Industrial Control Systems Technologies

Subjects: Computer Science, Artificial Intelligence

Contributor: Mary Nankya , Robin Chataut , Robert Akl

Industrial Control Systems (ICS), which include Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and Programmable Logic Controllers (PLC), play a crucial role in managing and regulating industrial processes. However, ensuring the security of these systems is of utmost importance due to the potentially severe consequences of cyber attacks.

industrial control systems SCADA DCS Industrial Automation and Control Systems (IACS)

1. Introduction

Industrial Control System (ICS) is an encompassing term that refers to various control systems and their associated instrumentation. It encompasses a diverse array of equipment, systems, networks, and mechanisms employed for the purpose of managing and automating industrial operations [1]. Virtually every commercial building and industrial facility, including those in production, transportation, power generation, and water treatment, relies on ICS devices and protocols. These systems heavily depend on the automation of mechanical and electrical processes. However, their connectivity to the internet poses a significant vulnerability, making them susceptible to cyber-attacks [2]. The global ICS market is experiencing substantial growth, primarily driven by the rising emphasis on automation, cloud computing, and digitization across various industries [3]. More innovative technologies are being developed, enabling remote access and control over the internet and within Information Technology environments. This shift towards increased automation and connectivity aims to achieve substantial business benefits. However, it also presents a challenge, as integrating Industrial Control Systems with external networks, such as the internet, expands the attack surface, making them more susceptible to cyber threats without proper security measures [4]. Over the past decade, cyber attacks on Industrial Control Systems have notably increased due to their heightened vulnerability to off-site attacks. Previously, these systems operated in isolated environments, relying heavily on human intervention. However, the growing inter-connectivity has exposed them to potential risks from remote adversaries. Consequently, ensuring robust security measures has become paramount to safeguarding ICSs from cyber threats [5].

An overview of an ICS contains several control loops, remote diagnostics, maintenance tools, and human interfaces built on layered network architectures using various network protocols. A summary of the basic components and process of an ICS is shown in **Figure 1**.

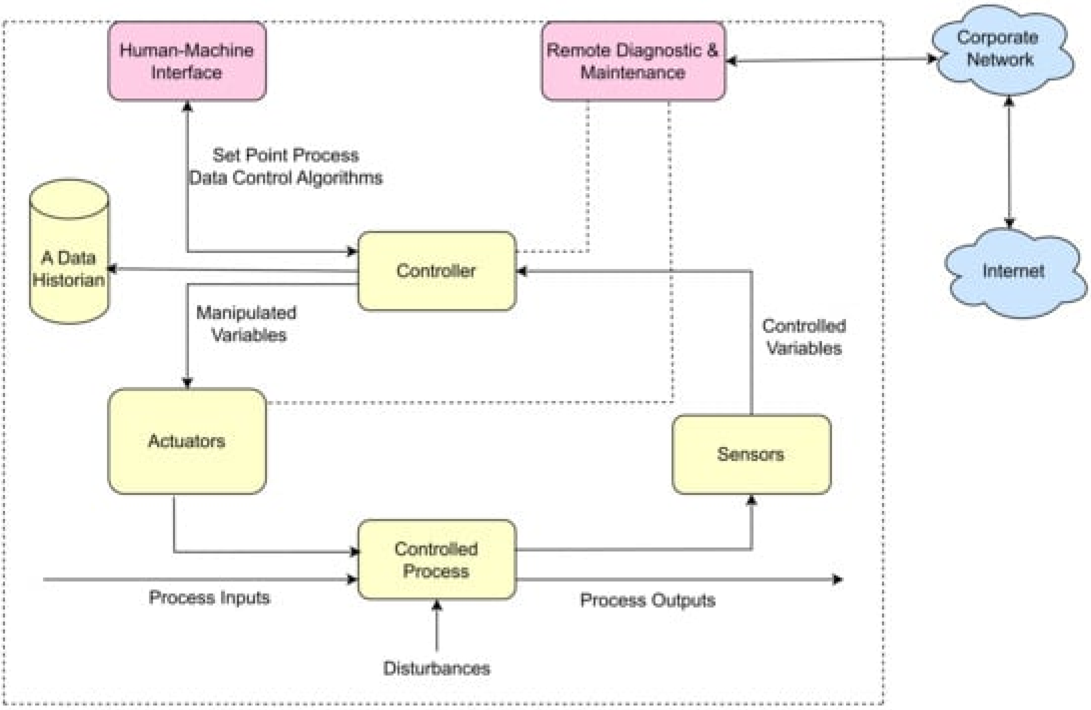

Figure 1. The basic components and operation of an Industrial Control System.

2. Industrial Control Systems Technologies

ICS has different technologies such as SCADA, DCS, Industrial Automation and Control Systems (IACS), PLCs, Programmable Automation Controllers (PACs), HMI, RTUs, control servers, Intelligent Electronic Devices (IEDs), and sensors [6]. The integration of these features contributes to the widespread adoption of Industrial Control Systems, leading to a market value of USD 130,060 million in 2022. The market is expected to experience a Compound Annual Growth Rate (CAGR) of 7.55% from 2023 to 2030, primarily driven by the increasing demand for energy-efficient and safe operations [7].

2.1. Supervisory Control and Data Acquisition

SCADA is among the most widely utilized technologies in Industrial Control Systems [8]. It functions as a software application designed to control industrial processes by collecting real-time data from remote locations, allowing for the management of equipment and conditions [9]. SCADA systems are composed of both hardware and software components. The hardware gathers and sends data to field controller systems, which subsequently transmit the data to other systems for real-time processing and display through a HMI. Additionally, SCADA systems maintain a comprehensive record of all events, enabling the reporting of process status and any encountered issues. These applications also include alarm functions that notify operators when hazardous conditions arise, ensuring prompt and appropriate responses [10]. SCADA provides organizations with the tools to make and deploy data-driven decisions regarding their industrial processes [11]. Applications of SCADA include the below [12]:

- Electricity generation, transmission, and distribution;

- Manufacturing industries or plants;
- Food and pharma productions
- Telecom and IT-based systems;
- Traffic control;
- Lift and elevator control;
- Oil and gas systems;
- Mass transit and railway traction.

SCADA employs a central computer to store information related to local and remote devices, enabling the control of industrial processes and facilities. The typical components of SCADA can be classified based on their respective definitions, as depicted in **Figure 2** below.

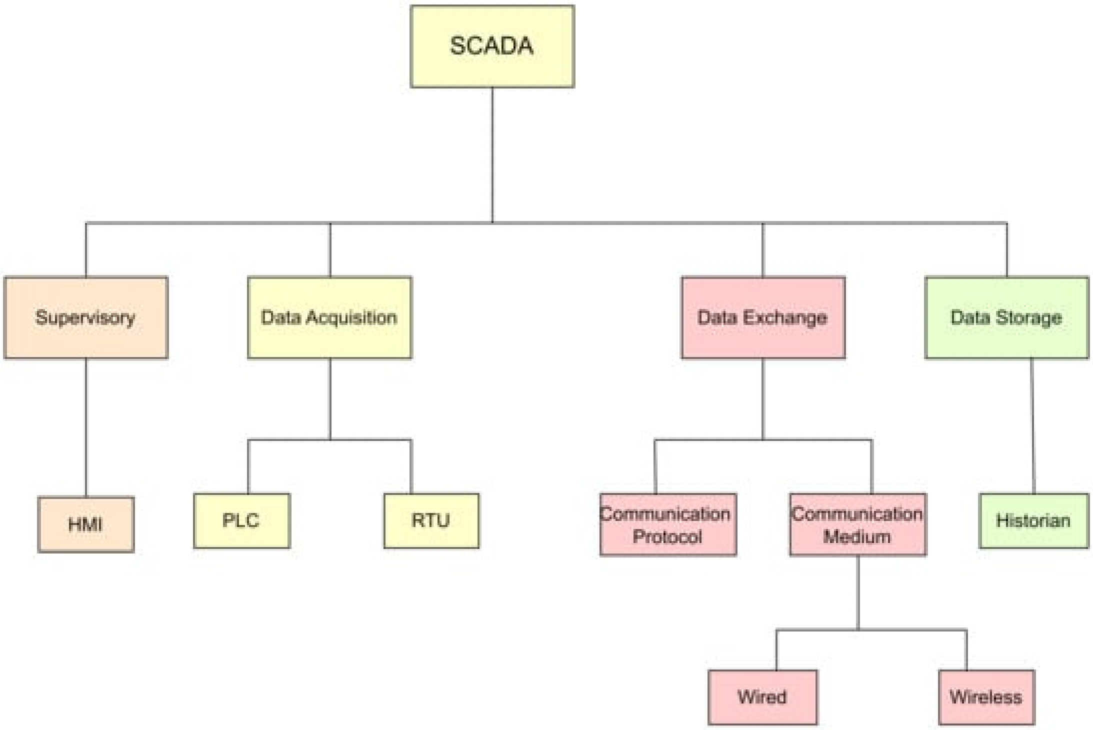

Figure 2. SCADA components.

- Supervisory control: Supervisory control serves as the fundamental role of the HMI. HMI software serves as an interface responsible for overseeing industrial processes. On the other hand, a master terminal unit (MTU) functions as a central supervisory controller that communicates with lower field devices, such as RTUs, through the ICS network;

- Data acquisition: Data can be acquired from two primary sources in the context of SCADA system as PLCs and Remote Telemetry Units (RTUs). Both the PLCs and RTUs interface directly with actuators and sensors in the field. RTUs are specifically designed to interface with sensors and collect telemetry data, which they then transmit to a primary system for further action. On the other hand, PLCs interface with the actuators to maintain and control industrial processes based on the telemetry data collected by the RTUs [13]. PLCs and RTUs act as physical interfaces between SCADA systems and field devices. However, their communication with the SCADA system differs. RTUs are well-suited for wide geographical areas due to their use of wireless communication methods. In contrast, PLCs are more tailored to local control applications [14];

- Data storage: The majority of SCADA systems employ a Structured Query Language (SQL) database for storing data with timestamps. A historian is a fully integrated SCADA software that collects real-time data from various SCADA devices and stores them in a database, such as mySQL;

- Data exchange: Communication protocols are used to exchange data between SCADA components.

SCADA Architecture

There are four generations of SCADA architecture in detail and summarizes the security strengths and vulnerabilities of each.

(a) First generation-Monolithic: The first generation of SCADA systems was developed when networks were not yet in existence. These early systems were not designed to connect with other systems, and communication was typically limited to Wide Area Networks (WANs) interacting with remote terminal units (RTUs) [15]. It defines application in remote areas within a factory where the conditions are unsafe, and physical access is restricted [16]. In the early-generation systems, redundancy was achieved by deploying two mainframe systems with identical configurations. One was designated as the primary and the other as the backup. These two systems were connected at the bus level. The standby system’s main role was to act as a monitoring entity for the primary system and would smoothly take over if it detected any indications of failure. Consequently, the standby system usually operated in an idle state, performing minimal to no processing tasks until a fail-over event became necessary [17]. **Figure 3** shows a typical first-generation SCADA architecture.

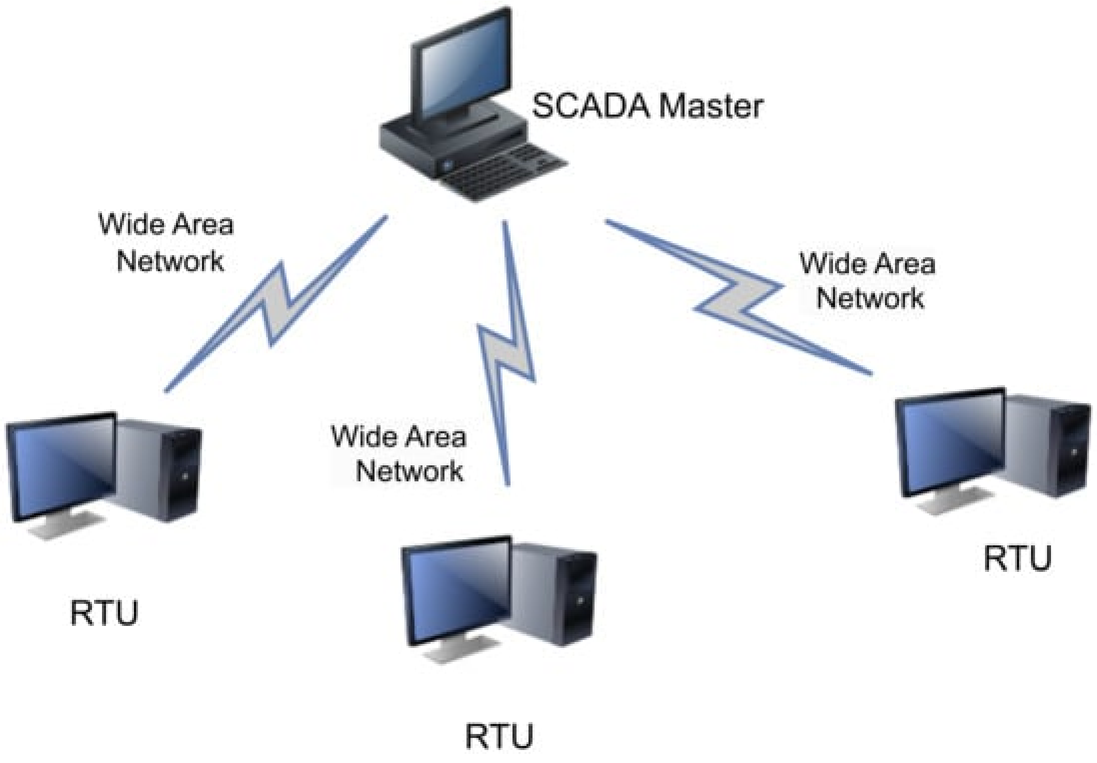

Figure 3. Monolithic SCADA system.

(b) Distributed SCADA system: Control functions were distributed across multiple systems during second generation [18]. Distributing the individual functions of the SCADA system across multiple systems resulted in a collective processing power that exceeded what could have been achieved with a single processor [19]. During the 1980s, SCADA systems harnessed the widespread adoption of proprietary local area networks(LAN) and more compact yet potent computers. This facilitated enhanced sharing of operational data not only within the plant but also at broader levels. These individual stations were used to share real-time information and command processing for performing control tasks to trip the alarm levels of possible problems. Only the developers cared about the SCADA security [20]. **Figure 4** below shows the Distributed SCADA architecture [21].

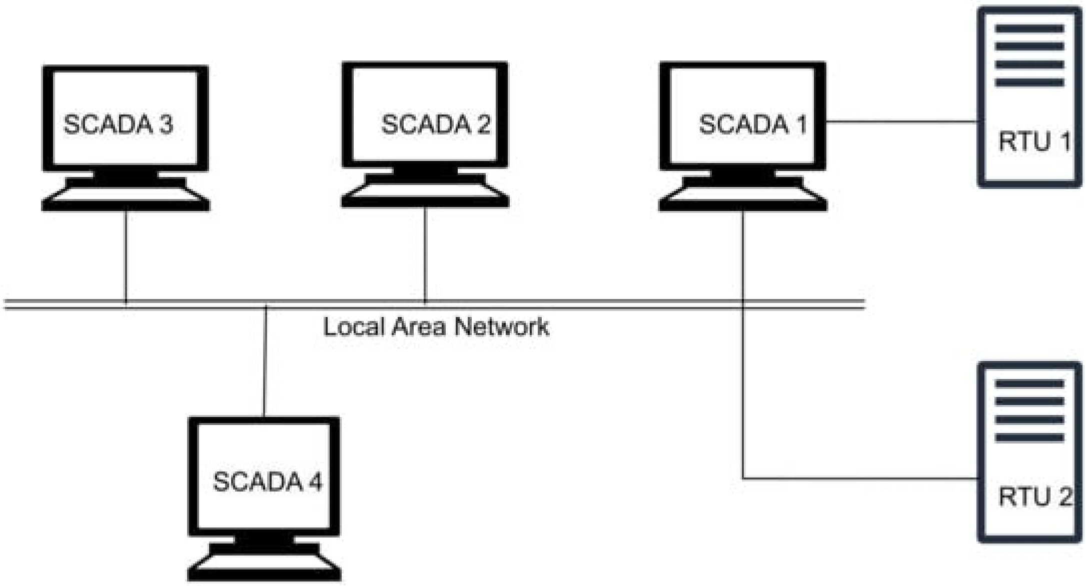

Figure 4. Distributed SCADA system.

(c) Internet of Things (IoT): IoT introduces a distinct approach to SCADA systems, substituting the requirement for PLCs with an emphasis on data modeling and advanced algorithms. This transition signifies a departure from the traditional reliance on mainframes or server in a facility, as data goes to cloud-based servers for sharing and storage [22]. IoT SCADA systems are flexible and easy to maintain and integrate. IoT brought several other advantages to SCADA, such as ease of use, flexibility, availability, cost efficiency, big data processing, and scalability [23]. **Figure 5** below shows the IoT SCADA architecture.

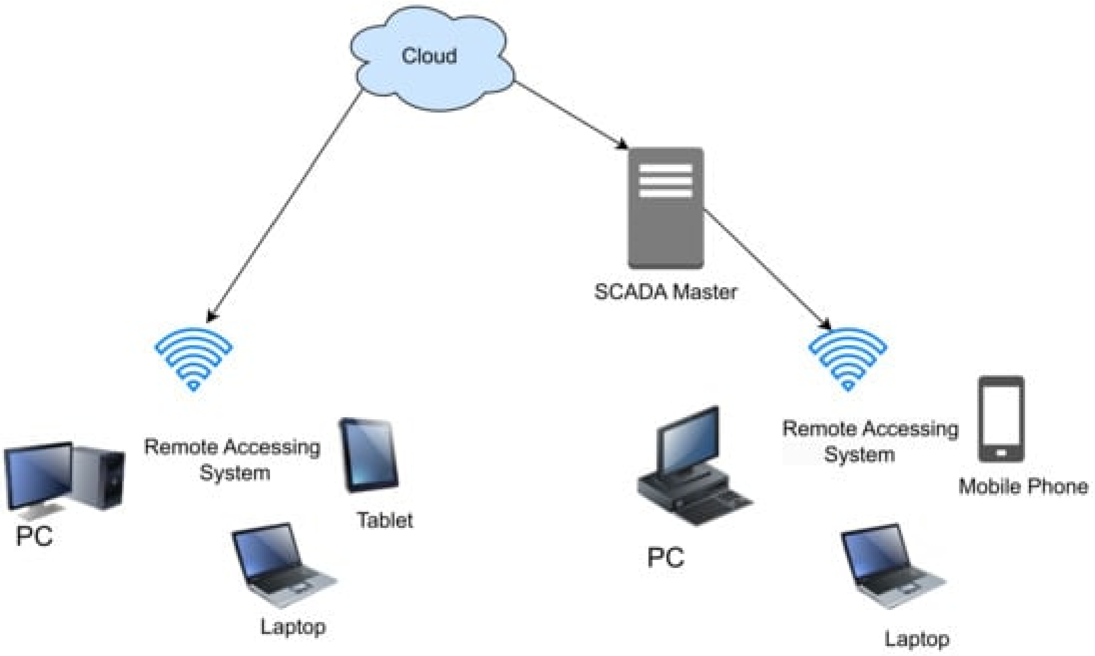

Figure 5. Internet of Things (IoT) SCADA system.

(d) Networked SCADA Architecture: During the third generation, the monitoring process heavily relied on the involvement of PLCs. They were integrated into the SCADA system, providing efficient and reliable data acquisition and control capabilities. This integration of PLCs enhanced the overall functionality and responsiveness of the SCADA system, enabling real-time monitoring and control of industrial processes across a distributed network. The third-generation SCADA architecture thus facilitated greater flexibility, scalability, and accessibility, making it more adaptable to modern industrial demands [24]. It can connect to the internet and third-party peripherals. Additionally, this architecture enhanced the performance level of SCADA by allowing several servers to run in parallel to handle several tasks [25]. **Figure 6** below shows the description of the Networked SCADA architecture.

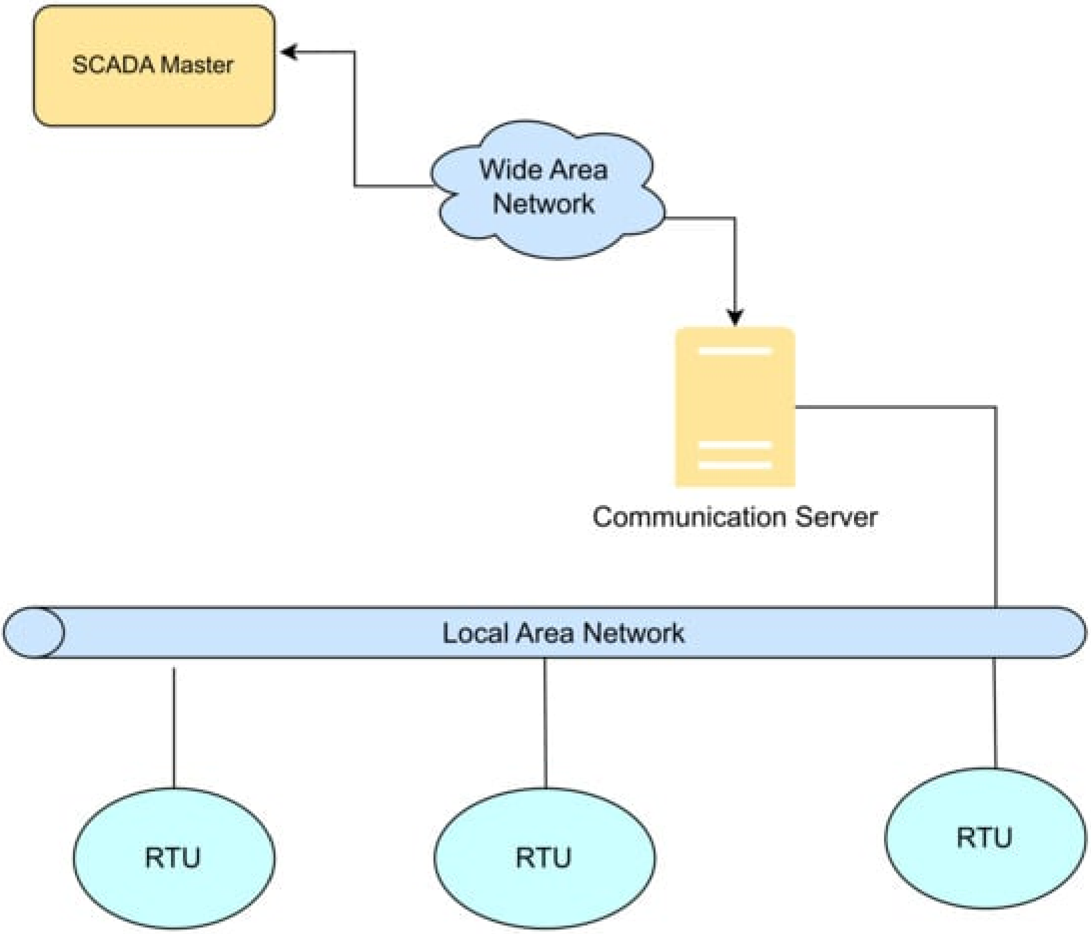

Figure 6. Networked SCADA architecture.

2.2. Distributed Control Systems (DCS)

Distributed Control Systems are comprised of controllers, sensors, and actuators that are distributed across different spatial locations [26]. The entire system's sub-components are controlled by multiple controllers, e.g., PLC [27]. DCS is frequently employed in various industrial process industries, including but not limited to the following:

- Agriculture;
- Chemical plants;
- Petrochemical and refineries;
- Nuclear power plants;
- Water and sewage treatment plants;
- Food processing;

- Automobile manufacturing;
- Pharmaceutical manufacturing.

Within the domain of DCS, automatic control revolves around the exchange of signals, facilitating bidirectional information flow, and the computation of control actions through decision-making processes [28]. DCS is also defined as an architecture where the subsystems are geographically distributed and functionally integrated [29]. DCS coordinates and supervises a complete plant of many variable processes. See below a distributed control system in **Figure 7**.

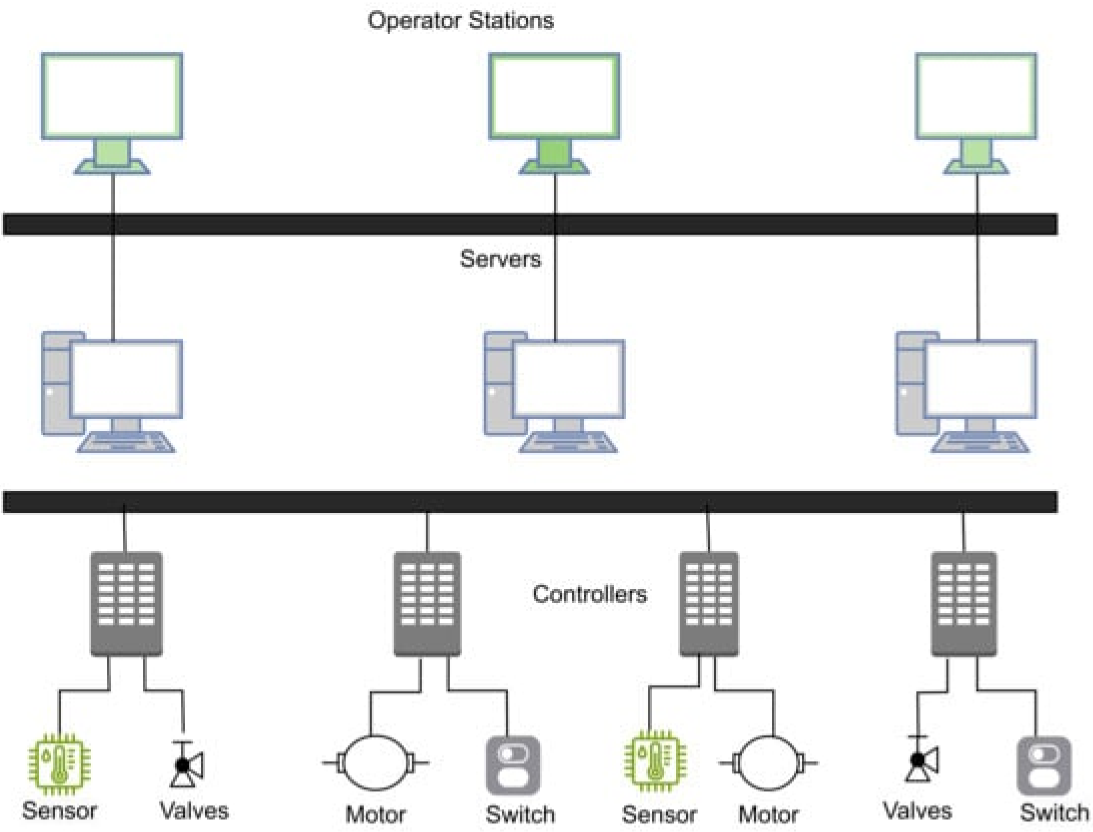

Figure 7. A distributed control system.

2.1.2. Function and Components of DCS

Components of DCS consist of the basic components, as listed below:

- An engineering workstation: This is the supervisory controller for the DCS as a whole. The station comes with configuration tools that empower users to undertake activities such as generating new loops, establishing input/output (I/O) points, and configuring distributed devices [30];
- An operator station: A station operator is a location where the user observes the ongoing process. At the station operator's interface, the operator can access process variables, control parameters, and alarms, which are essential for retrieving the current operating status [31];

- A process control unit: This control center acts as the brain of all process control by performing all the computation process algorithms and running all logical expressions. The control module takes an input variable that will be controlled, calculates it, and the results are compared with the set point, which is the value expected of the process. If the calculation results differ from the set point, the value must be manipulated and the results sent to the actuator [31]. This controller, which relies on microprocessor technology, is specifically engineered for automatic and compound loop control;

- A communication system: This system facilitates the transfer of data from one station to another, a crucial function in distributed control systems. The network protocols employed encompass Ethernet, Profibus, and DeviceNet;

- Smart devices: These refer to intelligent devices or bus technologies employed to substitute older I/O systems.

2.3. Programmable Logic Controllers

PLCs are industrial computer control systems designed to constantly monitor the status of input devices and make decisions according to a customized program in order to manage the status of output devices [32]. Early PLCs were able to execute tens of instructions per second; modern PLCs can perform bit operations in nanoseconds. They can function as autonomous systems, optimizing processes intelligently and independently [33]. PLCs rely on a programmable memory that stores instructions for executing a wide range of operations, encompassing logic functions, sequence control, timing, counting, and arithmetic calculations. Using digital or analog input and output interfaces, this memory supervises and manages a variety of mechanical equipment and production processes [34]. Industries that rely on PLCs include the following:

- Oil and Gas;

- Food and Beverage;

- Automotive;

- Pharmaceuticals;

- Transportation;

- Off Road Construction;

- Lifts and escalators;

- Medical applications;

- Automatic gate systems;

- Heating control systems.

2.3.1. Versions of PLCs

PLCs have evolved significantly, with a version incorporating Ethernet protocol based network connectivity that enables them to share data with a variety of devices and systems such as other PCs, SCADA, and even cloud-based platforms [35]. This enhanced connectivity and data sharing capability has further signified their pivotal role in ICS, as seen below.

- Real-Time Monitoring and Control: PLCs facilitate real-time monitoring and control of industrial processes. With their network connectivity, they can provide immediate data feedback, allowing for rapid decision-making and adjustments;

- Data Aggregation and Analysis: PLCs can collect and transmit data to centralized systems for analysis. This data is essential for process optimization, predictive maintenance, and quality control;

- Remote Accessibility: Connectivity enables remote accessibility to PLCs, allowing engineers and operators to manage and monitor processes from different locations, improving operational efficiency and reducing the need for onsite presence.

This version of the Ethernet protocol-based PLCs has several limitations despite its data sharing capability. These PLCs lacked standardization, leading to compatibility issues between devices from different manufacturers. They also present with data handling, processing, and storage limitations for more advanced applications. PLCs have become an integral part of the broader industrial landscape, especially within the frameworks of Industry 4.0 and the Industrial Internet of Things (IoT). A team of researchers proposed an IoT-PLC version that possesses regulatory control features, incorporates fog computing capabilities for tasks such as data filtering, field data storage, and supports various wireless interfaces that can be managed autonomously [36]. Their incorporation into these paradigms is of utmost importance and have solved the earlier mentioned limitations with the below capabilities, hence resulting into robust and secure solutions for modern industrial automation, as seen below [37].

- Enhanced Automation and Smart Manufacturing: PLCs contribute to the automation and intelligent control of industrial processes, aligning perfectly with the objectives of Industry 4.0 and industrial IoT, which aim to create smart and interconnected factories;

- Optimizing Resource Utilization: PLCs, as part of ICS, contribute to optimizing resource utilization, reducing energy consumption, and minimizing waste, which are central to sustainable and eco-friendly manufacturing practices;

- Data-Driven Decision Making: In Industry 4.0 and industrial IoT, data is a valuable asset. PLCs’ connectivity enables them to generate and share data, which is the foundation for data-driven decision-making, predictive maintenance, and process optimization.

2.3.2. Components of PLC system

Figure 8 below shows the components of a PLC system.

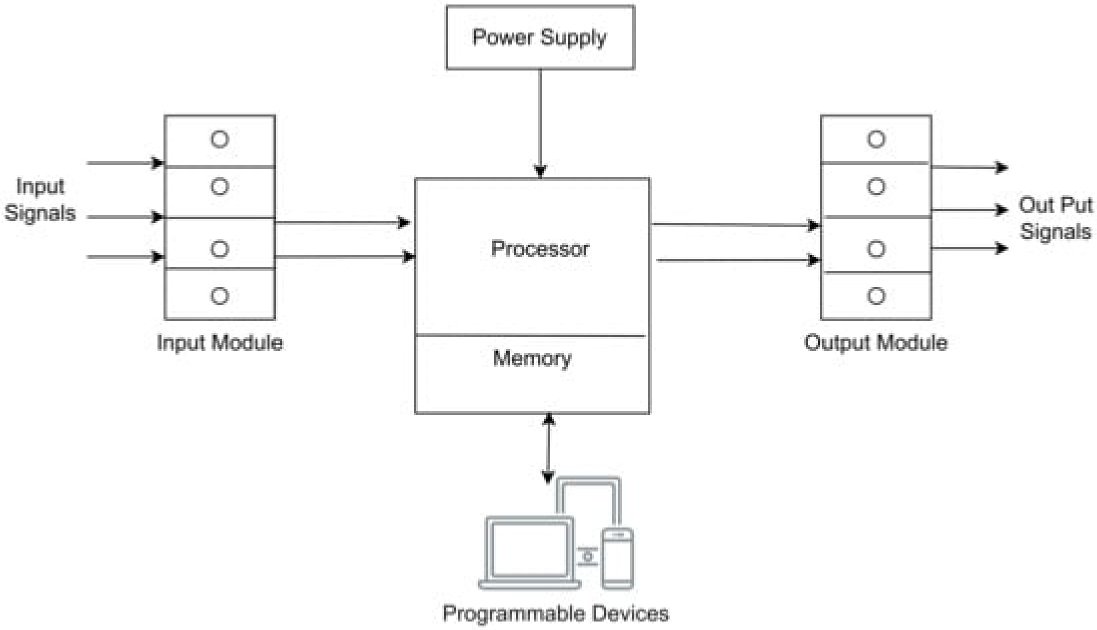

Figure 8. Components of a PLC system.

- Power Supply Unit: The power requirements are contingent upon the particular type of PLC employed in the application. This unit converts AC to DC voltage suitable for PLC. This unit comprises short-circuit protection switches at all levels, control transformers, switching power supply, and other components [38];

- Processor or CPU: This component includes a microprocessor, system memory, serial communication ports, and a LAN connection. A power supply may also be included in specific cases to deliver the necessary power to the CPU;

- Input/Out modules: Input and output modules serve as the connection points between the control environment's field devices (comprising both input and output equipment) and the processor. The input devices encompass sensors, push buttons, limit switches, and similar items, while the output devices consist of motors, relays, solenoid valves, and the like. I/O devices can be broadly categorized into two groups: discrete or digital modules and analog modules;

- Programmable devices: As seen in **Figure 8** above, Programming tools are utilized to load the specific program into the CPU's memory.

References

1. Industrial Control System. Definition. Available online: https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system (accessed on 24 May 2023).
2. Industrial Control System (ICS): Functional Components and Uses. 10 June 2019. Available online: https://study.com/academy/lesson/industrial-control-system-ics-functional-components-uses.html (accessed on 25 May 2023).
3. Santhi, A.R.; Muthuswamy, P. Industry 5.0 or industry 4.0S? Introduction to industry 4.0 and a peek into the prospective industry 5.0 technologies. Int. J. Interact. Des. Manuf. 2023, 17, 947–979.
4. Tariq, U.; Ahmed, I.; Bashir, A.K.; Shaukat, K. A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors 2023, 23, 4117.
5. 2022 the State of Operational Technology and Cybersecurity. Global Leader of Cybersecurity Solutions and Services. Available online: https://www.fortinet.com/resources-campaign/secure-ot/2022-the-state-of-operational-technology-and-cybersecurity (accessed on 27 May 2023).
6. Types of Industrial Control Systems. Available online: https://www.thomasnet.com/articles/instruments-controls/types-of-industrial-control-systems/ (accessed on 24 May 2023).
7. Industrial Control Systems (ICS) Market Size by 2030. Available online: https://www.coherentmarketinsights.com/market-insight/industrial-control-systems-ics-market-5587 (accessed on 24 May 2023).
8. Sverko, M.; Grbac, T.G.; Mikuc, M. SCADA Systems With Focus on Continuous Manufacturing and Steel Industry: A Survey on Architectures, Standards, Challenges and Industry 5.0. IEEE Access 2022, 10, 109395–109430.
9. Agarwal, T. SCADA System: Architecture, Components, Types and Its Applications. ElProCus. 7 January 2021. Available online: https://www.elprocus.com/scada-system-architecture-its-working/ (accessed on 29 May 2023).
10. Loshin, P. What Is SCADA (Supervisory Control and Data Acquisition)? WhatIs.com. 16 December 2021. Available online: https://www.techtarget.com/whatis/definition/SCADA-supervisory-control-and-data-acquisition (accessed on 29 May 2023).
11. Abusaq, M.J.; Zohdy, M.A. Analyzing the Impact of Security Characteristics on Industrial Control Systems. In Proceedings of the 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 25–26 March 2022; pp. 635–641.
12. S.M. SCADA Application in Manufacturing Industries and Power Generation. Instrumentation and Control Engineering. 11 March 2023. Available online: https://automationforum.co/applications-of-

scada/ (accessed on 3 June 2023).

13. Pathak, A. An introduction to supervisory control and Data Acquisition (SCADA) for Beginners. Geekflare. 16 January 2023. Available online: https://geekflare.com/scada-for-beginners/ (accessed on 29 May 2023).
14. Alanazi, M.; Mahmood, A.; Chowdhury, M.J.M. SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. Comput. Secur. 2023, 125, 103028.
15. Jeffries, M. Industrial Control Systems: The Four Generations of SCADA Architectures. Available online: https://www.maderelectricinc.com/blog/industrial-control-systems-the-four-genertions-of-scada-architectures (accessed on 29 May 2023).
16. Nagda, V.; Ojha, C.; Attada, S. Types of SCADA System Architecture. Instrumentation Tools. 18 April 2023. Available online: https://instrumentationtools.com/scada-system-architecture/ (accessed on 29 May 2023).
17. SCADA Architectures: Monolithic System. SCADA ARCHITECTURES: MONOLITHIC SYSTEM. Available online: https://powersystemsloss.blogspot.com/2012/01/scada-architectures-monolithic-system.html (accessed on 29 May 2023).
18. Admin. SCADA System Architecture, Types and Applications. WatElectronics.com. 9 May 2022. Available online: https://www.watelectronics.com/scada-system-architecture-types-applications/ (accessed on 29 May 2023).
19. Yadav, G.; Paul, K. Architecture and Security of SCADA Systems: A Review. Int. J. Crit. Infrastruct. Prot. 2021, 34, 100433.
20. Zhu, B.; Joseph, A.; Sastry, S. A Taxonomy of Cyber Attacks on SCADA Systems. In Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference, Dalian, China, 19–22 October 2011.
21. Björkman, G.; Sommestad, T.; Ekstedt, M.; Hadeli, H.; Liu, K.; Chenine, M. SCADA System Architectures. 2010. Available online: https://api.semanticscholar.org/CorpusID:109456860 (accessed on 29 May 2023).
22. Balsom, P. Understanding a Monolithic SCADA System. High Tide. 19 January 2023. Available online: https://htt.io/understanding-a-monolithic-scada-system/ (accessed on 29 May 2023).
23. Sajid, A.; Abbas, H.; Saleem, K. Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges. IEEE Access 2016, 4, 1375–1384.
24. Bindhumadhava, B.S.; Kumar, R.S.; Kalluri, R.; Pidikiti, D.S. SCADA Communication Protocols: Vulnerabilities, Attacks and Possible Mitigations. Csi Trans. Ict 2013, 1, 135–141.
25. Pliatsios, D.; Sarigiannidis, P.; Lagkas, T.; Sarigiannidis, A.G. A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics. IEEE Commun. Surv. Tutorials 2020, 22, 1942–

1976.

26. Sivaranjith. Function and Components of DCS. Instrumentation and Control Engineering. Available online: https://automationforum.co/function-and-components-of-dcs/ (accessed on 3 June 2023).
27. Vogel-Heuser, B.; Feldmann, S.; Werner, T.; Diedrich, C. Modeling network architecture and time behavior of Distributed Control Systems in industrial plant automation. In Proceedings of the IECON 2011—37th Annual Conference of the IEEE Industrial Electronics Society, Melbourne, VIC, Australia, 7–10 November 2011; pp. 2232–2237.
28. Distributed Control System. Available online: http://kazanets.narod.ru/files/DCS.pdf (accessed on 3 June 2023).
29. Scribd. What Is Distributed Control System (DCS)—DCS (Distributed Control Systems)—Industrial Automation, PLC Programming, SCADA and PID Control System PDF. Scribd. Available online: https://www.scribd.com/ (accessed on 3 June 2023).
30. Gillis, A.S. What Is a DCS? I Definition from TechTarget. WhatIs.com. 27 January 2023. Available online: https://www.techtarget.com/whatis/definition/distributed-control-system (accessed on 6 June 2023).
31. Hexa. What Is a DCS System and What Is It for? HEXA Ingenieros. 18 September 2020. Available online: https://hexaingenieros.com/what-is-a-dcs-system-and-what-is-it-for/?lang=en (accessed on 3 June 2023).
32. Sehr, M.A.; Lohstroh, M.; Weber, M.; Ugalde, I.; Witte, M.; Neidig, J.; Hoeme, S.; Niknami, M.; Lee, E.A. Programmable Logic Controllers in the Context of Industry 4.0. IEEE Trans. Ind. Inform. 2020, 17, 3523–3533.
33. PLCs Programmable Logic Controllers—A Complete Guide. Available online: https://uk.rs-online.com/web/content/discovery/ideas-and-advice/plcs-programmable-logic-controllers-guide (accessed on 7 June 2023).
34. Programmable Logic Controller|MachineMfg. MachineMfg. Available online: https://www.machinemfg.com/programmable-logic-controller/ (accessed on 7 June 2023).
35. Hajda, J.; Jakuszewski, R.; Ogonowski, S. Security challenges in Industry 4.0 PLC Systems. Appl. Sci. 2021, 11, 9785.
36. Mellado, J.; Núñez, F. Design of an IoT-PLC: A containerized programmable logical controller for the industry 4.0. J. Ind. Inf. Integr. 2021, 25, 100250.
37. Folgado, F.J.; González, I.; Calderón, A.J. Data acquisition and monitoring system framed in Industrial Internet of Things for PEM hydrogen generators. Internet Things 2023, 22, 100795.

38. Yu, F.A.Y.; Fu, S.B.H.; Qiu, T.C.T.; Wang, F.D.Z. Control System Design of Spacecraft Mechanical Ground Support Equipment Automatic Storage System. In Proceedings of the 2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), Tianjin, China, 19–23 July 2018; pp. 977–981.

Retrieved from https://encyclopedia.pub/entry/history/show/117087