**CHAPTER 2**

**LITRATURE REVIEW**

**2.1 SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) NETWORK**

**2.1.1 GENERAL**

Supervisory Control and Data Acquisition (SCADA) systems are Industrial Control Systems (ICS) broadly utilized by industries to study and control different processes such as oil and gas pipelines, water distribution, power supply grids, etc. These systems provide automated control and remote monitoring of services being employed in everyday life. For example, states and municipalities use SCADA systems to observe and regulate water levels in reservoirs, pipe pressure, and water distribution.

 A typical SCADA system comprises of components like computer workstations, Human Machine Interface (HMI), Programmable Logic Controllers (PLCs), sensors, and actuators. Historically, these systems had private and dedicated networks. However, because of the wide-range deployment of remote management, open IP networks (e.g., Internet) are now used for SCADA systems communication. This exposes SCADA systems to the cyberspace and makes them prone to cyber-attacks using the web.

**2.1.2** **SCADA NETWORK VULNERABILITIES AND THREATS**

Diagram

Description automatically generated

**Figure 1 : SCADA Architecture**

Critical infrastructures (CI) like the power system, oil and gas pipelines, water distribution, etc. are monitored and controlled by SCADA systems which the combine the CI together as a network through advanced Information Technologies (IT) . As shown in Fig 1, the SCADA system architecture for the electricity grid basically comprises of four major operational parts namely:

* The ``Field'' devices like sensors for sensing the status of SCADA equipment under concern (power level, pressure, etc.) and control them as per the received commands.
* The ``Remote Station'' devices which include the Remote Terminal Units (RTUs) and Programmable Logic Controllers. They serve the aim of sending and receiving digital data to and from the control centers and also the field devices.
* The ``Control Centre'' devices consisting of the Master Terminal Units (MTU) that issues command to the remote station devices.
* Human Machine Interface (HMI): devices which present processed data to operators usually via graphic user interface. With the interface, the operators can monitor, control and interact with SCADA processes.

Historically, when SCADA systems were first deployed, the key threat was sabotage through the physical destruction of the utility's hardware because the old SCADA systems had private and dedicated networks that are secured by traditional air gapped separations. However, over the past 20 years, SCADA networks have been equipped with IoT devices that sometimes communicate over open channels which exposes the networks to numerous vulnerabilities and network based cyber-attacks. These threats and attacks are projected to escalate in geometric rates in the upcoming future as intruders/attackers find the energy infrastructures (arguably the most important of all CI) as a lucrative avenue to gain attention. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) announced that, out of the 245 recorded cyber incidents on CI in 2014, seventy-nine have been focused on the energy sector.

Based on the motives and the reason of attacks, SCADA threats and attacks can be categorized as:

1. Internal/Malicious - operators, employees, or contractors with intentional motives to cause disasters to the SCADA network. For example, a well-publicized Stuxnet worm attack by a resentful engineer via a removable drive.
2. Internal/Non-malicious - operator making an accidental mistake that causes harm to power system network. For example, In 2003, Ohio Davis-Besse nuclear plant ``Slammer'' worm infection that led to the plant being disabled for hours.
3. External/Opportunistic - hackers seeking a challenge or fooling around.
4. External/Deliberate - this could be described as an attack by an external organized group that targets vulnerabilities in another nation/state power system like the 2015 cyberattack on Ukrainian power system network whereby the hackers were linked to Russia.

These experiences and several other reported cases have showcased the immeasurable consequences of attacks on SCADA networks.

**2.1.3 WSCC 9 BUS SYSTEM**

Graphical user interface, application

Description automatically generated

F

E

D

C

B

A

Load

Load

Load

776.5MVA

24KV, 50Hz

960MVA

26KV, 50Hz

1200MVA

26KV, 50Hz

**Figure 2 : Single Line Diagram of a WSCC 9 Bus System**

The power system network consists of three generators. It has three load buses–Bus 5, 6 and 8. Voltage and MVA rating of generators 1, 2 and 3 are 776.5 MW and 24 kV; 1200 MVA and 26 kV; 960 MVA and 26 kV respectively. The rating of the load connected to bus 5, 6 and 7 are 115 MW and 50 MVAR; 96 MW and 30 MVAR; 110 MW and 35 MVAR respectively. Work presented here, attempts to identify type of fault, fault location and the bus parameters in pre-fault, during fault and post-fault condition of LG, LL, LLG, LLL, LLLG fault. The faults are made to occur at load buses.

**2.1.4 FAULTS**

Basically, the Power System network equipment or appliances are so designed in such a way to perform a non-stop required function except in case of preventive maintenance or because of lack of external sources. The fault is the random character that may appear in the power system network, and because of this inability to perform the desired function, since the fault can occur at any situation and any location within the power system, the fault is random. The balanced three-phase A.C. is the steady-state operating mode of a power system, because of adverse external and internal changes within the system, the above condition is disrupted. In any case, if the insulation of the system fails in the following particular locations like Phase conductors or Phase conductor and earth or any earthed screens surrounding the conductors, the fault will occur.

**2.1.4.1 LEADING CAUSES OF FAULTS**

Faults within the power system grid occurs because of the various causes mainly it is categorized in two ways as follows:

1. Breakdown or failure at typical voltages due to deterioration of insulation, damage due to unpredictable causes like an unfortunate tree falling across the line, vehicles colliding with electric poles, short-circuiting by birds.
2. Breakdown or failure at abnormal voltages due to Lightning or Switching surges, Arcing ground.

In most cases, the chance of failure or breakdown occurs within the overhead lines (OL) due to the greater length of the conductor's exposure to the atmosphere. Transmission network or Transmission lines of the power system network used for the transportation of the majority power from the sending end to receiving end (i.e., from the generating station to the load centre) are due to its characteristics in nature it is always exposed to the all atmospheric condition either the temperature is high or low it is designed as per recruitment using the sag calculation by the due course this conductor has the highest fault rate when put next to the other equipment within the power systems. The practical study of grid failures could be a critical issue in many power system research, like network scheduling, equipment design, and alignment of protective systems.

**2.1.5 CATEGORIES OF FAULT**

In most cases, the chance of failure or short circuit fault is the most essential and dangerous common fault that probably occurs in the power system as already discussed. These kinds of faults occur due to breakdown or failure in the insulation of current-carrying phase conductors relative to earth or in the insulation between the phases.

The fault that occurred due to a short circuit in the three-phase a.c. Power circuit is

* The Line-to-Line Fault (L-L).
* Single Line to Ground Fault (L-G).
* Double Line to Ground Fault (L-L-G).
* All the three phases to ground Fault (L-L-L-G).
* All three phases short-circuited (L-L-L).

|  |  |
| --- | --- |
| Type of Fault | Percentage % |
| Single line to ground fault (L-G) | 65-70 |
| Line to Line fault (L-L) | 10-15 |
| Double Line to ground fault (L-L-G) | 8-10 |
| All three phase to ground fault (L-L-L-G) | 2-3 |
| All three-phase short circuited (L-L-L) | 2-3 |

**Table 1 : Types of faults and their probability of occurrence**

On the type, as mentioned earlier of a fault, the first three types are said to be unbalanced operating condition because it involves only one or two-phase, and hence, it is termed as unsymmetrical faults. i.e., in short, different currents in the three phases. The last two types of faults occurred in all three phases, and so it is termed as symmetrical faults i.e., equal fault current in the three phases with 120°. Compared to all the above faults, the line to ground(L-G) fault is the most common fault that occurred in the OH lines, whereas the balanced three-phase fault is the rare one, but it is the severe fault which occurred because of the carelessness of the operating personnel. Fault analysis is essential for secure and high-speed protective relaying supported by digital distance protection. Therefore, a proper evaluation of those methods is required.

**2.1.6 FAULT DETECTION AND CLASSIFICATION**

The techniques for detecting a fault and classifying them make use of changes in current and voltage signals just in case of fault. Techniques range from hand-coded expert-defined rules supported certain thresholds to artificial intelligence-based techniques like ANNs, vector supporting machines, and blurred decision systems. The methods vary from hand-coded and expert-defined rules based on certain thresholds to artificial intelligence-based techniques, like support vector machines, fuzzy decision systems, ANNs. Several characteristics and signal transformations were suggested and used for detection purposes, like Fourier and wavelet transformations. While protection of critical lines and system buses is ensured with local protection equipment like relays and circuit breakers, the info made available by PMUs offer the potential to extend understanding and situational awareness during a power management centre as also suggested using the output of a PMU-only state estimator for detection and classification of faults. during this context, the approaches in use decision trees, and employs support vector machines for this purpose. Such methods presume, as discussed above, the entire presence of all the measurements fully synchronization, given the promising results provided in these works. within the scope of this work, we've experimented with two fault detectors for the output of a PMU-only state estimator: one based on ANN and the other based on support vector machines. due to the observed superior performance of ANN and space limitations, we restrict our discussion and findings with ANNs within the following to detect and identify faults. Further work is ongoing for a comparison of various machine learning-based techniques for installation fault detection and classification.