SCADA

S. Venkatesan

Acknowledgement: The contents, example scripts and some figures are copied from various sources.
Thanks to all authors and sources made those contents public and usable for educational purpose

Introduction

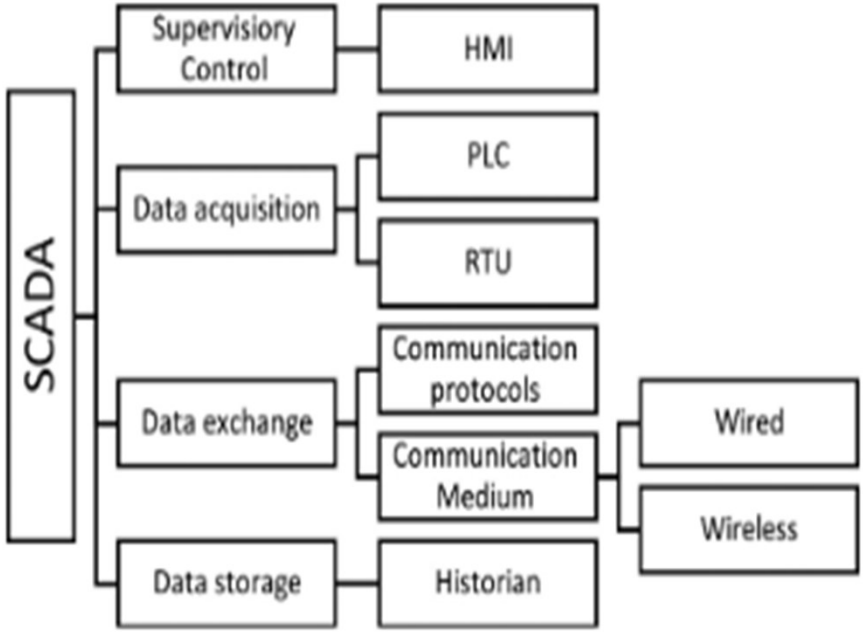
- SCADA stands for Supervisory Control and Data Acquisition
- Coined in 1970
- To monitor and automate the control processes of industrial automation.
- Architecture:
  - Sensors and Machinery passes the information to PLC or RTU
  - PLC or RTU route the information to computers running the SCADA software.
  - The software processes, distributes, and displays information on a Human Machine Interface (HMI) for a human operator to make decisions based on the information.

Program Logic Controller Vs Remote Terminal Unit

	PLC	RTU
Energy	PLCs require lower wattage because they are typically used in industrial settings and only need to operate for short periods of time.	RTUs require higher wattage because they need to remain powered for long periods of time in order to monitor remote locations. However, consumes less by putting sometime on sleep mode.
Application		RTUs can be used in remote locations or in harsh conditions that pose a danger to human life and can transfer data and communicate wirelessly.
Data Transfer	At intervals	Driven by events

Components

- Sensor
- RTU/PLC
- SCADA Master Unit / Sub-Master Unit
- Communication Networks
- Storage

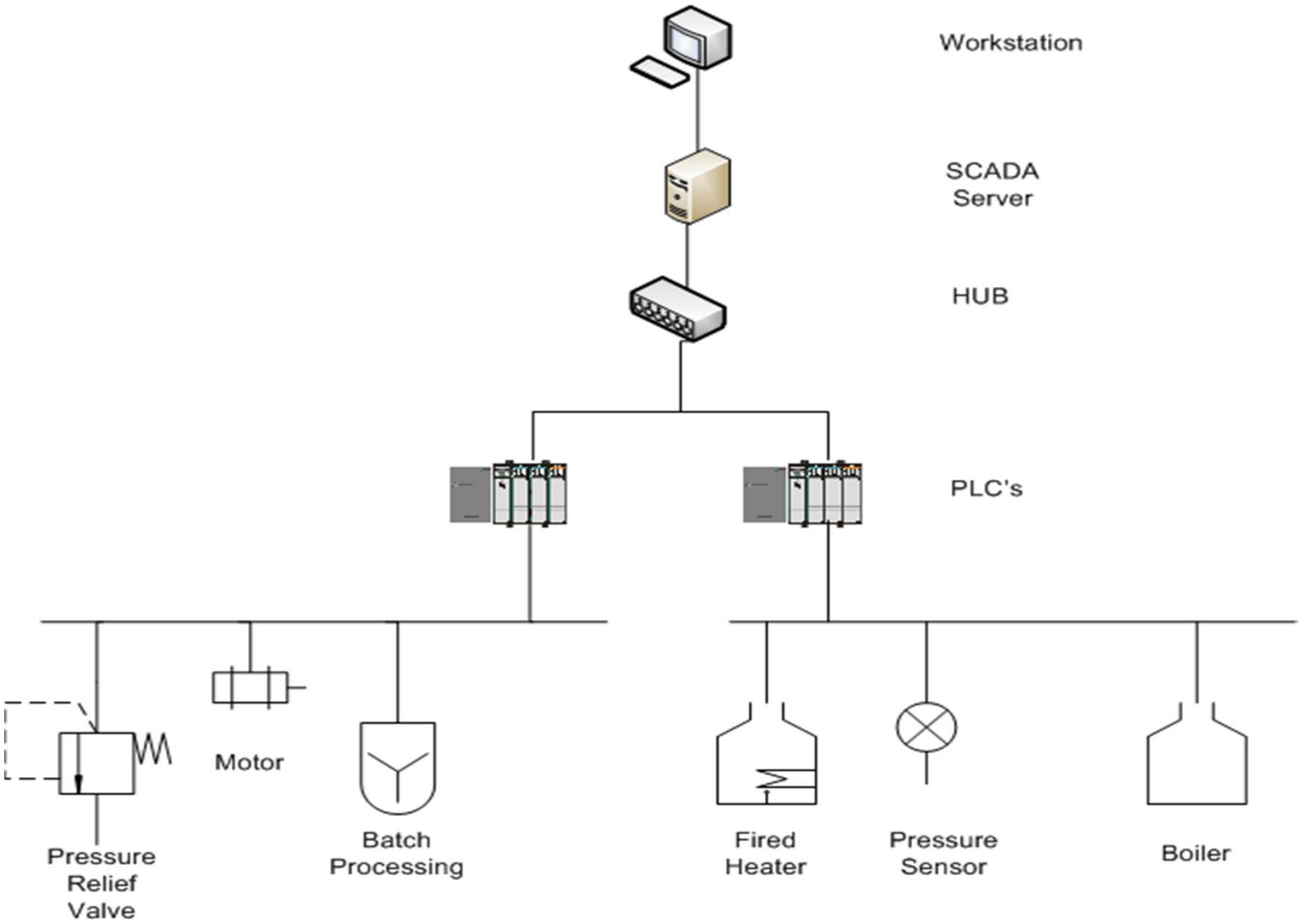


Manar Alanazi, Abdun Mahmood, Mohammad Jabed Morshed Chowdhury, “SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues”, Computer sand Security 2023.

SCADA Components

- Corporate network segment
  - Typical IT network
- SCADA network segment
  - Servers and workstations to interact with field devices
  - Human-machine interfaces
  - Operators
  - Software validation
- Field devices segment
  - Programmable Logic Controllers (PLC)
  - Remote Terminal Units (RTU)
  - Intelligent Electronic Devices (IED)

SCADA and PLC Overview



Functions

- Data Acquisition
- Network Data Communication
- Data Presentation
- Control

Advantages of the SCADA

- The data can be displayed in a variety of formats based on the needs of the user.
- Real data simulations can be obtained with the assistance of operators.
- It provides an interface to connect thousands of sensors across the wide region for various monitoring and controlling operations.
- The system is capable of storing large amounts of data.
- Real data simulations can be obtained with the assistance of operators.
- Many types of data can be gathered from RTUs connected with the master unit.
- Data can be monitored from anywhere, not just the local site, using advanced protocols and application software.
- It is fast in obtaining a response.
- The SCADA system incorporates unit redundancy to provide a backup in the event of faults or failures. This strengthens the system.

Disadvantages

- Installation costs are higher.
- Because the system is complex, skilled operators, analysts, and programmers are required to maintain the SCADA system.
- In terms of hardware units and dependent modules, the PLC-based SCADA system is complex.
- The system allows for the use of restricted software and hardware.

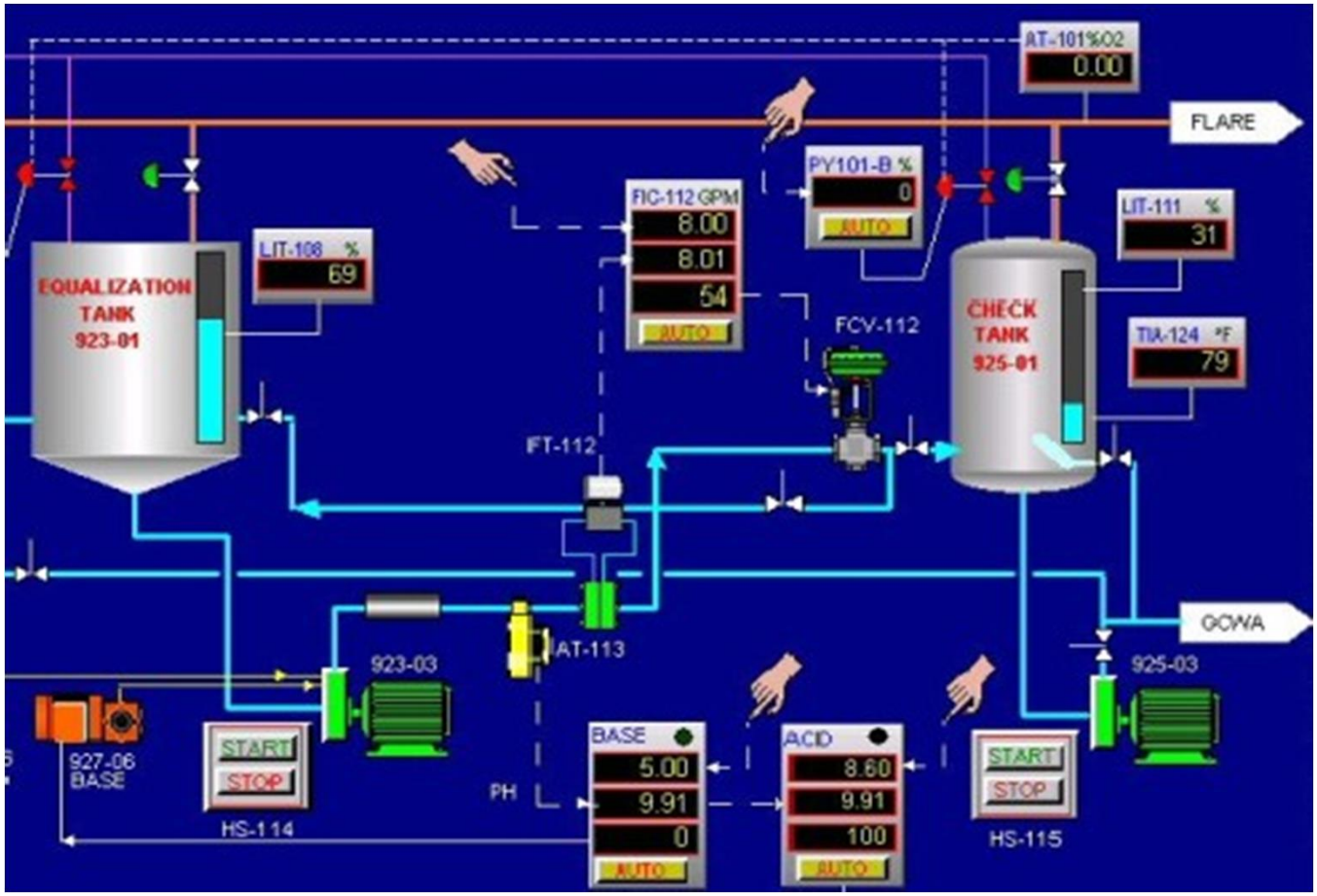
HMI

- A Human-Machine Interface (HMI) is a user interface or dashboard that connects a person to a machine, system, or device.

- Any screen that allows a user to interact with a device, HMI is most commonly used in the context of an industrial process.

- HMI screens can be used for a single function, like monitoring and tracking, or for performing more sophisticated operations, like switching machines off or increasing production speed, depending on how they are implemented.

An Example HMI



Source: http://controlsystemsusa.com/plcscada/SCADA.asp

Design

- Monolithic: In 1970s, control units or MTUs were hard-wired to RTUs.
- Distributed: In 1980s to 1990s, MTUs and RTUs communicated using communication protocols and servers. However, they did not allow Internet connection.
- Networked: In 2000s, SCADA architecture started using external networks like the Internet.
- Web-based SCADA: Currently, users can access SCADA systems using web browsers and mobile devices.

Communication Protocols

- Modbus, Profinet, Distributed Network Protocol 3 (DNP3), and IEC 60870 – 5.

- DNP3 has Bump-in-the-wire (BITW)

Applications

- Energy
- Water System
- Healthcare
- Chemical System
- Agriculture
- Nuclear System
- So on

Attackers

- Script kiddies
- Hackers
- Organized crime
- Disgruntled insiders
- Competitors
- Terrorists
- Hactivists
- Eco-terrorists

SCADA Security

- Perimeter Protection
  - Firewall, IPS, VPN, AV
  - Host IDS, Host AV
  - DMZ
- Interior Security
  - Firewall, IDS, VPN, AV
  - Host IDS, Host AV
  - NAC
  - Scanning
- Monitoring
- Management

Stuxnet

- Stuxnet reportedly destroyed numerous centrifuges in Iran's Natanz uranium enrichment facility by causing them to burn themselves out.

- Stuxnet has three modules:
  - a **worm** that executes all routines related to the main payload of the attack;
  - a **link file** that automatically executes the propagated copies of the worm;
  - a **rootkit** component responsible for hiding all malicious files and processes, to prevent detection of Stuxnet.

- Stuxnet, discovered by Sergey Ulasen, initially spread via Microsoft Windows, and targeted Siemens industrial control systems.

Attacks

- Implementation Level
  - Lack of Input Validation
  - Invalid Index Array
  - Improper Limitation of memory buffer
  - Improper Control Flow Management
- Configuration Level
  - Weak Password
  - Improper Access Control
  - Protection Mechanism Failure (on Data)
  - Improper Authentication

References

- https://www.plctechnician.com/news-blog/scada-system-what-it-and-how-it-works
- https://inductiveautomation.com/resources/article/what-is-hmi
- SAGARIKA GHOSH, AND SRINIVAS SAMPALLI, “A Survey of Security in SCADA Networks: Current Issues and Future Challenges”, IEEE Access, 2019.
- https://www.integraxor.com/support/scada-training/configure-simple-scada-system/
- Manar Alanazi, Abdun Mahmood, Mohammad Jabed Morshed Chowdhury, “SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues”, Computers & Security, Volume 125, 2023, 103028.