Bulletin of the *Transilvania* University of Braşov • Vol. 9 (58) No. 1 - 2016
Series I: Engineering Sciences

EVOLUTION OF SCADA SYSTEMS

Alexandru UJVAROSI[1]

Abstract: *The concept of SCADA is very often used in industrial world, as it is widely used in almost every field of industry and not only: manufacturing, electric power generation, transmission and distribution, building and facilities, traffic signals etc. But behind this concept, there is a history of over 50 years of development: from the first idea of supervisor control of systems to the most complex data acquisition and supervisory control systems nowadays. This paper presents the evolution, the architecture and the main components of a SCADA system.*

Key words: *supervisory control, data acquisition, process control.*

1. Introduction

The abbreviation of "SCADA" comes from Supervisory Control and Data Acquisition. Even if it sounds very familiar to the public, it is hard to locate a precise moment in the history when this term was first used. Most of the authors refer to the 1960s as the SCADA system beginnings. At that time, the need to monitor and control various processes grew, which led the engineers to search for solutions to fulfil these needs.

SCADA systems are generally used to monitor and control equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation - mainly, systems that are geographically wide spread [9].

There are some similarities between the SCADA concept and Industrial Control Systems, but generally both nomenclatures are accepted. ICS refers mainly to industrial automation and industrial processes [2]. Furthermore, the Data Acquisition as part of a SCADA system is the main difference between these two.

The evolution of SCADA systems can subject of two distinct approaches:

- by technologic evolution;
- by market evolution.

2. SCADA Systems by Technologic Evolution

For a better understanding of this approach, let's consider an example of a water pumping system in a city containing one central facility and several pumping stations, which are equipped with field devices (sensors, switches, valve actuators etc.).

Before the discovery of the transistor, there were no computers, thus the control of such a system was made by human force - several men were travelling to each station to control the system and check the state of the local system. Another solution was to permanently have men in each station manually operating and communicating data by telephone wires.

[1] Dept. "Electronic Systems and Integrated Communications", *Transilvania* University of Braşov.

2.1. Telemetry-based SCADA

The telephone wires were the key to development of the first SCADA system by the end of 1950s. The evolution of telemetry, telephone relay systems and coding schemes allows Westinghouse and North Electric Company to develop a supervisory control system called Visicode [5], which can be considered the beginning of the SCADA systems.

In the 1960s, several supervisory control systems based on telephone wires were developed, but the next true step in SCADA systems evolution was the development of solid state devices.

2.2. Minicomputers

The minicomputers, which used 8 bit or 16 bit processors, were able to perform the functions that were previously done by operators from the control panels installed in each station [5]. That was the moment when the engineers realized that computers are very useful in such said systems. The continuous development of this technology allowed the system to offer functions like data scanning, status monitoring, alarming and even data display [5].

2.3. Microprocessors

In the late 1960s, the development of transistors led to the appearance of microprocessors, and furthermore, the one of PLCs - the world's first PLC, manufactured by Bedford Associates, known as 084 or Modicon (Modular Digital Controller) [6].

This allowed SCADA systems vendors to develop various other functions, more cost-effective and more efficient.

Additionally, the Discrete Control Systems (DSC) were developed since then and were used to build supervisory control systems.

The continuous increase of processors speed and memory size allowed the SCADA systems to be real-time, more efficient and more reliable [5].

3. SCADA Systems by Market Evolution

Vendors quickly recognize the advantages of a SCADA system, so they started to build applications of process control and sold them to specific industries as turn-key solutions.

The technologic evolution and the need of more intelligent and security-safe systems led the vendors to develop new architectures of SCADA systems. This evolution of the system architecture and functions offered can be separated in three major "generations" of the system: Monolithic SCADA, Distributed SCADA and Networked SCADA [9].

Recently, some authors identified a new "generation" which is evolving nowadays - Internet of Things SCADA. This concept is based on the recently developed idea of cloud computing [7].

3.1. Monolithic SCADA

The first architecture concept of SCADA was based on the mainframe systems, in which networks are basically not existent. Therefore, first control systems were not able to interconnect with any other, so they were standalone systems.

Even if the term of Wide Area Network (WAN) was used, the only purpose of this "network" was to connect to different Remote Terminal Units (RTU) and interchange data with the master computer. Also, at that time, the protocols that we use today for WAN were not available.

However, the communication protocols available were developed by various RTU vendors and they were usable only with proprietary master computers from the same vendor. Even so, the protocols were

only able to permit scanning, control and data interchange between the master computer and the remote terminal's field sensors or actuators, Figure 1 [9].

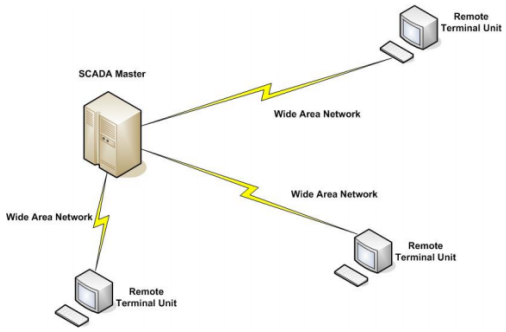

Fig. 1. *Example of Monolithic SCADA architecture*

The interconnectivity between different RTUs to a master computer was practically impossible, but the need of the industries forced the vendors to improve this disadvantage of SCADA systems. This is how these systems evolved to the second generation.

3.2. Distributed SCADA

The development and improvements in system miniaturization and the Local Area Network (LAN) technology [9] were the key factors that led to the distributed SCADA.

Multiple stations with various functions were able to communicate real-time with each other and interchange data between them. All of these new developed stations were acting like mini-computers and they were smaller and less expensive than the first generation equipments [9].

Starting with the second generation we can identify the appearance of actual SCADA common system components. The distributed stations described above were used as communication processors, human-machine interfaces, RTUs, calculation processors or database servers [9].

The LAN used in these kind of SCADA system was based on proprietary protocols developed by vendors. This offered the possibility of increasing communication speed, system reliability and real-time traffic optimization.

But again, all the devices connected to the SCADA LAN were not able to communicate with other external devices using other existing protocols. Therefore, the systems were distributed, capable to communicate with each other, but only with proprietary protocols supplied by vendors, Figure 2 [9].

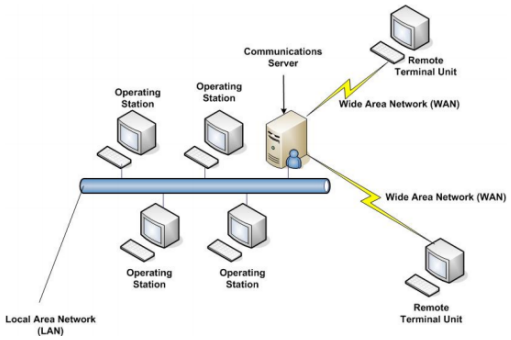

Fig. 2. *Example of Distributed SCADA architecture*

Even if the systems were more reliable due to distributed functionality, they were limited to hardware, software and peripheral devices provided by the vendor [9].

3.3. Networked SCADA

Continuous growth of all industries, the increased number of automated processes and the multiple vendors of industrial equipment caused the next step in SCADA evolution - networked systems.

The third generation of SCADA systems is very similar with the second one, except one primary difference: it is oriented to an open system architecture, rather than a vendor controlled and proprietary environment [9].

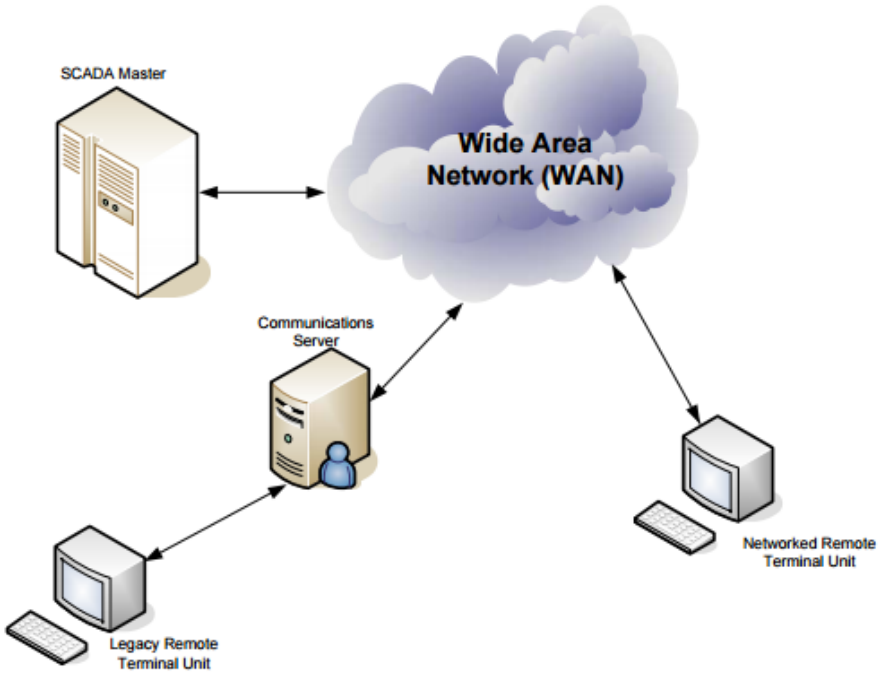

Fig. 3. *Example of Networked SCADA*

In this kind of system, the communication is based on open protocols, which allow SCADA functionality to be distributed in WANs, not only in closed LANs. Also, using open standards and protocols eliminated the SCADA limitations. Since then, SCADA systems were able to use more functions provided by third-party peripherals, like monitors, printers etc. [3].

This evolution forced the SCADA vendors to look for system vendors, which could develop new functions for SCADA master station, by building new basic computer platforms or operating system software [9].

One key factor that helped the fast development of the third generation of SCADA systems was the use of WAN protocols, such as Internet Protocol (IP), for communication between master station and peripherals. Basically, all the components of a SCADA could communicate with each other through Ethernet connection, Figure 3 [9].

The third generation of SCADA systems was possible due to vendors effort to understand and comply the market needs. The foundation stone of this system architecture was the development of a series of standards and specifications for industrial telecommunication.

In 1996, an industrial automation industry task force developed a standard called Object Linking and Embedding for Process Control (OLE for Process Control). In the same year, the OPC Foundation was created to maintain the standards [8].

This series of standards were a huge step in order to make SCADA systems development much easier and time effective.

3.4. OPC Foundation

The purpose of the OPC Foundation was to abstract PLC specific protocols, (such as Modbus, Profibus etc.) into a standardized interface allowing HMI/SCADA systems

to interface with all the devices from multiple vendors, using the open standards and protocols.

At the beginnings, the standards were restricted to the Windows operating system - this is why the first nomenclature of the standards was OLE for Process Control. The standards evolution led to the abbreviation of OPC - Open Platform Communications.

The OPC was developed by industry vendors, end-users and software developers [8].

4. SCADA System Common Components

After over 50 years of evolution, SCADA systems architecture crystallized in a solid structure containing several stations (devices), each of them fulfilling certain functions. Some systems may add complementary functions, but the basic SCADA system contains the following components: RTU, PLC, Telemetry System, Data Acquisition Server, Human Machine Interface (HMI), Historian Service and Supervisory Station (Central Computer).

4.1. RTU

The main function of a RTU is to collect data from field sensors and convert it to digital data, which is then sent to the supervisory system via a telemetry system. Also, a RTU should be able to receive commands from the supervisory system.

Optionally, a RTU can contain basic microcontrollers able to perform simple boolean logic instructions [3].

4.2. PLC

It is very similar with a RTU, but the control functions are more sophisticated, so it can locally control a process and execute simple and complex logic operations. The same as an RTU, a PLC gathers information from sensors and actuators and is capable to interchange data with supervisory control.

It is possible to connect a HMI module directly to local PLC - therefore, a station controlled by a PLC can be controlled locally, if the supervisory system agrees.

4.3. Telemetry System

This refers to the communication protocols and physically channel between stations and between stations and supervisory control. As it has been described above, the communication channel can be telephone wires, WAN circuits or even wireless systems as satellite (VSAT), radio, cellular or microwave [4].

4.4. Data Acquisition Server

This is an important component of a SCADA system. Based on Client-Server architecture and industrial protocols, it allows clients to access data located in RTUs or PLCs.

4.5. HMI

The Human Machine Interface is the device that presents the data gathered from RTUs and PLCs to a human operator, allowing the operator to interact with the process.

HMI is the Graphical User Interface (GUI) of the SCADA system - it collects data from DA Servers and process it into reports, graphics, trends, alarms, notifications etc.

4.6. Historian Service

This part of a SCADA system can accumulate and save into databases time-stamped data, Boolean events, alarms or any other kind of information collected from the system. Storing information in databases allows clients to perform queries

and get statistical data, graphic trends, which can be displayed even on the HMI devices connected to the system [1].

4.7. Supervisory Control

This is the main part of a SCADA system and is generally a computer that contains specific software which can control all the other devices connected, running algorithms, sending commands to the other devices etc. - basically, this is the SCADA headquarters.

5. SCADA Applications

The need of control the automation processes in the industry field is certain, and so is the use of SCADA for geographically wide spread systems. The advantages are obviously: real-time observation and control of the system, time-effective maintenance, cost effective solution.

Actual SCADA systems are more and more reliable, having numerous security functions (redundancy, functionality distribution), that can practically make the system failure-safe.

References

1. Aquino-Santos, R.: *Emerging Technologies in Wireless Ad-hoc Networks: Applications and Future Development: Applications and Future Development.* IGI Global, 2010, p. 43.
2. Byres, E.: *SCADA Security Basics: SCADA vs. ICS Terminology*. Available at: https://www.tofinosecurity.com/blog/scada-security-basics-scada-vs-ics-terminology. Accessed: 21.04. 2016.
3. Hieb, J.: *Security Hardened Remote Terminal Units for SCADA Networks*. University of Louisville, 2008.
4. Liptak, B.: *Instrument Engineers' Handbook, Fourth Edition. Vol. Two: Process Control and Optimization.* CRC Press, 2005.
5. Russel, J.: *A Brief History of SCADA/ EMS.* Available at: http://www.Scada history.com/. Accessed: 21.04.2016.
6. http://makox.com/plc-scada/1-introduction-of-plc-scada/history-of-plc-scada/. Accessed: 21.04.2016.
7. http://www.fastcompany.com/biomimicry/how-the-internet-of-things-is-turning-cities-into-organisms/. Accessed: 21.04.2016.
8. https://opcfoundation.org/. Accessed: 21.04.2016.
9. *** Office of the Manager NCS: *Supervisory Control and Data Acquisition (SCADA) Systems.* Communication Technologies Inc., 2004.