INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 3, Issue 6)
Available online at www.ijariit.com

Comparative Analysis of Traditional SCADA Systems and IOT Implemented SCADA

Ram Dhobley
Vishwakarma Institute of Technology, Pune, Maharashtra
ramdhobley25@gmail.com

Abhay Chopde
Vishwakarma Institute of Technology, Pune, Maharashtra
abhay.chopade@vit.edu

Abstract: SCADA system stands as an abbreviation of Supervisory Control and Data Acquisition. It focuses on the supervisory level and is not a full control system. It is a computer system which gathers and analyses real time data. They are useful in monitoring and controlling a plant or industrial equipment like telecommunications, water, waste control, energy, oil-gas refining, and transportation. It gathers information about a mishap, transfers it back to a central site and alerts the home station about the mishap, carries out necessary analysis and control, like determining if the mishap occurred is critical, and display the information in a logical and organized fashion. They can be relatively as simple as a system which monitors environmental conditions of a small office building, or as complex as a system that monitors all the activity in a nuclear power plant.

IOT acts as a complementary setup to SCADA. SCADA system generates information which acts as one of the data sources for IOT. While the focus of SCADA on monitoring and control, the focus of IOT is firmly on analyzing machine data to improve productivity.

Keywords: Architecture, Communication, Vulnerabilities.

I. INTRODUCTION

SCADA systems are used to control dispersed. The integration of data acquisition systems with data transmission systems and HMI software is done by the SCADA to provide a centralized monitoring and control system for multiple process inputs and outputs. SCADA systems are designed to collect field information, transfer it to a central computer facility (via different communication protocols), and display the information to the operator graphically or textually (via Human Machine Interface), and thus allow an operator to monitor or control an entire system from a central location in real time. Based on the sophistication and setup of the individual system, control of any individual system, operation, or task can be automatic. SCADA systems consist of both hardware and software.

The Internet of things (IOT) is made up of a network of physical devices connected via electronic embedding, software setups, sensors-actuators, network connectivity which act together for the objects to connect and exchange data. Each 'thing' is uniquely identifiable through its embedded computing system and is also able to inter-operate within the existing Internet infrastructure. IOT allows objects to be sensed or controlled remotely across different networking infrastructures. Thus it creates opportunities for more direct integration of the physical world into computer-based systems, which results in improved efficiency, accuracy and economic benefit and also cuts down on human intervention. When IOT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, virtual power plants, smart homes, intelligent transportation and smart cities among many others

II. ARCHITECTURE

SCADA system is a centralized system, a software package that is positioned on top of hardware. A supervisory system gathers data on the process and sends the commands control to the process. The SCADA is a remote terminal unit which is also known as RTU, which performs most control actions automatically along with PLCs. The RTUs consist of the programmable logic converter which can be preset manually. Overall, SCADA system can be classified into two parts which are Clint layer (responsible for the man machine interaction) and Data server layer (responsible to handle the process data activities). The SCADA station refers to the servers composed of a single PC. The data servers communicate with devices in the field through process controllers like PLCs or RTUs. The connection of PLC to the data servers is made either directly or via networks or buses. The SCADA system utilizes a WAN and LAN networks, which consists of internet protocols used for communication between the master station and devices. The RTUs convert the sensor signals to digital data and sends digital data to master, according to the master feedback received by the RTU, it applies the electrical signal to relays. RTUs or PLCs perform most of the monitoring and control operations.

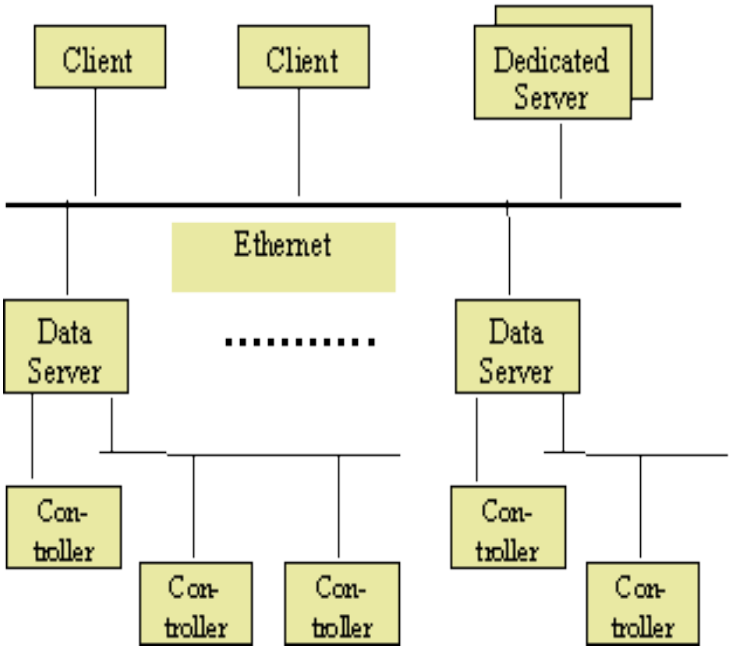

Fig: Block Diagram for Architecture of SCADA

In IOT, sensors collect data from the environment or object under measurement and turn it into useful data. The data from the sensors start in analog form, which needs to be aggregated and converted into digital streams. Data acquisition systems (DAS) perform these data aggregation and conversion functions. The DAS joins the sensor network, groups the outputs, and performs the ADC conversion. The Internet gateway receives the aggregated and digitized data and routes it over Wi-Fi, wired LANs, or the Internet, to Stage 3 systems for further processing. Post data digitization and aggregation, the data may require further processing before it enters the data center. Edge IT systems perform post processing. Data that needs more in-depth processing where feedback doesn't have to be immediate, is forwarded to the physical data center or cloud-based systems, where more powerful IT systems can analyze, manage, and securely store the data. The processing type which gets executed at this stage remains the same for the platform.

III. COMMUNICATION

Server-client and server-server communication is in general on a publish-subscribe and event-driven basis and uses a TCP/IP protocol. The controllers are then polled at a user defined polling rate, which is changes from parameter to parameter. The controllers pass the requested parameters to the data servers. Time stamping of the process parameters is typically performed in the controllers and this time-stamp is taken over by the data server. For controller and communication protocol to support the unsolicited data transfer, the products must support this too. They provide communication drivers for most of the common PLCs and widely used field-buses. VME, on the other hand, is generally not supported. A single data server can support multiple communications because of the presence of multiple slots for interface cards. The configuration data are stored in logically centralized but physically distributed database that is generally of a proprietary format. The RTDB resides in the memory of the servers in a proprietary format for performance reasons. The archive and logging format are usually also proprietary.

In IOT, the "Thing" must communicate through the Internet to be considered an "IOT" node, and it must also adhere to the Internet Engineering Task Force's (IETF) Internet Protocol Suite. Devices must communicate with each other (D2D). Device data should then be collected to be sent to the server infrastructure (D2S). That server infrastructure has to share device data (S2S), possibly providing it back to devices, to analysis programs, or to people. From 30,000 feet, the protocols can be described in this framework as:

1. **MQTT**: a protocol for collecting device data and communicating it to servers (D2S)
2. **XMPP**: a protocol best for connecting devices to people, a special case of the D2S pattern, since people are connected to the servers
3. **DDS**: a fast bus for integrating intelligent machines (D2D)
4. **AMQP**: a queuing system designed to connect servers to each other (S2S)

IV. VULNERABILITIES

SCADA

Lack of monitoring. Without active network monitoring, it is impossible to detect suspicious activity, identify potential threats, and quickly react to cyber-attacks.

Slow updates. With advancement, SCADA systems become more vulnerable to new attacks. Maintenance of the firmware and the software updates may become inconvenient over time but is necessary for maximum protection.

Lack of knowledge about devices. Connecting devices to a SCADA System allows for remote monitoring and updates, this means the knowledge about network connected devices is often incomplete.

Not understanding traffic. Managers need to know what type of traffic is going through their networks. Only then they can make informed decisions about how to respond to potential threats.

Authentication holes. Authentication solutions can easily be defeated due to common unsafe practices such as poor passwords, username sharing, and weak authentication.

IOT

Insecure web interface: Web server/app, there may have flaws in the code that allow the device to be attacked.
Ineffective authentication/authorization: Operability of many devices with their default (insecure) settings is a factor of concern.
Insecure network services: if maintenance services are on open, insecure or vulnerable ports they are potential security holes.
Lack of transport encryption: Device sending private information over an insecure protocol would allow anyone to read it.
Privacy concerns: unencrypted information puts your personal information is at risk.
Insecure cloud interface: Cloud management interface this represents another potential security weakness.
Insecure software/firmware: The device can be patched to address discovered vulnerabilities, also, installing certain software's might brick the device.

V. CONCLUSION

Both the traditional SCADA systems and IOT implemented SCADA have their sets of advantages and vulnerabilities. It is being estimated that by 2020, 50 billion devices or /things will be connected to the internet. The dynamics of entire automation industry is changing, and this is the dawn of a new age of industrial revolution, or industry 4.0. Industry 4.0 is the name of the era responsible for the emerging trend automation and data exchange in manufacturing technologies. It includes cyber-physical systems, the Internet of things, cloud computing and cognitive computing. By working on the vulnerabilities possessed by IOT devices, we can very truly shift from a traditionally implemented SCADA to an IOT implemented one and make Industry 4.0 a living reality.

