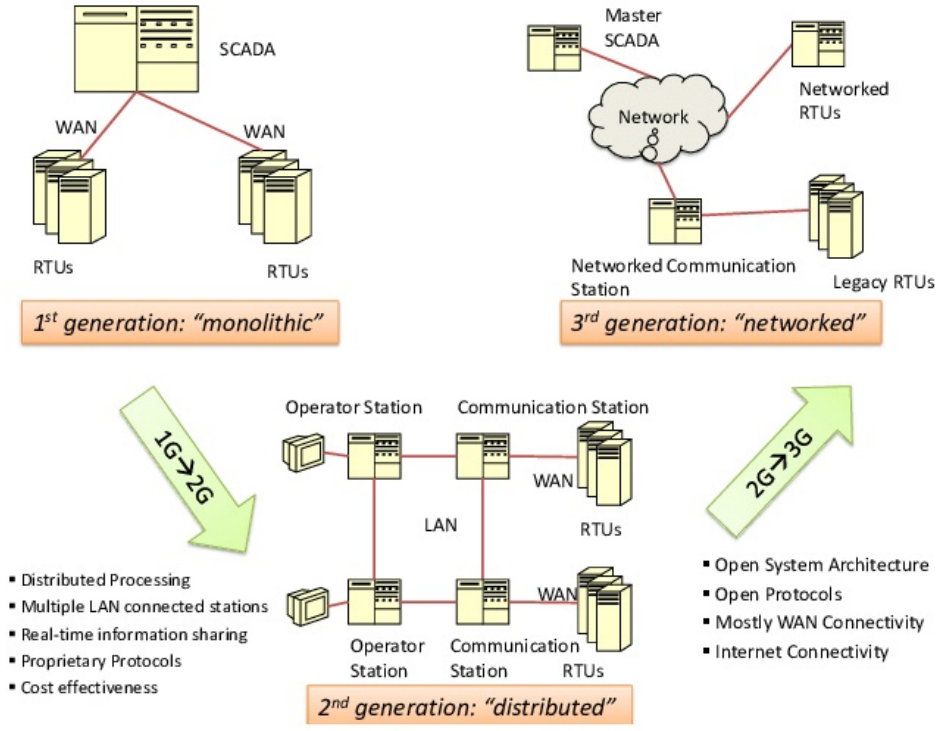


Figure 2.12: SCADA evolution

While Modbus functions as a single-layer protocol, DNP3 and Foundation Fieldbus employ a four-layer architecture. Modbus is chiefly designed for low data volume tasks. Only DNP3-SA and Profibus offer encryption and authentication control, contrasting with Modbus's lack of security. While IEC-6870-5-101 and IEC 61850 don't support encryption, they do permit authentication control. Several factors influence protocol selection for communication, including system utility and the SCADA system's deployment location. Opting for the most suitable protocols ensures scalability potential for the developed system. Flexibility in integrating security within communication protocols is crucial. Beyond these conventional communication protocols, IIoT-based SCADA systems employ various IoT protocols like Zigbee, Bluetooth Low Energy (BLE), and Long Range (LoRA) for communication.

Chapter 3

Human Interface Machine (HMI)

Contents

3.1 Introduction

Human-Machine Interface (HMI) refers to the user interface that connects a person to a machine, system, or device. It provides a means of interaction between the user and the machine, allowing users to control, monitor, and manage the machine's operations effectively. HMIs are crucial components in various industries, including manufacturing, automotive, healthcare, and utilities.

3.2 Components of HMI

Both hardware and software are the main components of the HMI interface [5].

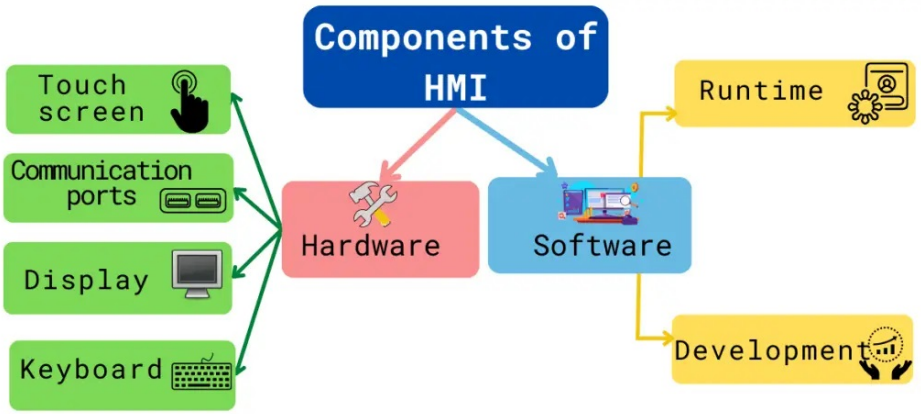


Figure 3.1: Components of HMI

3.2.1 Visual Display Unit (VDU) or Screen

This is where the information is displayed to the user. It can be a touchscreen, monitor, or any other display device.

Figure 3.2: Visual Display Unit (VDU)

3.2.2 Input Devices

These devices allow users to interact with the HMI. Common input devices include Industrial touchscreens, Industrial Keyboards, Industrial Mouse, and joysticks.

- **Industrial Touchscreens**: a display device which allows the user to interact with a computer by touching areas on the screen.

Figure 3.3: Touchscreens (front side)

- **Industrial Keyboards** Housed in aluminum, foil, glass, stainless steel, or silicone, Industrial keyboards are rated IP65 or IP68 and can include a mouse

Figure 3.4: Touchscreens (back side)

button, joy-stick, mouse-pad, or numeric keypad.

- **Industrial Mouse** Encased in stainless steel or silicone with a plastic base, Industrial mice are Industrial mice protection level are rated IP65, IP67 or IP68. Some mice can be immersed into detergents

- **Industrial joy-stick** Industrial joysticks are invaluable control devices for precisely operating machinery of all sizes. Some utilize switches which are specific to each possible direction and are activated by direct input.

  In other types of joysticks, the output signal continuously varies with lever deflection.

3.2.3 Control Devices

These devices enable users to control the machine or system through the HMI. Examples include buttons, switches, and sliders.

3.2.4 Communication Interface

This component facilitates communication between the HMI and the machine or system it controls. It can support various communication protocols like Modbus, Ethernet/IP, and Profinet.

Figure 3.5: Industrial Keyboard

Figure 3.6: Enter Caption

3.2.5 Software

The software running on the HMI processes the data, controls the display, and manages user inputs. It may include programming environments, runtime environments, and visualization tools.

Figure 3.7: Industrial Mouse

Figure 3.8: Industrial joy-stick

Figure 3.9: Industrial joy-stick

Figure 3.10: Buttons

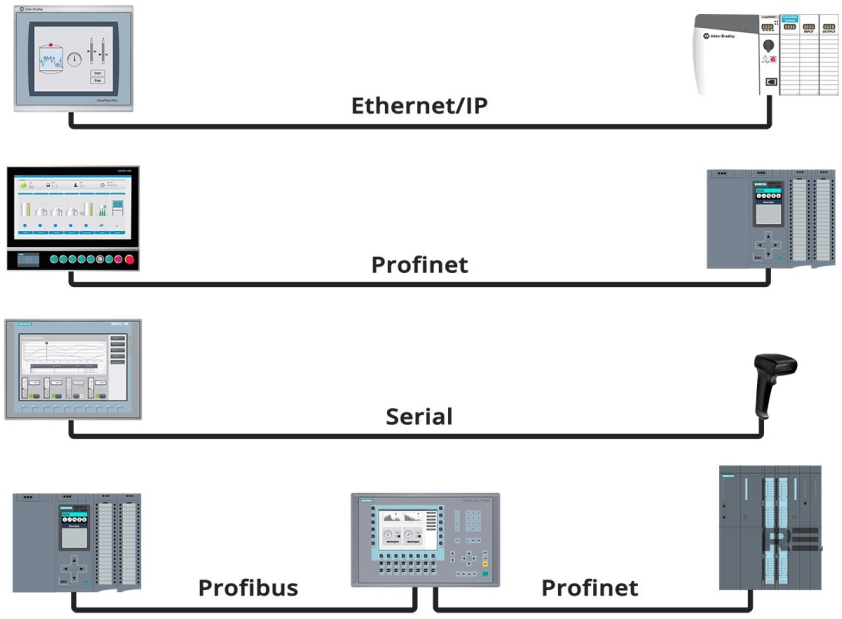


Figure 3.11: HMI Communication Interface

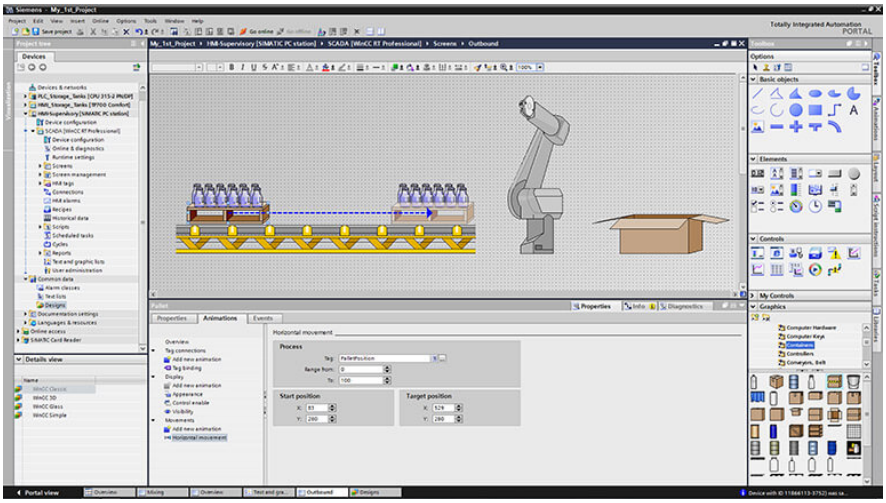


Figure 3.12: HMI software

3.3 Types of HMIs

There are various kinds of HMIs used in industrial settings.

3.3.1 Graphical User Interface (GUI)

Graphical User Interfaces (GUIs) are arguably the most prevalent form of HMI interface. They convey information to operators using graphical elements like buttons, icons, and menus, facilitating interaction with the system.

Figure 3.13: Graphical User Interface

GUIs are capable of showcasing real-time data, managing parameters, and issuing alarms and notifications.

3.3.2 Touchscreen HMIs

These HMIs Touchscreen interfaces have gained popularity in industrial environments owing to their intuitive design.

Operators can interact directly with the system by touching the screen, eliminating the requirement for external input devices such as keyboards or mice. Touchscreens are frequently integrated with GUIs to enhance the user experience.

Figure 3.14: Touchscreen HMI

3.3.3 Web-based HMIs

With the evolution of web technologies, numerous HMIs now utilize web-based interfaces.

Figure 3.15: Web-based HMI

These interfaces are accessible through web browsers on a range of devices including computers, tablets, and smartphones. Web-based HMIs provide flexibility in accessi-

bility, enabling operators to remotely monitor and control systems.

3.3.4 Mobile HMIs

Mobile HMIs are tailored for smartphones and tablets, offering operators the convenience of overseeing and managing industrial processes while on the move. These

Figure 3.16: Mobile HMI

interfaces typically incorporate responsive design elements to guarantee usability across various screen sizes.

3.4 Advantages of HMI

There are many advantages of Human-Machine Interfaces (HMIs):

1. **Enhanced operational efficiency** The human-machine interface (HMI) serves as a powerful tool for empowering operators and enhancing productivity. With intuitive interfaces, HMIs facilitate quicker decision-making and significantly reduce training time, ultimately boosting operator productivity.

2. **Intuitive Interfaces for Agile Decision-Making:** HMIs revolutionize the operator experience by offering intuitive interfaces aligned with human cognitive patterns. Through streamlined menu structures, contextualized data displays,

and straightforward controls, operators can swiftly access vital insights and execute decisions with remarkable agility.

3. **Customizable Dashboards and Real-Time Data Visualization**

   A key aspect of HMI design is its customizable dashboards and real-time data visualization capabilities. This feature allows operators to configure displays tailored to their specific needs, ensuring that the most pertinent metrics and operational parameters are readily accessible. Real-time data visualization further enhances this advantage by presenting actionable insights at a glance, enabling informed decision-making and proactive responses to dynamic production scenarios.

4. **Improved operational visibility**

   HMIs serve as the frontline of operational visibility, providing comprehensive insights into machine performance, production metrics, and process status. This heightened visibility facilitates proactive decision-making and improved operational efficiency.

5. **Comprehensive Insights and Performance Metrics**

   HMIs act as gateways to a wealth of operational data, offering real-time access to critical performance metrics such as production output, machine utilization, energy consumption, and quality indicators. By aggregating and presenting this information coherently, HMIs empower operators and management alike with a holistic understanding of operational dynamics, facilitating informed decision-making and strategic planning.

6. **Real-Time Monitoring for Proactive Maintenance**

   The hallmark of HMI prowess lies in its capability for real-time monitoring, enabling operators to oversee machinery performance and process parameters. This real-time insight facilitates prompt identification of anomalies or inefficiencies and supports proactive maintenance initiatives. By preemptively addressing potential issues and deterring unexpected downtime, HMIs play a pivotal role in fortifying operational continuity and optimizing asset utilization.

7. **Streamlined process control**

   In industrial automation, HMIs play a crucial role in enabling centralized control of complex systems. By coordinating disparate elements into a cohesive operational framework, HMIs streamline operations and optimize resource utilization, thereby propelling productivity.

8. **Centralized Control and Operational Harmony**

   HMIs serve as the nerve center of industrial processes, consolidating control functionalities and data visualization within a unified interface. This centralized control architecture fosters operational harmony and empowers operators to orchestrate multifaceted systems with precision and confidence. Through seamless integration with diverse equipment and machinery, HMIs enhance operational agility and responsiveness, laying the groundwork for increased efficiency and resource optimization.

9. **Touch-Screen Interfaces and Interactive Controls**

   At the heart of the HMI are its touch-screen interfaces and interactive controls, revolutionizing the landscape of process adjustments and configuration changes. By offering intuitive touch-based interactions and responsive controls, HMIs facilitate operational parameter adjustments accessible to operators across diverse skill levels. This user-centric approach expedites process adjustments and mitigates the likelihood of errors, enhancing operational reliability and adaptability [6].

10. **Integration with IOT and analytics**

    The convergence of HMIs with Internet of Things (IoT) devices heralds a new era of operational intelligence, empowering industrial enterprises with unparalleled capabilities for data-driven decision-making. This synergy amplifies operational insights and unlocks the potential for predictive maintenance, condition monitoring, and performance optimization.

11. **Empowering Data-Driven Decision-Making**

HMIs equipped with IoT integration capabilities serve as conduits for harnessing the flood of data originating from interconnected devices across the industrial ecosystem. By coordinating this diverse array of data streams, HMIs enable operators and stakeholders to glean actionable insights and make informed decisions rooted in data and analytics. This data-driven approach allows proactive responsiveness and strategic foresight.

12. **Unleashing the Potential for Predictive Maintenance and Performance Optimization**

    The integration of HMIs with IoT devices drives industrial enterprises into the realm of predictive maintenance, where anomalies and potential failures are foreseen and preemptively addressed. Through real-time condition monitoring and predictive analytics facilitated by HMIs, operators gain the ability to anticipate maintenance requirements, optimize equipment performance, and avert costly downtime. Additionally, the amalgamation of HMI-enabled data analytics and IoT devices fosters continuous refinement of operational processes and resource utilization.

13. **Flexibility in diverse industrial environments**

    HMIs embody adaptability, seamlessly integrating into diverse industrial environments and accommodating customized workflows with finesse. This inherent flexibility underpins agile manufacturing processes and positions industrial enterprises to swiftly respond to evolving business requirements, epitomizing operational agility and resilience.

14. **Accommodating Customized Workflows**

    HMIs excel in accommodating bespoke workflows tailored to the unique demands of varied industrial settings. Whether in discrete manufacturing, process industries, or hybrid production environments, HMIs adapt to specific operational nuances, ensuring that critical processes are harmonized and monitored with precision. This customization prowess fosters operational harmony and reinforces the enterprise's capacity to adapt swiftly to shifting market demands and production

paradigms.

15. **Supporting Agile Manufacturing Processes**

    Adaptable HMI solutions play a pivotal role in underpinning agile manufacturing processes, where responsiveness, efficiency, and adaptability reign supreme. By seamlessly aligning with dynamic production requisites and accommodating rapid reconfigurations

3.5 Conclusion

Human-Machine Interface (HMI) plays a vital role in connecting users to machines and systems, enabling efficient monitoring and control. With advancements in technology, HMIs have evolved to offer more intuitive interfaces, remote access capabilities, and real-time monitoring features. However, ensuring security, usability, compatibility, and scalability remains essential when designing and implementing HMIs in various applications.

By understanding the components, types, advantages, and challenges of HMIs, organizations can leverage this technology to improve productivity, enhance user experience, and drive innovation in their operations.

Chapter 4

Lab Work

Contents

4.1 Introduction

Lab work SCADA offers a practical approach to learning about SCADA systems in controlled environments. Through hands-on experiments and simulations, students gain valuable insights into the functionalities, configurations, and applications of SCADA technology.

In lab work SCADA setups, students interact with SCADA software and hardware components to monitor, control, and analyze simulated processes or systems. These experiments mimic real-world industrial scenarios, providing participants with practical experience in configuring SCADA systems, managing alarms, visualizing data, and troubleshooting common issues.

By engaging in lab-based SCADA activities,students develop a deeper understanding of SCADA concepts and gain essential skills for working with SCADA systems in various industries. Additionally, collaborative projects and teamwork opportunities in laboratory settings enhance the learning experience and prepare students for real-world applications of SCADA technology.

In this chapter, we present six laboratory works:

1. **Getting Started-WinCC Flexible 2008**
2. **Tag Management**
3. **Alarm Management and Historical Data Configuration**
4. **Data Logging and Trend Display**
5. **SCADA Network configuration PROFIBUS & MPI**
6. **Project 01 : Parking Management**

4.2 Lab's work No 01 : Getting Started-WinCC Flexible 2008

The objective of this lab session is to introduce students to the WinCC Flexible environment and its basic functionalities, Also teach students how to design and configure screens for an HMI [7].

- Activities:

1. Overview of the WinCC Flexible interface and main components.
2. Creating a new project: setting up project parameters, selecting device types.
3. Exploring the project structure: project view, device view, and working with different editors.
4. Simple hands-on exercise: create a basic project, save it, and understand the file structure.
5. Designing operator interfaces: adding static and dynamic objects (e.g., text fields, buttons, images).
6. Configuring navigation: creating menus, buttons, and screen-switching logic.
7. Customizing screen properties: layout, color schemes, and fonts.
8. Hands-on exercise: design a main screen with navigation to sub-screens.

4.2.0.1 Creating a project

1. ***What is a project?***

   The project serves as the foundation for configuring the user interface. Ensure to create and set up all the necessary objects within the project to effectively operate and monitor as per the required specifications.

   - Screens are utilized to illustrate and manage the project system.

Figure 4.1: WinCC Flexible 2008

- Tags facilitate the transfer of data between the HMI device and the project system.
- Alarms are implemented to indicate the operational status of the project system on the HMI device.

2. ***Start WinCC flexible***

   The WinCC flexible project wizard initiates. It assists in project creation by leading students through configuration settings step by step. Offering various scenarios for commonly needed configurations, the project wizard aids in completing the setup by selecting the provided scenarios.

3. ***Create a new project***

4. ***Choose the control unit***

   To select the type of HMI, there are several configurations to choose from:

   - Small configuration machine
   - Large configuration machine
   - Distributed configuration machine
   - Choosing HMI, Network & PLC

Figure 4.2: Start WinCC flexible 2008

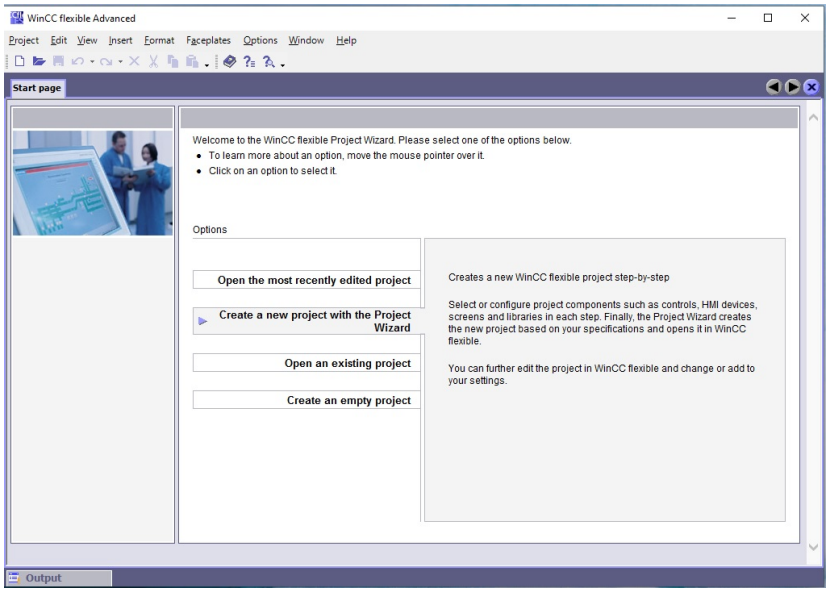


Figure 4.3: Create a new project

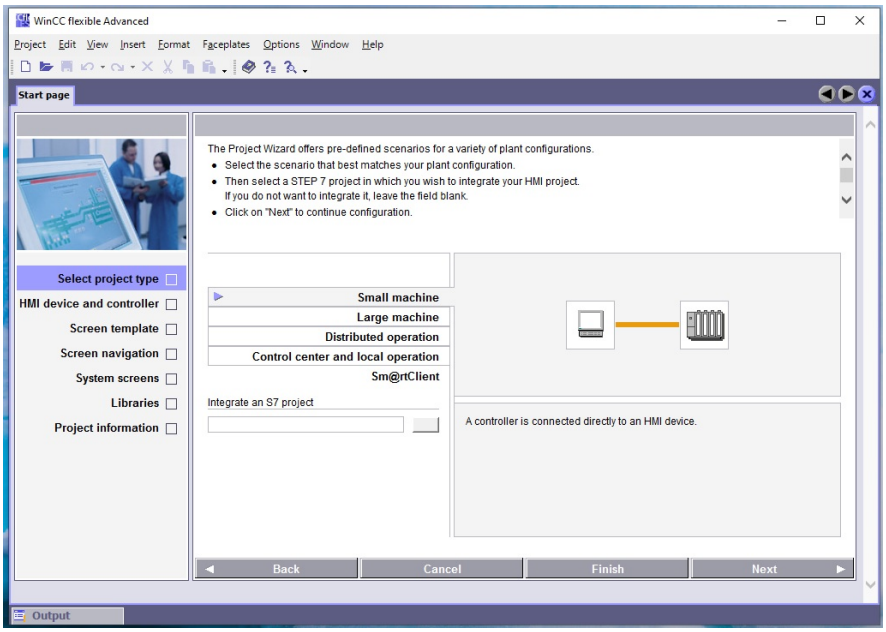


Figure 4.4: Small configuration

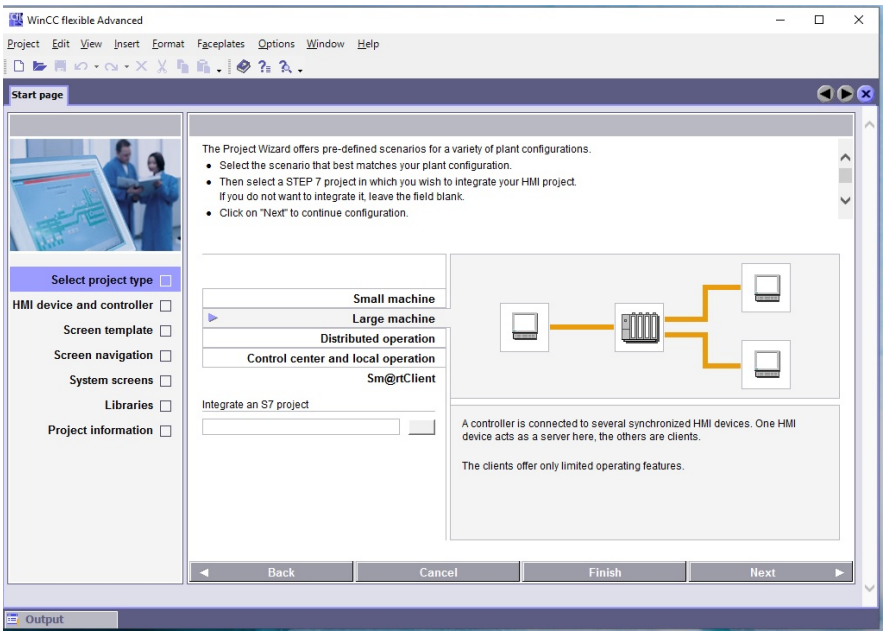


Figure 4.5: Large configuration machine

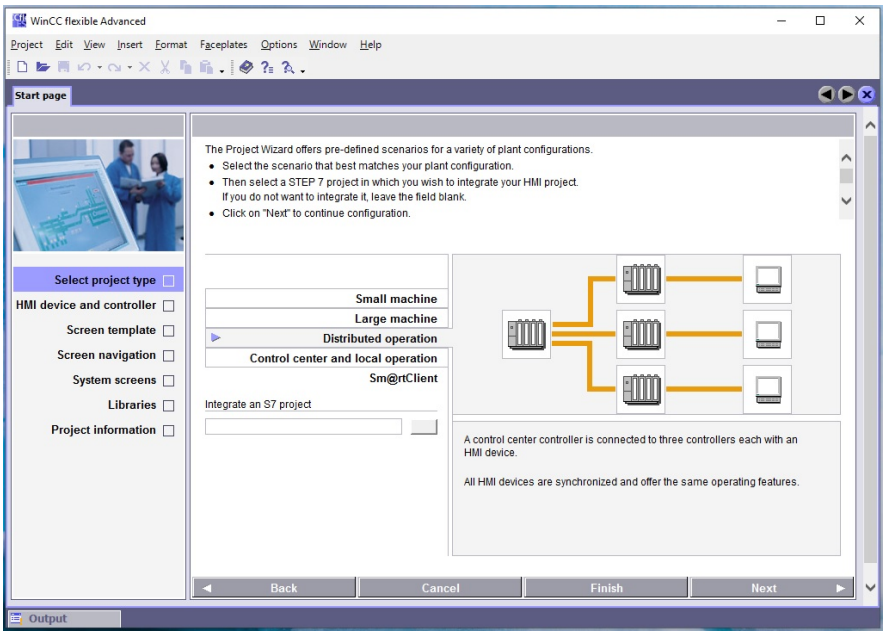


Figure 4.6: Distributed configuration machine

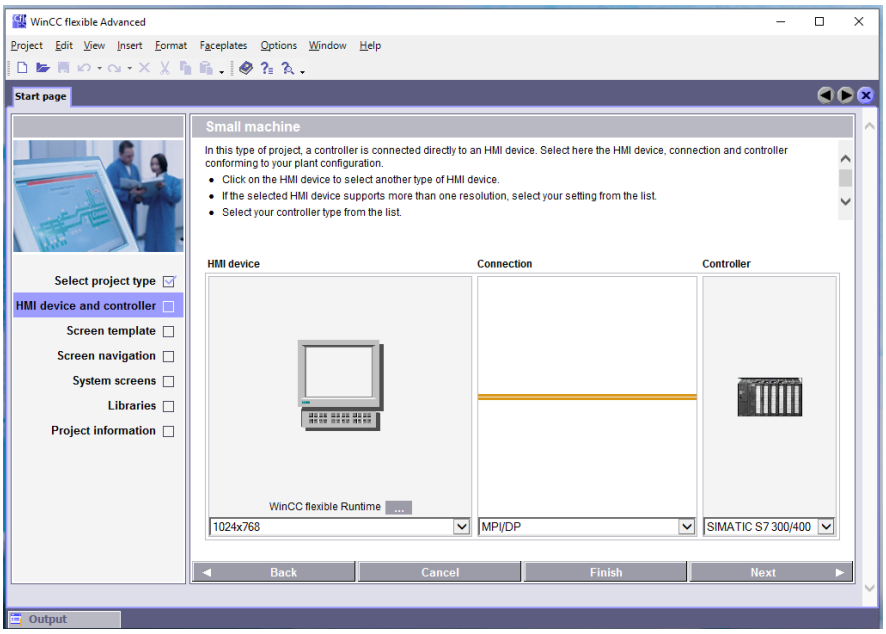


Figure 4.7: Choosing HMI, Network & PLC

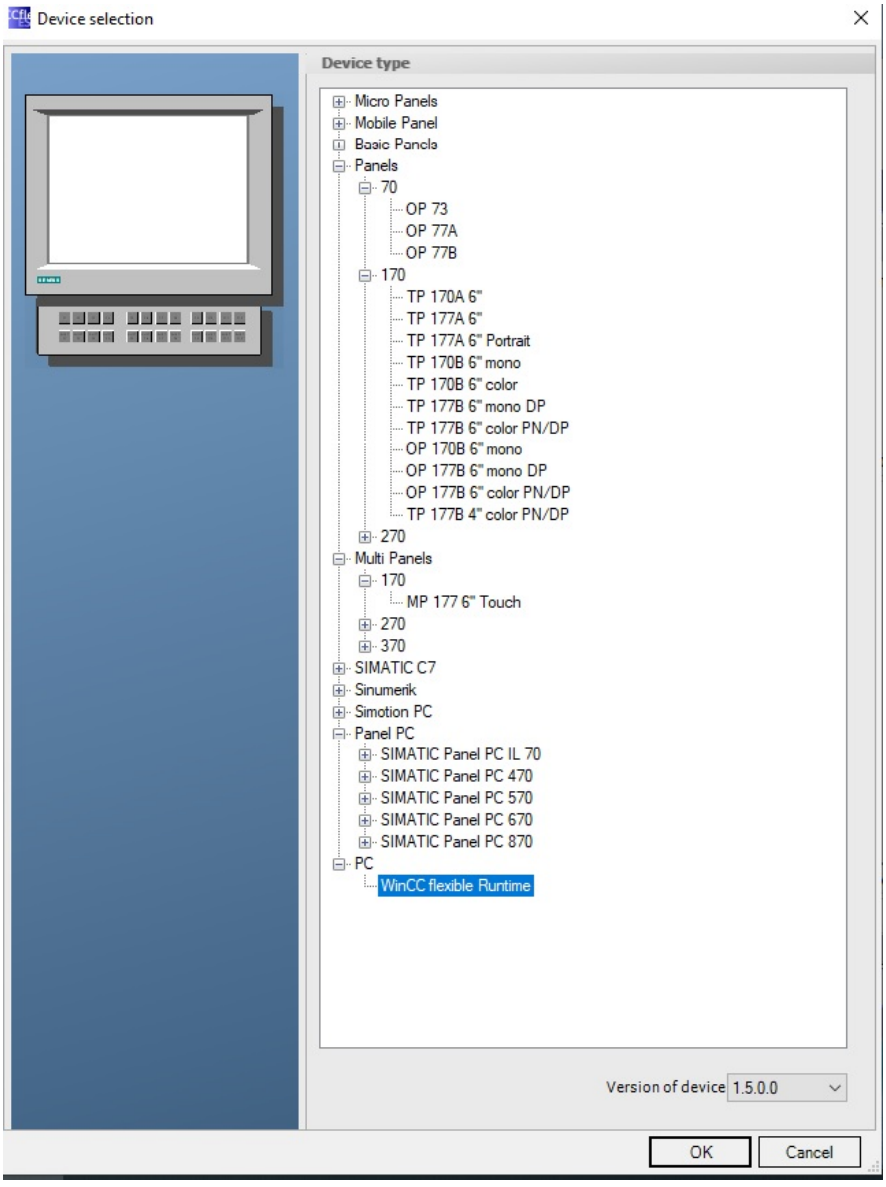


Figure 4.8: Choosing HMI

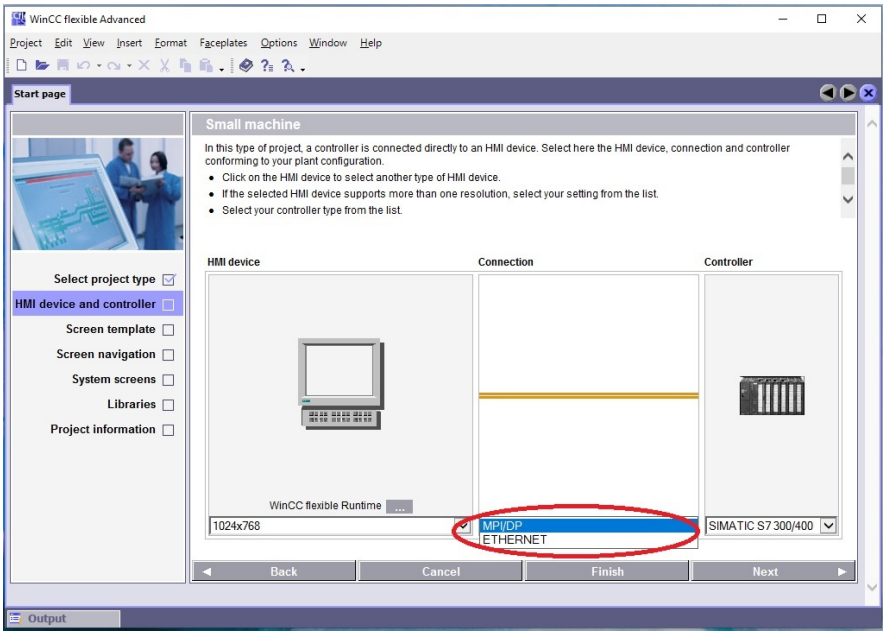


Figure 4.9: Choosing Network

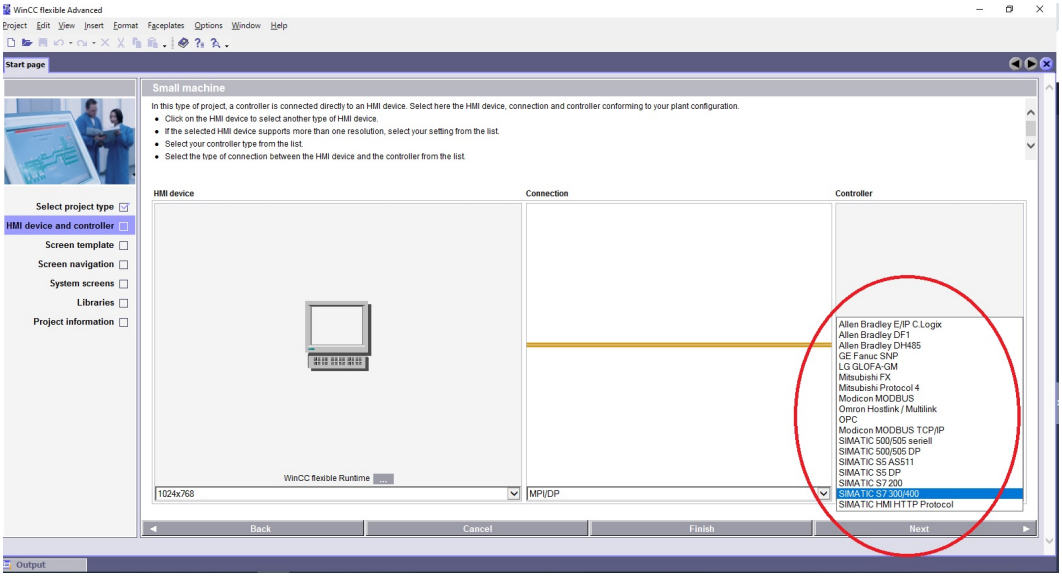


Figure 4.10: Choosing Controller PLC

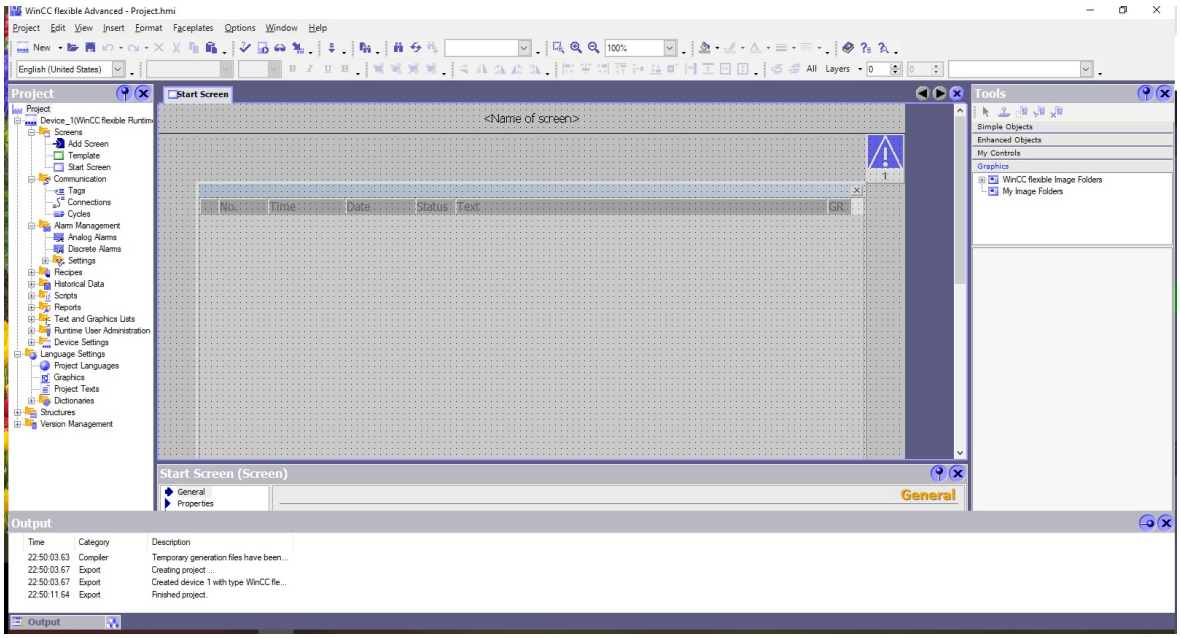


Figure 4.11: Project WinCC

4.3 Lab Work No 02: Tag Management

Lab's work Objective: Learn to create and manage tags for effective data communication. Activities:

1. Understanding tags: difference between internal and external tags DI/DO, AI/AI & memory variables .
2. Creating tags: defining tag properties (name, data type, address).
3. Linking tags to PLC variables: setting up communication channels.
4. Hands-on exercise: create and configure tags for a simple automation task.

4.4 Lab Work No 03: Alarm Management and Historical Data Configuration

Lab's work Objective: Configure alarms and historical data logging to monitor system performance.

1. Setting up alarms: defining alarm conditions, severity levels, and messages.
2. Configuring alarm actions: sound alarms, log events, send notifications.
3. Historical data configuration: setting up data logging, storage, and retrieval.
4. Hands-on exercise: configure alarms for a temperature control system and set up historical data logging.

4.5 Lab Work No 04: Data Logging and Trend Display

Lab's work Objective: Learn to log process data and create trend displays for analysis.

1. Configuring data logging: selecting variables, defining logging intervals.

2. Creating trend displays: adding trend objects, configuring display settings.

3. Analyzing trends: interpreting trend data, identifying patterns.

4. Hands-on exercise: log and display temperature and pressure trends over time.

4.6 Lab Work No 04: SCADA Network configuration PROFIBUS & MPI

Objective: Configure a SCADA network using PROFIBUS and MPI protocols to establish communication between different devices.

1. ***Introduction to PROFIBUS and MPI Protocols Overview of PROFIBUS:*** Understand the basics of PROFIBUS, its types (PROFIBUS DP, PROFIBUS PA), and its applications. Learn about the PROFIBUS communication model and its advantages in industrial environments. Overview of MPI (Multi-Point Interface): Understand MPI protocol, its use for communication between Siemens PLCs and other devices. Learn the advantages and typical use cases of MPI.

2. ***Setting Up the Hardware Components Required:***

   Siemens PLCs (e.g., S7-300/400 series) PROFIBUS cables and connectors MPI cables HMI device (e.g., Siemens HMI panel) SCADA software (e.g., WinCC) Connecting the Devices:

   Connect the PLCs using PROFIBUS cables in a daisy-chain or star topology. Ensure termination resistors are used at the ends of the PROFIBUS network. Connect the PLCs and HMI using MPI cables to create an MPI network. Power on all devices.

3. ***Configuring the PROFIBUS Network Open the SCADA Software:***

   Launch WinCC or your preferred SCADA software. Creating a New Project:

   Create a new project and configure the project settings (project name, save location, etc.). Adding Devices to the Project:

Add all the PLCs and HMI devices to the project. For each device, specify the device type and communication parameters. Configuring PROFIBUS Settings:

Navigate to the network configuration section. Add a new PROFIBUS network. Assign each device to the PROFIBUS network. Set the network address for each device (unique address for each device on the network). Setting Communication Parameters:

Configure the communication speed (baud rate) and other relevant parameters for the PROFIBUS network. Ensure the settings are compatible across all devices.

4. ***Configuring the MPI Network Adding MPI Network:***

   In the SCADA software, add a new MPI network. Assign the PLCs and HMI to the MPI network. Setting MPI Parameters:

   Assign unique MPI addresses to each device. Configure the communication parameters (e.g., transmission rate). Interfacing PROFIBUS and MPI:

   Ensure that the PLCs are correctly configured to communicate over both PROFIBUS and MPI networks. Configure any necessary routing between the two networks within the SCADA software.

5. ***Setting Up Tags and Communication Links Creating Tags:***

   Define tags for data points that will be monitored or controlled via the SCADA system. Assign these tags to the corresponding PLC variables. Linking Tags to Devices:

   Map the created tags to the PLCs on the PROFIBUS and MPI networks. Ensure correct data addressing and linkage. Testing Communication:

   Perform a communication test to verify that the SCADA software can successfully read from and write to the PLCs over both networks.

6. ***Configuring the HMI Designing HMI Screens:***

   Create HMI screens that display data from the PLCs. Add controls (buttons, switches) to allow interaction with the PLCs. Linking HMI to Tags:

Configure the HMI to display data from the tags created in the SCADA software. Set up alarms and notifications as needed.

7. ***Final Testing and Validation Full System Test:***

   Conduct a full system test to ensure all devices communicate correctly over PROFIBUS and MPI. Verify that data is accurately displayed on the HMI and that control actions work as expected. Troubleshooting:

   Identify and resolve any communication issues. Check cable connections, network configurations, and device settings.

8. ***Documentation and Reporting Document the Configuration:***

   Record the network configuration settings, device addresses, and communication parameters. Include screenshots and diagrams of the network setup.

Prepare a Lab Report: Summarize the steps taken, challenges faced, and how they were resolved. Include test results and observations. By following these detailed steps, students will gain practical experience in configuring and managing SCADA networks using PROFIBUS and MPI protocols, enhancing their understanding of industrial communication systems.

4.7 Project 01 : Parking barrier

4.7.1 Objective

The main objective of this project is to develop an automatic barrier that controls vehicle access to a secured area, utilizing GRAFCET to model and manage the various stages and transitions in the barrier's operational cycle and made the supervision system of this automatic barrier .

4.7.2 Functional Specifications

4.7.2.1 Vehicle Detection

A presence sensor must detect the arrival of a vehicle in front of the barrier. The sensor should be capable of detecting different types of vehicles (cars, motorcycles, trucks).

4.7.2.2 Opening and Closing Commands

The barrier should automatically open when a vehicle is detected. The barrier should automatically close after the vehicle has passed through. An adjustable delay should be integrated between vehicle detection and barrier opening.

4.7.2.3 Safety

The barrier should be equipped with safety sensors to prevent collisions with vehicles or pedestrians. The barrier should stop or remain open if an obstacle is detected during closing.

4.7.2.4 Manual Control

Manual control buttons should be installed for opening and closing the barrier in emergencies. Manual controls should have priority over automatic commands.

4.7.3 Technical Specifications

4.7.3.1 Sensors

Presence sensor for vehicle detection. Safety sensors to detect obstacles. Position sensor to determine the barrier's status (open/closed).

4.7.3.2 Actuators

Electric motor for opening and closing the barrier. Relays for motor control.

4.7.3.3 Control Units

A programmable logic controller (PLC) to manage sensor and actuator signals. Human-Machine Interface (HMI) for user interaction and system monitoring.

4.7.3.4 GRAFCET

Modeling the different stages of the barrier cycle (detection, opening, passage, closing). Transitions between stages based on sensor signals and manual commands.

4.7.4 Operational Cycle (GRAFCET Example)

4.7.4.1 Initial State

Barrier closed, sensors waiting for vehicle detection.

4.7.4.2 Vehicle Detection

Transition to the opening state when the presence sensor detects a vehicle. Opening the Barrier

Motor activation to open the barrier. Transition to the passage state when the barrier is fully open.

4.7.4.3 Vehicle Passage

Barrier remains open until the vehicle has completely passed. Transition to the closing state once the vehicle has passed.

4.7.4.4 Closing the Barrier

Motor activation to close the barrier. Transition to the initial state once the barrier is fully closed.

4.7.5 SCADA system design

In the final section, after testing the automatic barrier system in the PLCSIM environment, the student will design the SCADA system based on the knowledge gained

from previous lab work.

4.8 Conclusion

These detailed lab works provide a comprehensive, hands-on learning experience for students, ensuring they gain practical skills and a deep understanding of WinCC Flexible and its applications in industrial automation.

General Conclusion

SCADA (Supervisory Control and Data Acquisition) systems have become integral to modern industrial operations, providing a robust platform for monitoring, controlling, and optimizing various processes. The evolution of SCADA systems from simple telemetry systems to sophisticated, networked architectures has significantly enhanced their capabilities and applicability across diverse industries. This conclusion highlights the key aspects and the overall impact of SCADA systems.

1. Enhanced Operational Efficiency SCADA systems have revolutionized industrial operations by providing real-time monitoring and control capabilities. By continuously collecting data from various sensors and devices, SCADA systems enable operators to make informed decisions quickly. This real-time insight helps in optimizing production processes, reducing waste, and improving overall efficiency. Automated control features minimize the need for manual intervention, thereby streamlining operations and reducing human error.

2. Improved Decision-Making The comprehensive data analysis and visualization tools offered by SCADA systems are critical for effective decision-making. Operators can view detailed graphical representations of system performance, trends, and potential issues. This data-driven approach facilitates proactive maintenance, early detection of faults, and timely interventions, which are essential for maintaining high levels of productivity and safety. The ability to store historical data also aids in analyzing past performance and making strategic improvements.

3. Scalability and Flexibility Modern SCADA systems are designed to be highly scalable, accommodating the growing needs of industrial enterprises. They can be easily expanded by adding new sensors, controllers, and other components without significant

overhauls. This flexibility ensures that SCADA systems can adapt to changing business requirements and technological advancements. The integration with IoT (Internet of Things) further enhances this scalability, enabling seamless connectivity with a wide array of devices.

4. Enhanced Security Measures Given the critical nature of the processes controlled by SCADA systems, security has become a paramount concern. Advanced SCADA systems incorporate robust security measures to protect against cyber threats. These measures include encryption, authentication, and intrusion detection systems. Additionally, regular security audits and updates are essential to safeguard against evolving threats. The security of SCADA systems is vital to prevent disruptions that could have severe economic and safety implications.

5. Interoperability and Standardization The adoption of open standards in SCADA systems, such as DNP3, IEC 60870-5, and OPC, has greatly improved interoperability. This standardization allows different devices and systems to communicate seamlessly, regardless of the manufacturer. Interoperability is crucial for integrating various components within a SCADA system, enabling a cohesive and unified operational framework. This also simplifies maintenance and reduces costs associated with proprietary systems.

6. Cost-Effectiveness While the initial investment in SCADA systems can be substantial, the long-term benefits far outweigh the costs. By optimizing resource utilization, reducing downtime, and improving efficiency, SCADA systems contribute to significant cost savings. The ability to perform remote monitoring and control also reduces the need for on-site personnel, further lowering operational expenses. Additionally, the preventive maintenance facilitated by SCADA systems extends the lifespan of equipment, thereby reducing replacement costs.

7. Support for Regulatory Compliance SCADA systems play a crucial role in ensuring compliance with industry standards and regulations. They provide detailed records of operational data, which can be used to demonstrate adherence to safety, environmental, and quality standards. Automated reporting features simplify the process of regulatory compliance, reducing the administrative burden on organizations.

8. Future Prospects The future of SCADA systems is poised for further advance-

ments with the integration of artificial intelligence (AI) and machine learning (ML). These technologies can enhance predictive maintenance, optimize control strategies, and provide deeper insights into complex industrial processes. The ongoing development of edge computing will also contribute to faster data processing and reduced latency, further improving the efficiency of SCADA systems.

In conclusion, SCADA systems are indispensable for modern industrial operations. Their ability to provide real-time monitoring, enhance decision-making, ensure scalability, and improve security makes them a cornerstone of industrial automation. As technology continues to evolve, SCADA systems will undoubtedly incorporate more advanced features, driving further efficiency and innovation in the industrial sector. Organizations that invest in robust SCADA solutions are well-positioned to achieve higher productivity, better resource management, and sustained competitive advantage.

Bibliography

[1] Stuart A. Boyer. Scada: Supervisory Control And Data Acquisition. ISA Press, 2009.

[2] Stuart G. McCrady. Designing SCADA Application Software, A Practical Approach. Elsevier, 2013.

[3] Edwin Wright David Bailey. Practical SCADA for Industry. Elsevier, 2003.

[4] Jacob Brodsky Robert Radvanovsky. Handbook of SCADA/Control Systems Security. CRC Press, 2016.

[5] Mindsmapped. What is hmi? definition and introduction, n.d.

[6] PubNub. Human machine interface (hmi): What is hmi and how it works?, n.d.

[7] Human-machine interface, n.d.