RESEARCH ON THE SCADA SYSTEM

NIKOLOZI JAIANI – Master's Student

E-mail: jaianinick@gmail.com

Georgian Technical University

Be received 08.11.2022

Abstract. ***With the rapid development of information technology, People become more and more dependent on the automatic technology in some special industries like oil, electricity and chemistry. As a novel technology, Supervisory Control and Data Acquisition (SCADA) provides core functionality of Energy Management Systems (EMS) and Distribution Management Systems (DMS) in combination with base system services, the data engineering system, the user interface, and the front-end.***

Keywords: ***Supervisory control and data acquisition, service oriented architecture, enterprise service bus (ESB).***

Introduction

SCADA (Supervisory Control And Data Acquisition) is a system to automate industrial control and monitoring. SCADA includes field sensors, Programmable Logic Controllers (PLC) and Remote Telemetering Units (RTU). SCADA systems are used in all industry sectors where it is required to provide operator control over technological processes in real time. This software is installed on computers and uses I/O drivers or OPC/DDE servers to communicate with an object. Program code can be either written in one of the programming languages or generated in a design environment. Functions of SCADA are: Data Processing, Supervisory Control, Network Modification (Online), Selection Management, General Summary, Multi Phase, Display Open Lines, Redundant Data Sources, Topology Analysis and Network Coloring and Area of Control (AOC).

Review of SCADA

SCADA plays a vital part in providing means for upgrading their operating productivity, reducing maintenance costs, minimizing the number of outages, helping to avoid problems and leading to safer operation of the entire infrastructure. GSE reported improved reliability of supply with stable frequency and voltage because of implementation SCADA system across the country of Georgia [1]. They reported safe integration of increasing renewable generation because of implementation of SCADA system.

GSE Georgian State Electricity Transmission System Operator implemented SCADA in 2007, below I am providing which challenges they had before, and which benefits they gained after implementation:

Challenges:

- **Annual Conceptions Growth.**
- **Integration of Renewables into the Grid.**
- **Maintain power system stability despite increasing grid dynamics through volatile electricity flows.**
- **Manage cross-border interconnections.**
- **Enable inter-area energy exchange with Europe, meet the ENTSO-E requirements.**

Solution:

- **Network reliability improvement by SCADA/EMS Spectrum 7, Siguard DSA and other APPs.**
- **Following approved development plan.**

Benefits:

- **Improved reliability of supply with Stable frequency and voltage.**
- **Safe integration of increasing renewable generation.**
- **Harmonization with the standards of the European Network of Transmission System Operators (ENTSO-E) .**

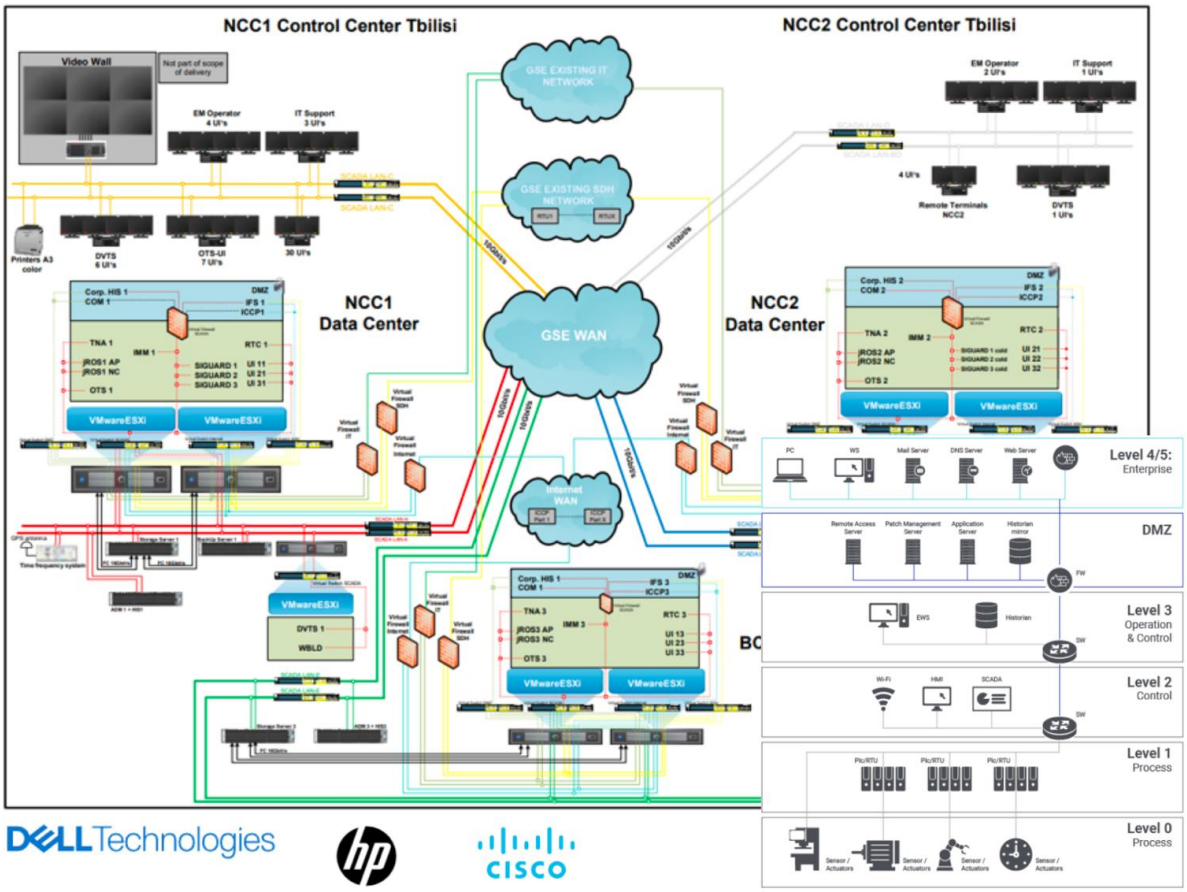
An important part of most SCADA implementations is alarm handling [2]. The system monitors whether certain alarm conditions are satisfied, to determine when an alarm event has occurred. Once an alarm event has been detected, one or more actions are taken (such as the activation of one or more alarm indicators, and perhaps the generation of email or text messages so that management or remote SCADA operators are informed). In many cases, a SCADA operator may have to acknowledge the alarm event; this may deactivate some alarm indicators, whereas other indicators remain active until the alarm conditions are cleared.

Above review of literature can be summarized as, SCADA (supervisory control and data acquisition) is a system, which can monitor and control the process remotely. SCADA operates on signals over communication channels. SCADA system offers variety of advantages over conventional monitoring and data collection systems. The most important aspect of SCADA is one can monitor the process from any remote place. Real time data is available for processing. Quick actions can be taken once the fault is detected. SCADA system can be successfully implemented in variety of application which includes Industrial applications, Infrastructure applications, Energy Applications, Defense, Space etc.

Cybersecurity

Typical Cyber Security principles are Confidentiality, Integrity, and Availability (CIA). Cyber Security for control systems changes the priorities to Availability, Integrity, and Confidentiality (AIC).

SCADA developers understands the need to ensure that customer systems are secure. The measures taken to meet this obligation cover a wide range – from background checks on employees through restricting and digitally recording access to facilities. It includes employee training, restricting access to in-house customer systems, documents and data, safeguarding any remote access capability, and protecting information about security vulnerabilities.



HW Architecture and Cyber Security in GSE [1]

Three Tier 2 Data Centers

- **Physical HW: 13 Servers, 10 Switches and 3 Firewalls.**
- **Virtual: 65 Virtual and 9 Virtual Firewalls.**

Main and Reserve Dispatch Centers

- **40 Active workplaces.**

Cyber Security

- **Segregated Network, Purdue Model.**
- **There is no route from internet, servers, users.**
- **or any other networks to SCADA Network.**
- **Any Information exchange between SCADA and IT Network happens through the DMZ.**
- **Any routes from SCADA or outside networks terminated in DMZ.**

- **Privileged Access Management (PAM).**
- **Web Application Firewall (WAF).**
- **Integration of SCADA logs in SIEM in progress.**

Conclusion

As SCADA network are more and more popular for the industry, the data fusion and analyzing problem become more and more prominent. The Intelligent Alarm Processor provides information about the kind of the fault, the fault location and possibly failures of protective devices after a network disturbance, as well as an explanation of its consequences. Traditional method paid much attention on the reliability and security of SCADA network, yet some factors like convenience and usability are neglected. This paper introduced the concept and described live example of benefits and solutions SCADA can provide to industry sector.

R E F E R E N C E S

1. **GSE (Georgian State Electrosystem). Tbilisi. Georgia.**
2. **Boyer, Stuart A. SCADA Supervisory Control and Data Acquisition. USA: ISA – International Society of Automation. 2010.**