INVESTIGATIONS ON POWER SUPPLY AND SCADA SECURITY ISSUES OF 25 KV AC TRACTION SYSTEM

A DISSERTATION SUBMITTED TOWARDS THE PARTIAL FULFILMENT
OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF
MASTER OF TECHNOLOGY
IN

POWER ELECTRONICS SYSTEM
(2014-2016)

SUBMITTED BY
JITENDER KUMAR
Roll No.2K13/PES/507

UNDER THE GUIDANCE OF
Prof. Narender Kumar, DTU

Department of Electrical Engineering
Delhi Technological University
(Formerly Delhi College of Engineering)

July 2012

CERTIFICATE

This is to certify that this project titled " INVESTIGATIONS OF POWER SUPPLY AND SCADA SECURITY ISSUES OF 25KV AC TRACTION SYSTEM " submitted in partial fulfillment of the requirements for the award of Degree of Master of Technology by Jitender Kumar at Delhi Technological University is a record of original research work carried out by him under my guidance. Any material borrowed or referred to is duly acknowledged.

Jitender Kumar
2K13/PES/507
M. Tech. (P/T) PES

ACKNOWLEDGEMENT

I express my sincere thanks to my project guide Prof. Narender Kumar, for providing me an opportunity to work under his guidance and tireless support during the course of the project. His continued cooperation, never-ending encouragement, meticulous guidance and uninhibited support at various stages helped me in preparation of this research study.

I would also like to thank Professor Dr. Vishal Verma, Dean of PG courses & Controller of Examinations of DTU and Sh. Amritesh for their cooperation and support.

I would also like to acknowledge the vital role of my seniors and colleagues from present organization Delhi Metro Rail Corporation Limited, in providing me with the opportunity to gain insight into the existing traction drive system of train along with its technical and failure details.

Jitender Kumar
2K13/PES/507
M. Tech. (P/T) PES

ABSTRACT

Recently, Need of electrical railways are felt as most preferred mode of public transport because of fossil energy depletion and to prevent global warming due to carbon emission. 25KV AC network is adopted in cities having high traffic or cover long distances. 25 kV AC traction has the economical advantages of less number of traction sub-stations and capacity to carry large traffic and suited for urban cities having passenger capacity of more than a lakh per day. Power supply for 25KV AC traction system is fed to overhead conductors at feeding post location through traction sub-station having 02 transformers in hot/standby configuration. This power supply is used by locomotives with the help of pantograph for current collection. When any problem occurs in the network due to signalling or locomotive failure, there is a tendency of bunching of trains in one feeding section which causes tripping of traction feeder breakers on overcurrent. During such scenario, it should be possible to allow parallel operation of traction transformers with a mechanism to reduce the fault level.

Feed from one substation on single phase 25 kV, depending on number of trains and voltage drop, gets limited to 16 to 20 kMs. Therefore, Neutral section is implemented between two different sources to prevent bridging of two different phases.

When a train passes through a neutral section, the electrical power supply phase is changed. Before negotiating neutral section, the train must switch off the circuit breaker to avoid transients such as inrush currents and arcs. If train circuit breaker doesn’t open while negotiating healthy section to dead section, there is huge arc due to current break which cause severe damage to overhead components. Also, life of the train circuit breaker owing to its frequent operation is affected.

Conventional neutral section has demerits and operational implications which demands to explore new technology to be used in place of neutral section. Fail safe mechanism using Semi-conductor commutated neutral section is analyzed in this report to mitigate these problems when trains pass through the neutral section.

An alternate of conventional neutral section and fault level limiter is discussed in this report.

Further, SCADA system implemented for control and monitoring of traction system should be well secure to ensure reliable monitoring and safe control of traction devices. Vulnerability assessment of traction system and remedies are discussed in this report.

This thesis investigates aspects of semi-conductor based neutral section, Superconducting fault current limiter and its security aspects of SCADA system for a 25KV AC traction system.

Following are the objectives of research/Project:

a) To compare the conventional neutral section with semi-conductor based neutral section using mat lab simulation

b) To simulate switching of 25KV supply using series connected IGBTs and studies its response during normal and transient conditions.

c) To simulate semiconducting fault current limiter to reduce fault level during transient conditions.

d) To assess vulnerability aspects of SCADA system for 25KV AC traction system from security point of view.

e) To analyze different SCADA security aspects at interface level, communication level, hardware and software level of a 25KV AC traction SCADA system for a 25KV AC traction system and recommend solutions to improve SCADA security.

Table of Contents

LIST OF FIGURES

CHAPTER-1

INTRODUCTION

1.1 General

Power supply for 25KV AC traction system is fed to overhead conductors at feeding post location through traction sub-station. This power supply is used by locomotives with the help of pantograph for current collection. Feed from one substation on single phase 25 kV, depending on number of trains and voltage drop, gets limited to 16 to 20 KMs. Therefore, Neutral section is implemented between two different sources to prevent bridging of two different phases. A conventional neutral section is as shown in fig.1.1

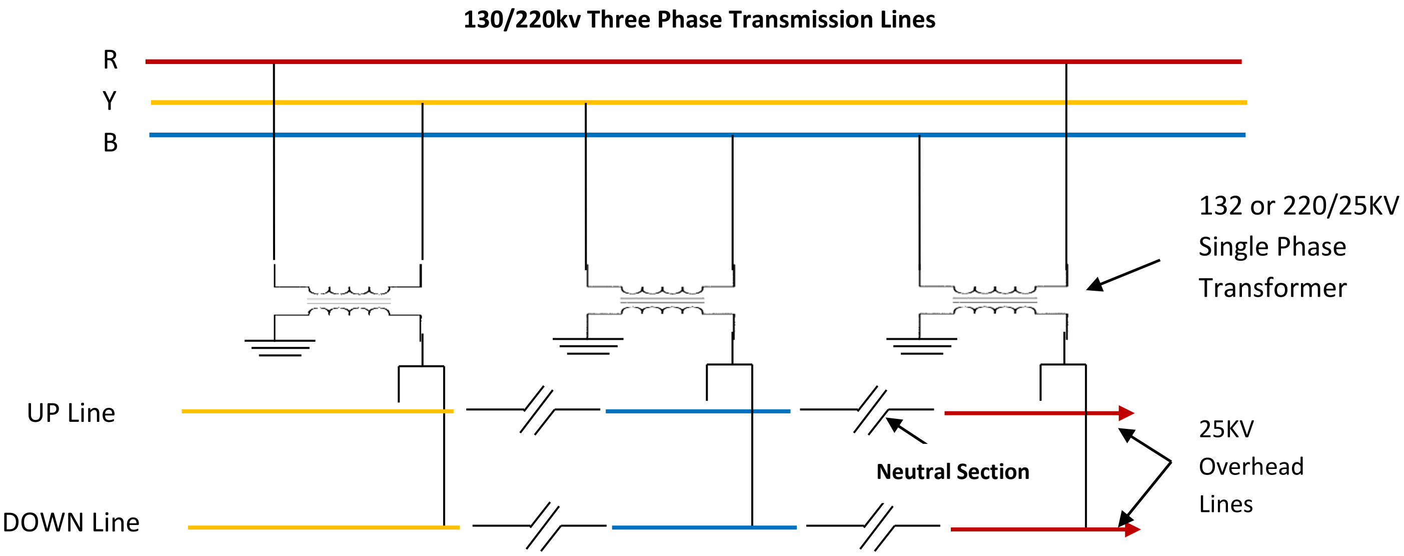


Fig.1.1: 25KV AC Traction System

Conventional neutral section has demerits and operational implications which demands to explore new technology to be used in place of neutral section. Semi conductor switch has opening and closing time in terms of microseconds or even less. Therefore, semiconductor switch is considered as a medium for current break. Fail safe mechanism using Semi-conductor based neutral section is analyzed in this report.

1.2 Power Supply Arrangement

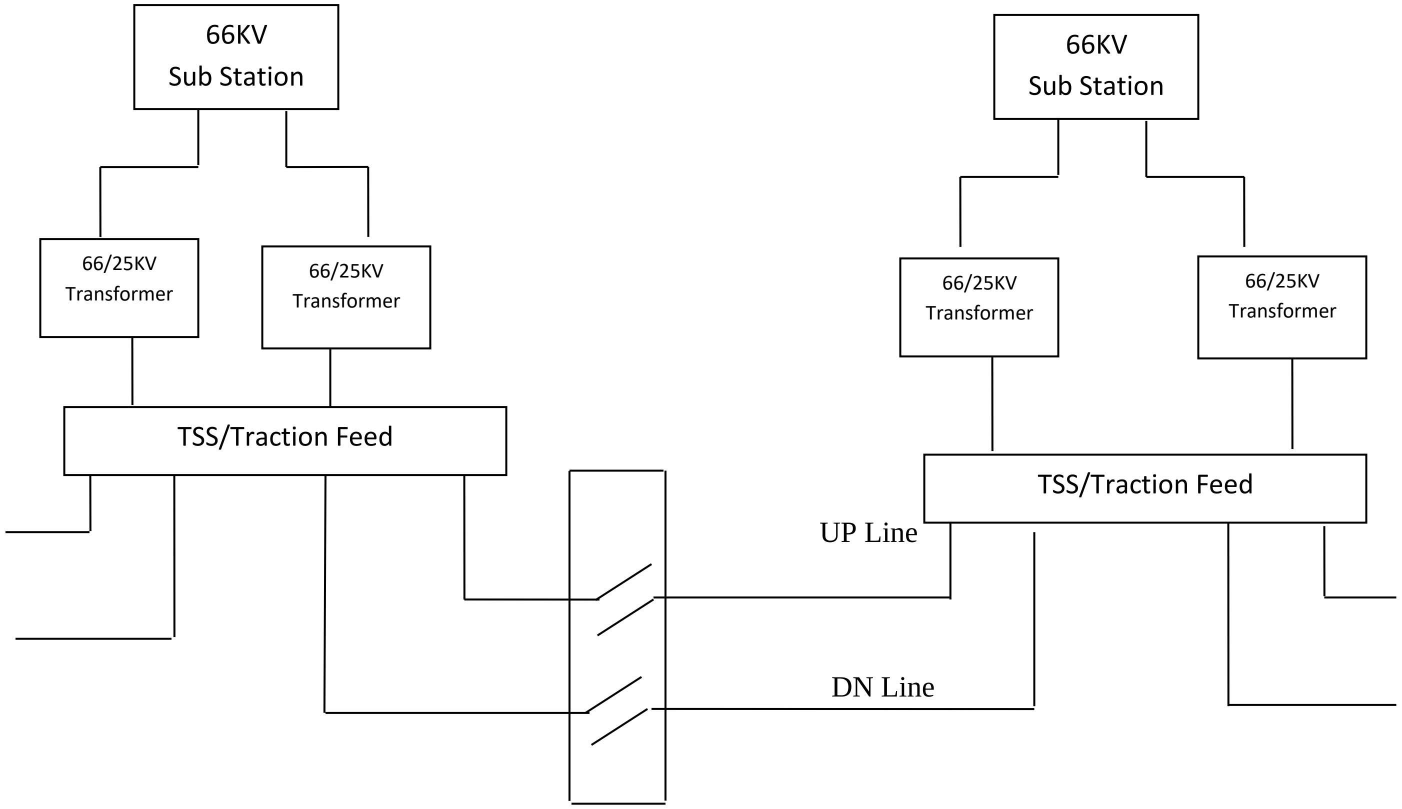


Fig.1.2: Neutral Section

Fig.1.2 shows typical arrangement of Power supply arrangement for a 25 KV AC traction system. Each substation has two transformers in hot/standby configuration and are electrically separated using neutral section. When one 66KV substation fails, Power Supply is extended from adjacent Substation by closing breakers at Neutral Section.

During extended feed, frequent OCR tripping and melting of OHE connectors and jumpers have been reported, data measured by Power Analyzer is shown in fig.1.3 as below:

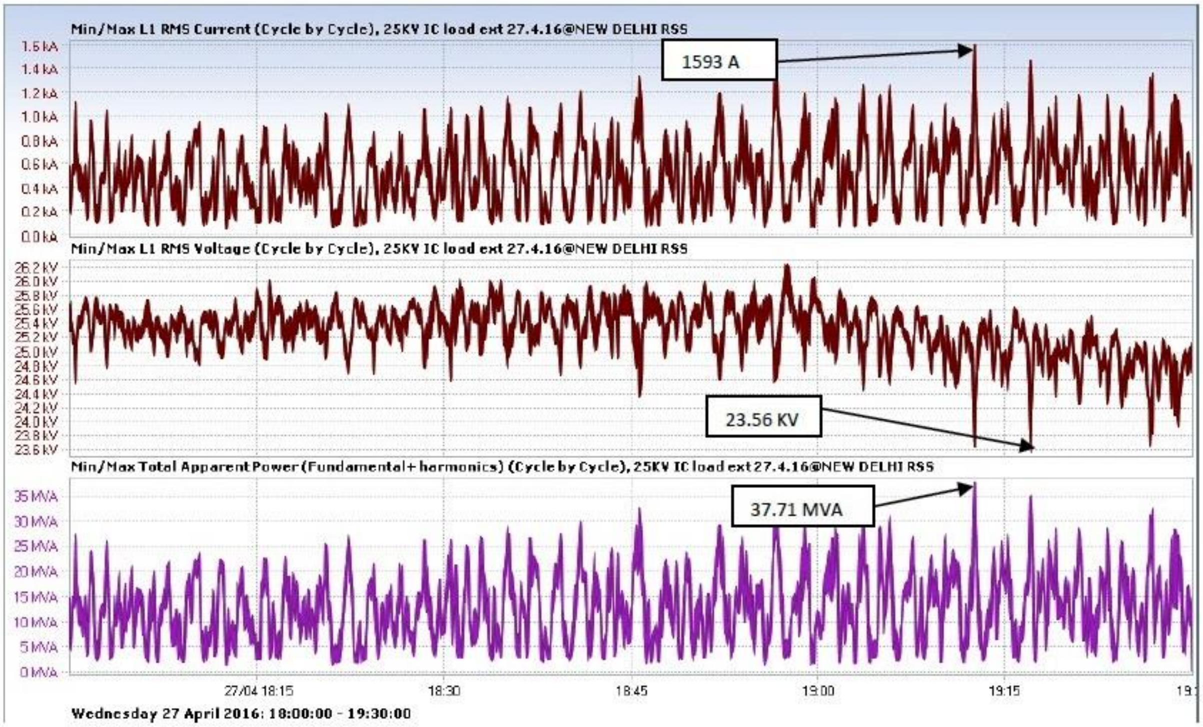


Fig.1.3: Power Analyzer log of 25KV TSS during extended feed condition

There are two traction transformers in a substation which act in hot/standby configuration. Data of transformer is as below:

Transformer Capacity	30MVA
Ratio	66/27.5KV
Impedance	13.5%
OHE Fault capacity	10KA

Fault level calculations are done as below.

1	Short circuit calculations of 66/25KV TSS with transformers in parallel	
2	System Voltage in KV	66
3	% Imp of 66/25KV Transformer (Tx) at RSS Delhi	13.8
4	Transformer Primary Voltage	66
5	Transformer Secondary Voltage	25
6	Tx Capacity in MVA	30
7	PU value of 30 MVA Tx on 30MVA base	0.138

8	Ohmic Value value of 30 MVA Tx reffered to25KV	2.875
		3 Ph SC KA
9	Fault Level 66KV Bus 100MVA Base-Source Imp KA	13.65
10	SC MVA Source	1559.51
11	PU on 100 MVA Base	0.0641
12	%impedance 100MVA base	6.4123
13	%Impedance 30MVA base	1.9237
14	PU Impedance 30MVA base	0.0192
15	Ohmic Value	2.7932
16	Ohmic Value refferred to 25KV system	0.4008
17	Total Ohmic Impedance of Tx	1.6
18	Total Ohmic Impedance Tx+source 66system	2.04
20	Short Ckt Current on 25 KV side Highest Current Terminal Fault at Transformer	12263

If both transformer are operated in parallel configuration, fault level will increase the withstand capacity of equipments. Hence fault current limiter (FCL) needs to be provided when both transformer are operated in parallel.

1.3 Conventional neutral section

Neutral Section is a short section of insulated and dead overhead equipment, which separates the areas fed by adjacent sub-station or feeding post.

Why Neutral Section :

- Feed from one substation on single phase 25 kV, depending on number of trains and voltage drop, gets limited to 16 to 20 kMs
- Further, feed is taken from another substation
- To keep system balanced within permissible limits , single phase traction supply is taken from different phase at adjacent substations.
- If OHE is continuous between 2 RSSs, two phases will get short circuited.

Since the neutral section remains 'dead', warning boards are provided in advance to warn and remind the Train Operator of an approaching train. Generally special care is taken in fixing the location of neutral sections, on level tangent tracks, far away from stop signals or track circuit bonding etc. to ensure that the train coasts through the neutral section at a sufficient speed, to obviate the possibility of its stalling and getting stuck within the neutral section zone.

Train computer is fed the information about neutral section location i.e. the two stations between which it lies and also the start & end distance from the starting station. The train computer is also programmed for the logic that Vacuum Circuit Breaker (VCB) must be opened at location defined for the neutral section and if, not so then force opens the VCB [3]. The start station location is conveyed to train computer by Automatic Train Protection (ATP). Immediately after that, it starts counting the distance and monitoring the VCB status. In case the normal neutral section logic fails to open the VCB, train computer based on pre-programmed logic forces VCB to open. The only condition for above logic to work is, live ATP and correct starting station to neutral section start and end distance. Normally, the circuit breaker gets opened through neutral section detector (NSD) activated by track side magnet before approaching the neutral section and then switched 'on' at the other side of the neutral section by another track side magnet.

1.4 Types of Neutral Section :

1. Three SI type: This type of neutral section is equipped with 03 nos. section Insulator. The distance between these section insulators in the direction of train movement is 27m & 3m respectively. The neutral section cannot be bypassed only the supply can be extended by closing the bridging interrupter placed across neutral section. Following problems have been reported in this neutral section :
   - Melting of droppers
   - Flashing of insulators
   - Stalling of train in NS
   - Non opening of train VCB – Reliability of VCB opening not 100%

2. PTFE (Poly Tetra Floro Ehylene) Type: This type of neutral section is equipped with 02 nos. of PTFE type neutral sections as shown in fig.1.4. The length of neutral section is 6.6 meters and is grounded at mid-point. The neutral section cannot be bypassed only the supply can be extended by closing the bridging BM.

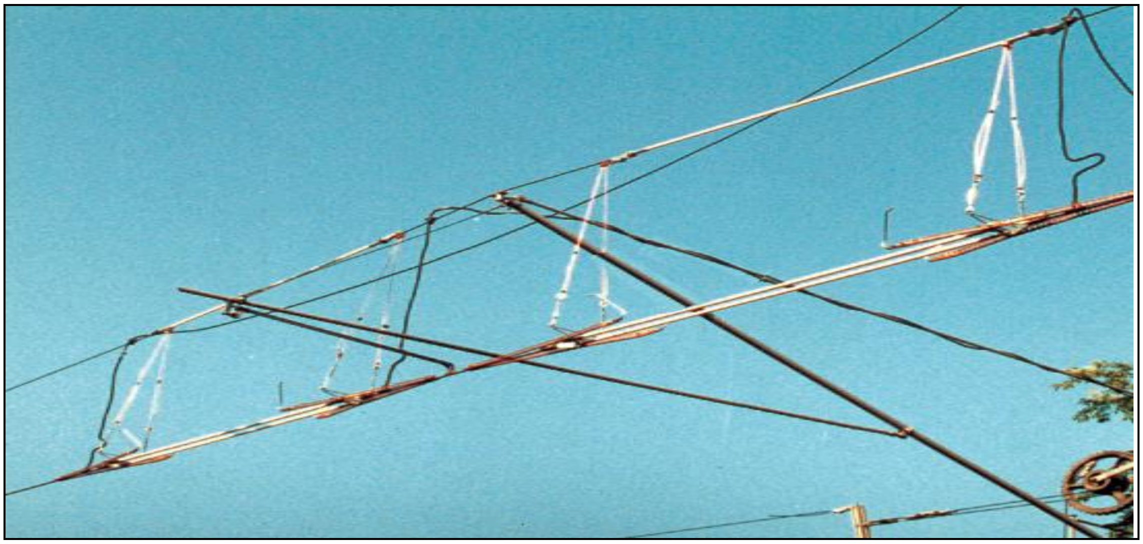


Fig.1.4: PTFE Type Neutral Section

Problems Faced in PTFE Neutral Section :

- PTFE rod and runners are required to be replaced periodically
- Limited capability to withstand non opening of VCB – Flashing

In order to protect the train from undesired arc between Pantograph and Catenary, it is desired that when the traction unit passes through that region the traction unit is automatically powered down and disconne cted via a VCB before entering a neutral section and is automatically connected after passing the neutral s ection.

1.5 Working of neutral section

Neutral section detector is installed to protect the train from undesired power transmission between pantograph and catenary when the traction unit passes through that region the traction unit is automatically disconnected via a VCB before entering a neutral section (Dead section) and is automatically reconnected after passing the neutral section.

Switching off of the current is done by the main switch of the loco, either because the loco position is detected automatically by sensing magnets (inductors) placed at track side as shown in fig.1.5

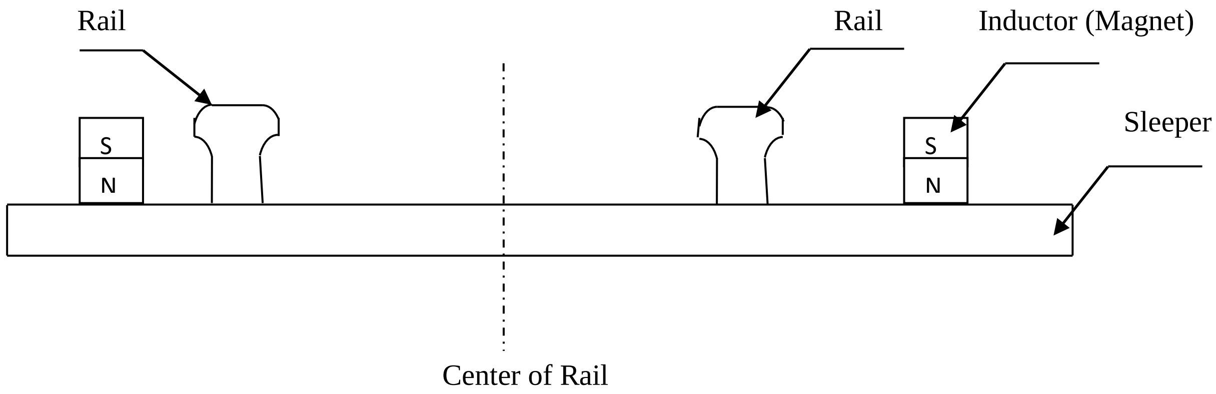


Fig.1.5: Working of Neutral Section

When Train approaches neutral section, Train borne equipment senses the magnet and give command to vacuum circuit breaker of the train. Traction circuit of a train is shown as fig.1.5

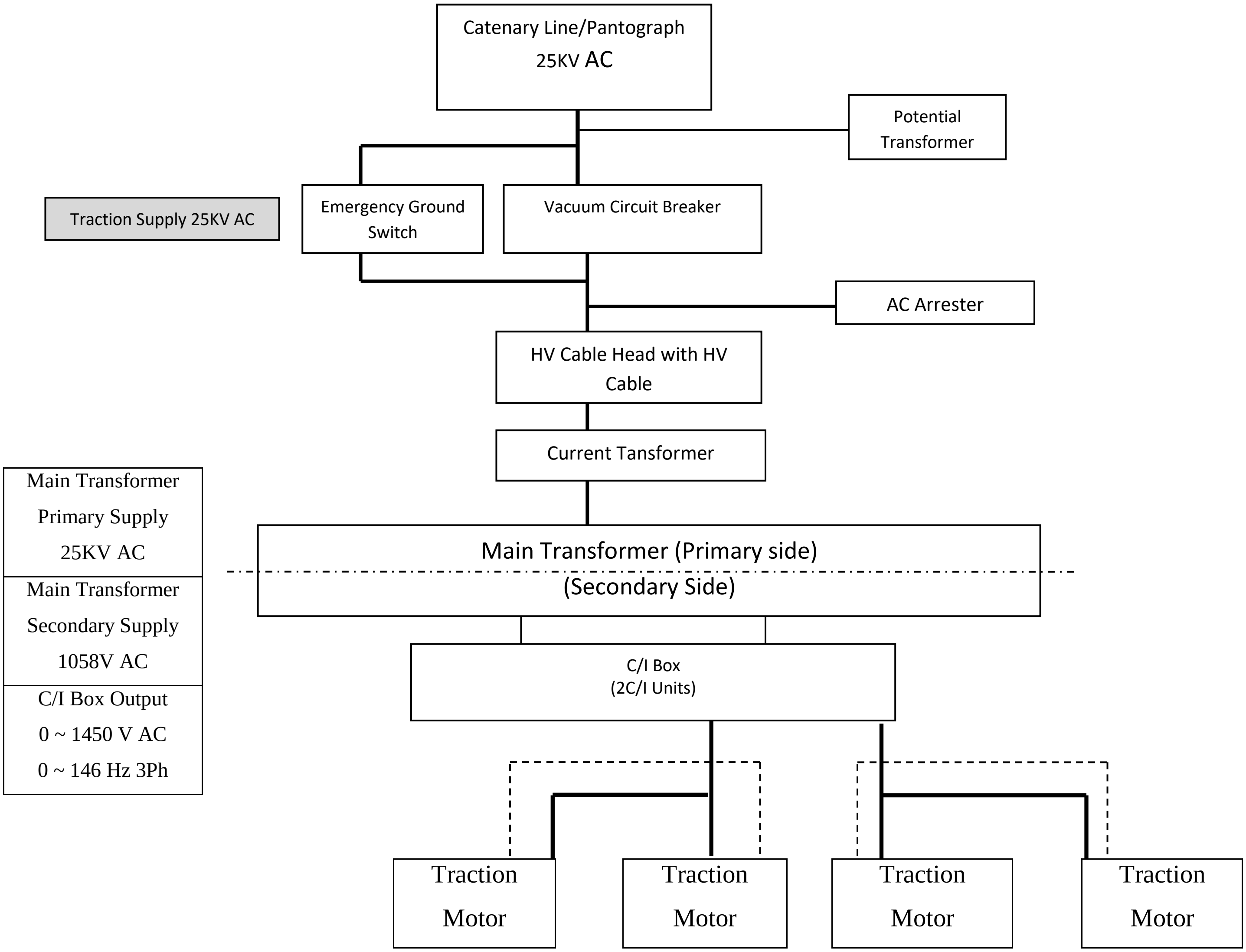


Fig.1.6: Traction circuit of loco-motive

1.6 Issues involved in Neutral section

a) Some instances have been observed when train negotiates neutral section in power consuming mode. Due to sudden current break, there is heavy flashing at section insulator of neutral section which results in to melting of droppers and runners.

b) Due to frequent opening or closing of Circuit breakers of locomotives while negotiating neutral section, periodic overhaul and maintenance needs of circuit breakers gets increased.

c) Due to increasing traffic, headway of trains needs to be reduced which demands more neutral sections. Increased number of neutral sections will increase number of operations of circuit breaker.

d) In driver less locomotives, operator is not available to monitor opening of circuit breakers.

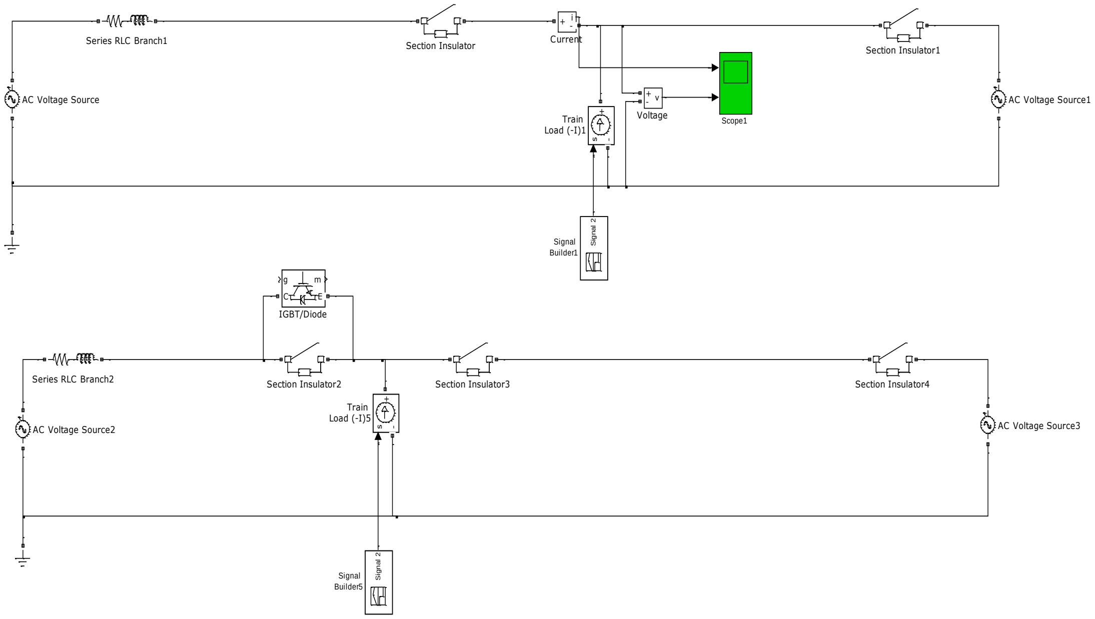


Fig.1.7: Comparison of conventional neutral section and SCNS

Above problems can be resolved by exploring alternate location of current break instead of Train circuit breaker. Switching time of such device should be less and adjustable as per train speed. Power electronics switch is explored in this report. With the switched neutral section using semi-conductor as switch for current break, opening and closing of train circuit breakers will not be required. Therefore no special arrangements, e. g. track magnets are required for train detection and also no signaling is necessary for instructing the loco driver to trip the main switch.

Another risk for the switch, which could occur, is short voltage peaks which can appear during turn-off. These voltage peaks are a function of the current which is turned off (dI/dt) and the inductance L of the electrical circuit. We counter this risk by two measures:

a) The semiconducting devices are only turned-off at zero-current transition.
b) The semiconductor is equipped with a snubber circuit which will protect the switch against voltage peaks.

Cyber attacks on Supervisory, control and data Acquisition (SCADA) system are not only on the increase, but have transitioned from speculative to indisputable. With the increasing number of connections between SCADA systems, corporate networks and the internet, combined with the move from proprietary protocols to more standardized and open solutions, they are becoming more susceptible to the kind of network attacks that are found more commonly in IT environments. Physical isolating systems and 'security by obscurity' is not longer enough to protect the system. Recommendations are detailed for rugged and reliable security gateway solution to detect threats and control access to critical components. Introduction

Supervisory, Control and Data Acquisition (SCADA) system has been used in power system for control and monitoring of power supply network. Power system automation consists of following main components:

a) Control
b) Measurement
c) Monitoring
d) Data communication.

In addition to power system, this system is also used at water treatment plants, Oil sector, industrial control system and building management system.

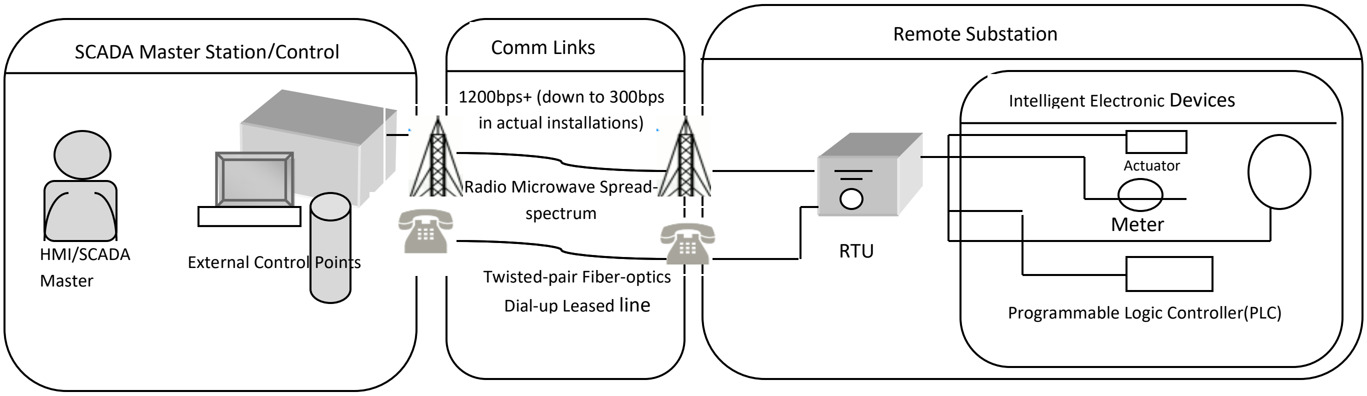

SCADA Master Station/Control
HMI/SCADA Master
External Control Points
Comm Links
1200bps+ (down to 300bps in actual installations)
Radio Microwave Spread-spectrum
Twisted-pair Fiber-optics Dial-up Leased line
Remote Substation
RTU
Intelligent Electronic Devices
Actuator
Meter
Programmable Logic Controller(PLC)

Fig.1.8: Basic architecture of a typical SCADA system

If any power supply failure occurs due to any problem in grid supply, power supply is switched over to alternate source promptly to maintain punctuality of trains. SCADA system involves:

i. **SUPERVISION:**

Traction Power Controller (TPC) supervises the receiving sub-stations, 25KV AC network as well as unattended 33KV/400V auxiliary sub-stations from OCC through SCADA system.

ii. **Control:**

Traction Power Controller (TPC) performs control operations of circuit breakers, interrupters, isolators and tap changers provided in different substations as per need.

iii. Data acquisition:

Process information is stored on a process database and a report database in the form of event list, alarm list, graphs and measurement reports.

An Operation Control Centre (OCC) is set up for Remote control of electric traction and auxiliary power supply. This is supervised and controlled by Traction Power Controller (TPC).

The entire Power Supply system is monitored and controlled locally as well as from the Operation control centre (OCC)

The entire power supply system with backup arrangements from alternative source for operation is to be monitored and controlled locally as well as from the Operation Control Centre (OCC) by Traction Power Controller (TPC). The Power Supply architecture is designed to ensure that any failure of any electrical equipment does not lead to any disturbance in Metro train services.

Fig.1.8 shows basic architecture of a typical SCADA system. There are 06 basic components of SCADA network :

a) Remote equipments : RTUs/IEDs/PLC
b) Communication interface between sensors/ relays/IEDs and remote equipment
c) Communication interface between Remote equipment and SCADA control centre
d) Master terminal equipment at SCADA control centre Communication interface between MTU and operator work-station
e) Communication interface between SCADA netwrk and corporate network

Attacks on SCADA network can be done at any of the above level. As mentioned above, SCADA system is used for critical applications. Hence, security of SCADA network has become an essential requirement. Cyber attacks on industrial. The most notorious incident that arguably propelled the vulnerability of SCADA network was the discovery of Stuxnet attack in June 2010, a weaponized form of malware. Stuxnet targeted the Natanz nuclear facilities in iran with great precision, causing nuclear centrifuge equipment to wear out at a vastly increased rate. Once a system has been “owned” such as a PLC, then new “ladder logic” can be uploaded. During the attack on Natanz with Stuxnet, it was reported that the controller logic was changed to cause the centrifuges to speed up / slow down rapidly [9].

According to PwC, the average number of detected incidences in the power and utility sector soared six fold in 2014-by far the highest reported by any industry [10].

In this para, vulnerable aspects of SCADA network have been identified and recommendations are made to protect the SCADA network from any undesired access.

I. SCADA SECURITY ISSUES

Historically, SCADA network was physically isolated from corporate network and internet. Due to following reasons, SCADA system is getting more vulnerable to threats:

A. Change of communication network from serial to Ethernet

Conventionally, communication network for SCADA was based on serial communication with no access to outside environment. Serial communication is lesser prone to security threats. With technological change and to get benefit of TCP/IP based protocols of higher bandwidth, higher response time and flexibility, communication network of new installations are based on Ethernet technology.

B. Adoption of open protocols

Earlier, proprietary protocols were being used for communication of field devices with SCADA control centre. Proprietary protocols were having advantage of limited knowledge of protocol structure to outside world but come at the cost of monopoly, higher cost and limited functions. With the adoption of open protocols, users got tremendous advantage of interoperability, standard functions and gateway solutions. However, new possibilities has opened for attackers to cause disruption of utility services.

C. Interface between IT environment and SCADA network

Now a days, some information of SCADA is shared on corporate network like intranet or SAP or maintenance/asset management system. Due to this, malwares which were commonly found on IT networks can be found on SCADA network.

Exploits are available on internet which is specific to vendor software for HMIs, SCADA masters, historians and other application software. Protocol specific exploits for Modbus, DNP3 and ICCP can be downloaded from internet [11]. Remote terminal unit (RTU) test sets, to issue commands toRTUs are commonly available on the market. The systems do not authenticate and have little to no data validity checking [12].

II. RISKS AND THREATS

Fig.1.9 shows Sources from which malicious code penetrates SCADA networks. Various parts of SCADA network is analyzed and following possible risks and threats are identified:

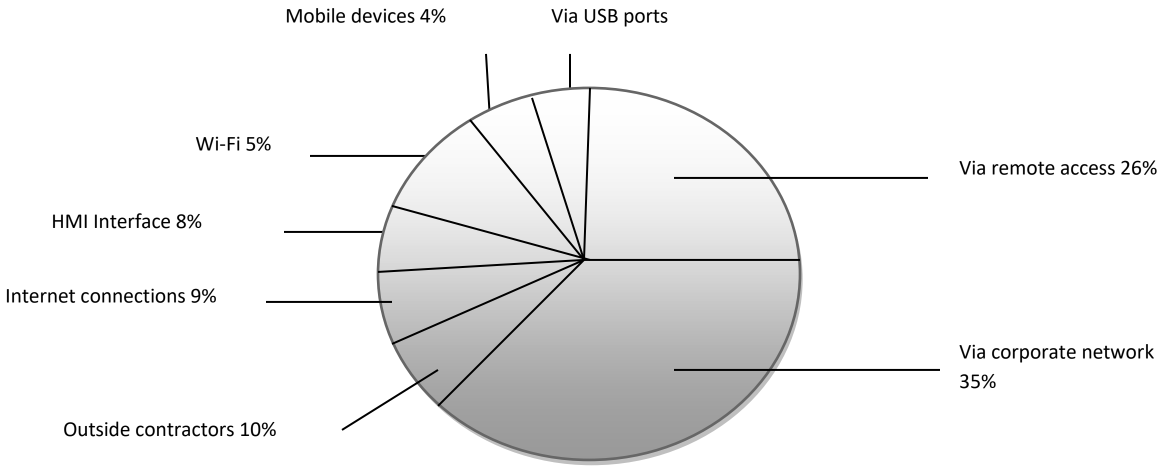


Fig.1.9: Sources from which malicious code penetrates SCADA networks

A. Substation Level

- Lack of physical security to RTU/PLC/bay controllers
- No door opening alarm of field devices
- Non-availability of CCTV surveillance of control room
- Use of default password for access to RTU/PLC/BCUs
- Lack of protection mechanism in Laptop used for configuration of field devices against virus/malware.
- Unencrypted Remote access given to OEM to check/modify device configuration.
- Non- updation of Security patches issued by OEM.
- Non- availability of Safety instrumented systems for critical commands.
- Unmonitored Changes in RTU/PLC/BCU.

B. Communication network

- Use of unprotected communication between RTU and control centre.
- Shared channel by different utilities of organization
- Unprotected interface between IT network and SCADA network
- Use of corporate network for communication.

C. Control centre

- Non-Availability of Antivirus software
- Security patches issued by operating system OEM is not installed.
- Interface between corporate network and SCADA network is not well secured.
- Internet connectivity
- Use of Conventional Firewall used for SCADA system which do not support SCADA protocols
- Default user ID and passwords are used by operator.
- Wireless communication between RTU and control centre.
- Accessibility to Unused ports.
- Lack of information for SCADA engineers on the state of technological network and processes
- Unmonitored Changes in SCADA software
- Use of external laptops for taking back-up
- Use of pen-drives for taking back-up
- Use of third party software on SCADA servers and work-stations.

- Use of obsolete operating systems for running SCADA applications
- SCADA system plays an important role to monitor functioning of neutral section. Security aspects of complete SCADA network starting from interface point to operation control centre is discussed in this report.

CHAPTER-2

2.1 GENERAL

This paper proposes automatic power changeover switch system applied superconducting fault current limiter (SFCL) of the Korea electric railway using 25 kV-AC Scott transformer [1] using thyristors but due to commutation problems of thyristors and need of SFCL to limit fault current.

The design is to research a device of locomotive auto passing neutral section which can test the coming of electric locomotives into Neutral Zone precisely, issue the corresponding signal to control locomotive power, detect the leaving of locomotive from the Neutral Zone, send out the corresponding signal to control the locomotive by electricity but there are still chances of going locomotive in charged section due to malfunctioning of control circuit or loco breaker failure

1) Paper under reference (1) discussed auto passing neutral section by making use of train borne and track borne equipments. As this technique involves operation of loco circuit branches, technique needs to be developed for auto passing neutral section without any need of opening or closing of loco circuit breakers.

2) Manuals under reference [2],[3] and [4] has covered design considerations of neutral section and power supply of 25KV traction system. Due to limitation of use of single transformer in TSS and disadvantages of conventional neutral section, alternative techniques needs to be explored.

3) Paper under reference [6] and [7] discussed various techniques to ensure equal sharing of voltage across the series connected devices in high voltage network. Voltage across switch while turn off needs to be simulated and snubber and gate control techniques needs to be employed for voltage balancing.

4) Paper under reference [8] has discussed for utility of SFCL for traction system to protect changeover switch system. Proposed configuration involved Scott connected transformer with neutral section at feeding post. Resistor type SFCL is used to reduce the magnitude of fault current during transient conditions.

   Further, it is required to study the response of power system during transient condition with parallel operation of transformers and neutral section in between two adjacent traction sub stations.

5) Paper under reference [9] and [10] discussed design and location of SFCL for reduction of magnitude of fault level. SFCL is simulated for 25KV AC traction system.

6) Paper under reference [11], [12] , [13] and [14] has discussed risks and threats of SCADA system. Vulnerability assessment has been done to fix attack prone areas in SCADA system of 25KV AC traction system.

7) Paper under reference [15] to [20] have discussed remedies of different types of SCADA network and protocols. 25KV AC traction system is based on principle of distributed intelligence which sends data to control centre on wide variety of protocols. Most of the Substations are unmanned as permitted by CEA2010 and DERC regulations. This demands greater focus on physical security also which is monitored by SCADA system. Remedies of SCADA security are discussed in this report in details.

CHAPTER-3

Modeling of system

3.1 General

Simulation of Semiconductor commutated neutral section (SCNS) with superconducting fault current limiter (SFCL) is done to address following issues of 25KV neutral section:

a) Switching operations of train circuit breakers are avoided while negotiating of train through neutral section.
b) Arcing between pantograph and overhead conductor is prevented.
c) Need of sensing circuits for VCB opening and closing are eliminated.
d) During peak hours, it is possible to do parallel operation of traction transformers with reduced fault level.

3.2 System Configuration

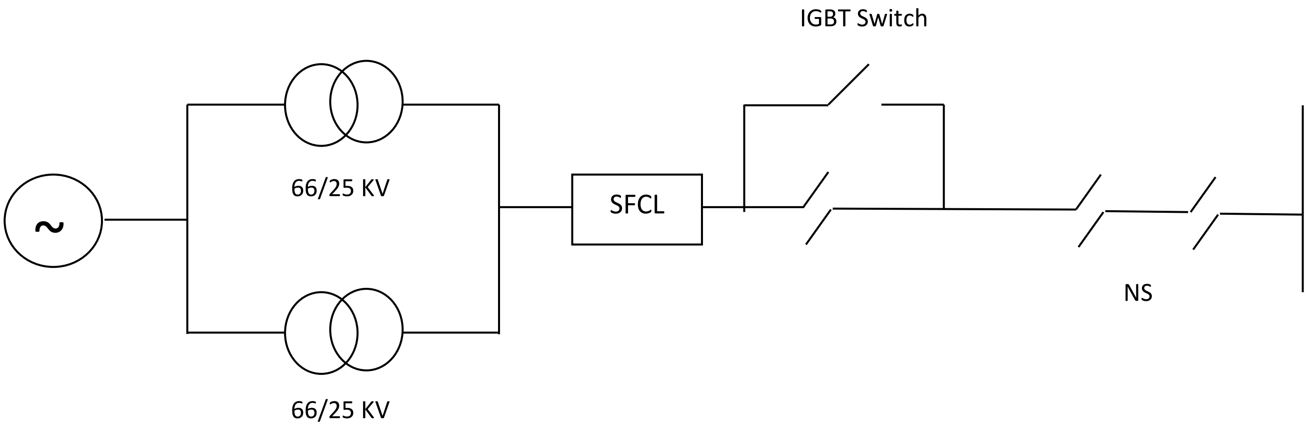


Fig.3.1: System Configuration

Proposed system configuration is shown in the above fig.3.1

Both traction transformers are simulated in parallel configuration.

3.3 Functional Principle of SCNS

The SCNS switching device consists of the semiconducting switch and its controller. Series connected IGBTs are connected in series with conventional neutral section. The switch is normally on, that means the device is closed all the time until a train is arriving at the section insulator of the system as shown in fig.3.2

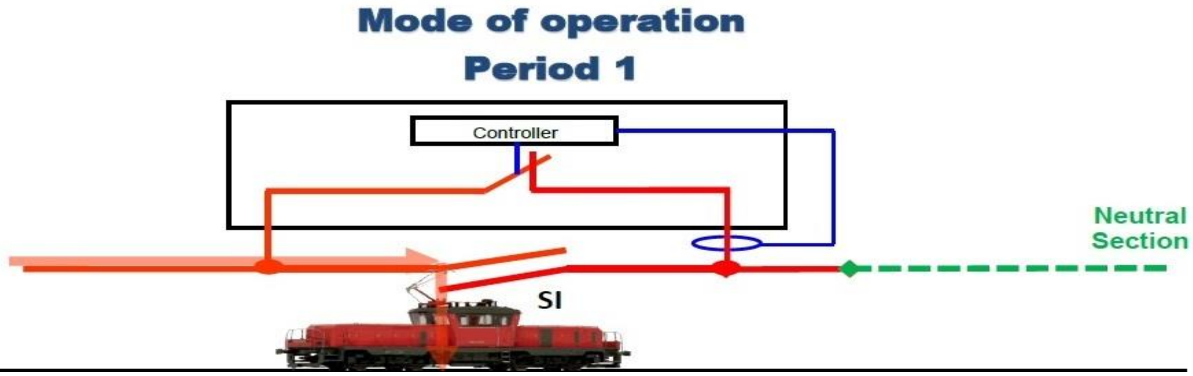


Fig.3.2: Function Principle of SCNS

As soon as the train pantograph has passed the SI a current is flowing through the closed switch and will be detected by the current probe as shown in fig.3.3. Then a signal is transmitted to the controller for opening the semiconducting switch. By that, the current is interrupted and the train can enter into the neutral section without any current consumption.

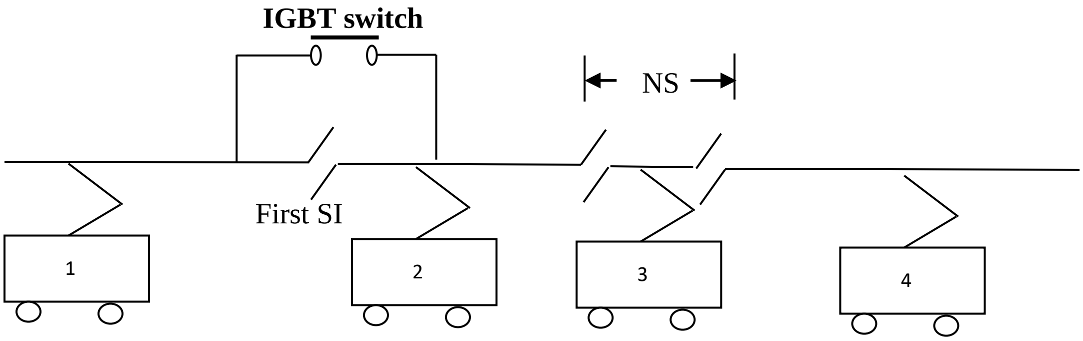


Fig.3.3: Neutral Section

	Switch Position
When train is before Neutral Section (1)	ON
Train Crosses SI	ON
Train in SCNS Zone (2)	OFF
Train in NS Zone	OFF
Train crosses Neutral section (4)	ON

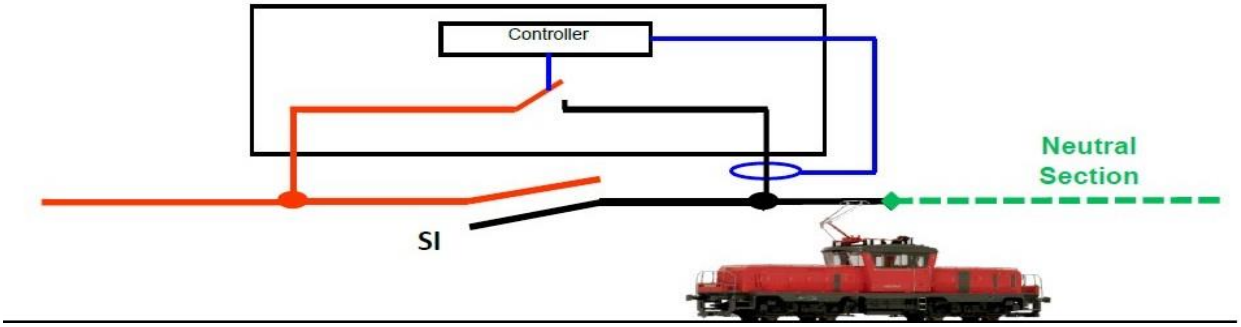


Fig.3.4: Function Principle of SCNS

After the train passed the neutral section the switching device has to be reset in its normally-on position before the next train is arriving. The trigger time to reclose the switch is determined by the length of the neutral section and the speed of the train and is set in advance.

3.4 Functional Principle of SFCL

Superconducting fault current limiter is a device which has virtually zero resistance under normal operating conditions but involves rapid loss of super-conductivity in the occasion of a short circuit, which limits the current more rapid and effective way. Fault current limiter depends on their nonlinear response to current, temperature and magnetic field variations (as shown in fig.3.5) and causes a transition between and normal conducting state to the superconducting state.

Material used for superconductor Nbti, BSCCO-2212, YBasCu077K

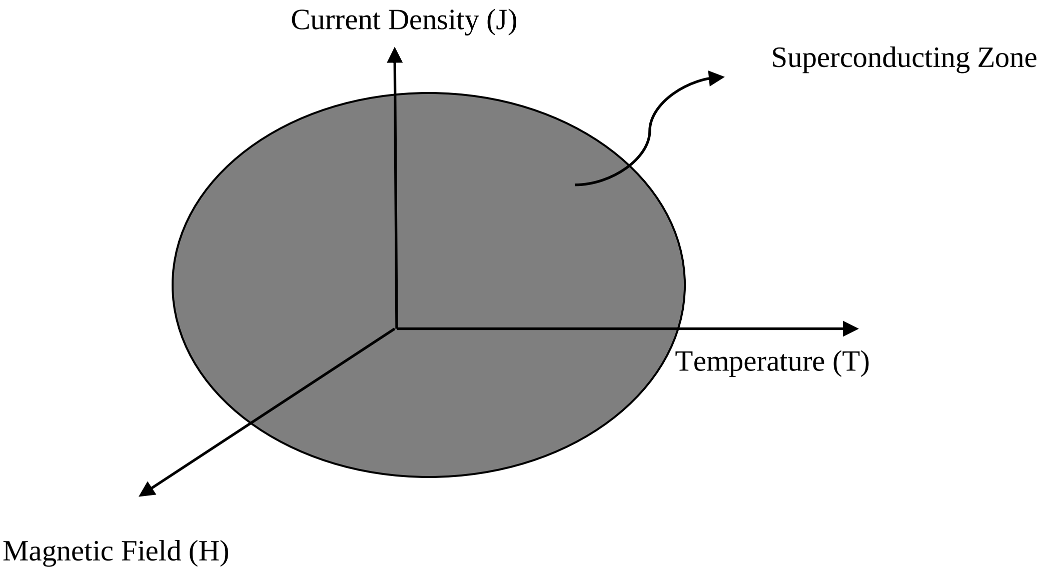


Fig.3.5: Characteristics of superconductor material

The qualifications of SFCL are:

a) Very low impedance during normal operation.
b) High impedance system during short-circuit.
c) SFCL has the quality of fast operation characteristics of within one fourth of cycle.

Whereas response time of modern protection system is of the order of 4 to 6 cycles

1) Sensing time of Relay = 20ms
2) Switching of Relay trip contact = 10ms
3) MTR operation time = 10ms
4) CB trip time = 40ms

Total = 80 msec

There are two types of SFCLs available in marker : Resistive type and inductive type. Resistive type FCL is considered for 25KV AC traction system as inductive type FCL may cause sub-synchronous resonance with system under certain loading conditions. Moreover inductive type FCL is much bigger and heavier than that of resistive type.

Location of SFCL

An introduction of resistance may disturb the impedance relay characteristics of distance protection installed in traction substation during fault, hence SFCL is installed at the 25KV bus (after 25KV circuit breakers).

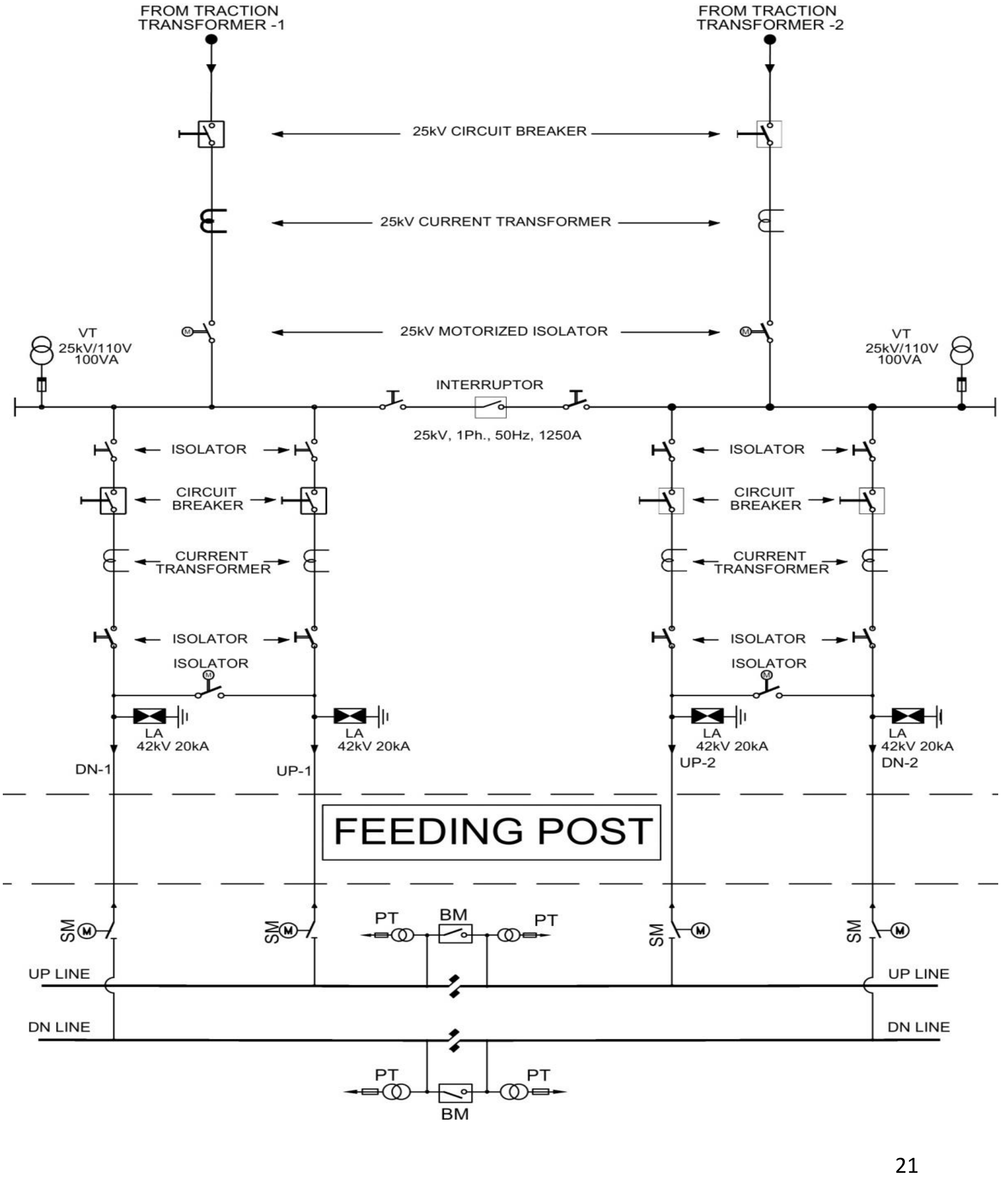


Fig.3.6: Sectioning diagram of Traction Sub-station

With SFCL, backup protection installed at 25KV incomer needs to be equipped with voltage dependent over current (VDOC). Due to VDOC component, reduction of fault current will not cause any difference in relay tripping analysis.

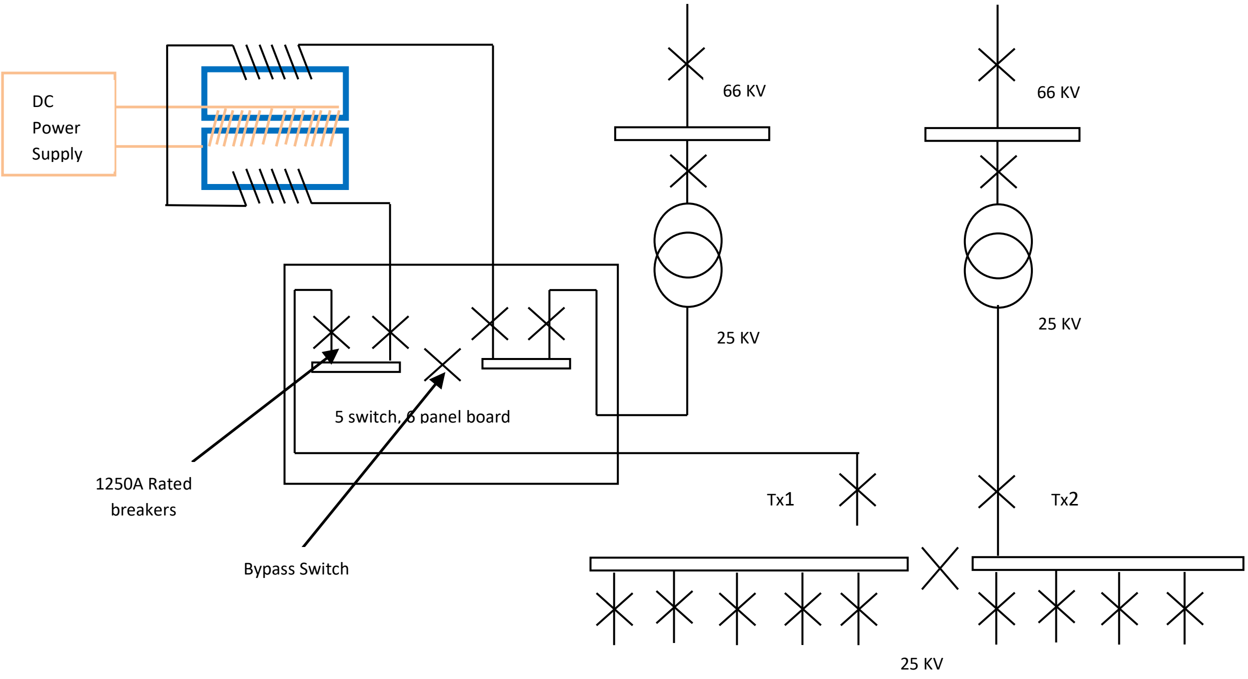


Fig.3.7 Location of SFCL

Main drawback of using SFCL is its high cost, cooling requirement, emit strong magnetic field and cause steady power dissipation losses due to hysteresis. Superconducting elements are required to be cooled to dissipate power looses. Hence, Cryogenic compressors are employed along with water chillers for cooling purpose.

SFCLs is proposed to be provided using bypass switch so that during normal conditions SFCL will run on bypass mode so to avoid its running cost. When feed is extended, bypass switch will open and close the SFCL switch as shown in fig.3.7 with activation of its cooling mechanism.

3.5 Calculation of RCD Snubber circuit of SCNS

07 Strings of 6.5 KV IGBTs are connected in series.

S/N	Parameters	Value
1	Rated Collector Emitter voltage	6.5 KV
2	Rated Current	750 A
3	Peak Current	1500 A
4	Isolation Voltage	10.2 KV

Passive snubber using resistor-capacitor-diode (RCD) is used in parallel with series connected IGBTs for transient sharing. The presence of large capacitor reduces the voltage imbalance but increases commutation time of device and snubber power loss. [3]
As SCNS application requires less switching operations (600 in a day), Snubber power loss is very less. Calculation of Snubber capacitance & resistance is as follows:

A) Calculation of Snubber Capacitance

$$C = \frac{I_L t_f}{2V_S}$$

I_L = Max Current (considered as 1000 Amperes in case of fault at neutral section)

t_f = Turn off time (5520 ns for 6.5KV IGBT)

V_s = Voltage across IGBT (6000V)

$$\frac{30 \text{ X } 1.414}{7} = 6.06\text{KV}$$

$$C = \frac{1000 \text{ X } 5520 \text{ X } 10^{-9}}{2 \text{ X } 6.06} = 440\ \mu\text{f}$$

B) Calculation of Snubber Resistance

$$R = \frac{2}{t_{ON\ min}\,C_S}$$

$= 85 \text{ X } 10^9\Omega$

3.6 Matlab simulation of ASNS

To fulfill bidirectional switching ability of the high voltage semi-conductor device, IGBT strings of 6.5KV rating in 7 numbers are connected in series. A snubber capacitor of 440µf is connected in parallel with each IGBT to limit the turn-off dv/dt. Using 440µf capacitor in RCD snubber, voltage stress during switching is well below the allowable limit of 10KV/mS.

Train issues with semiconductor switch in 25KV network are to maintain voltage balance across the device, dv/dt transients and isolation of gate signal from power line.

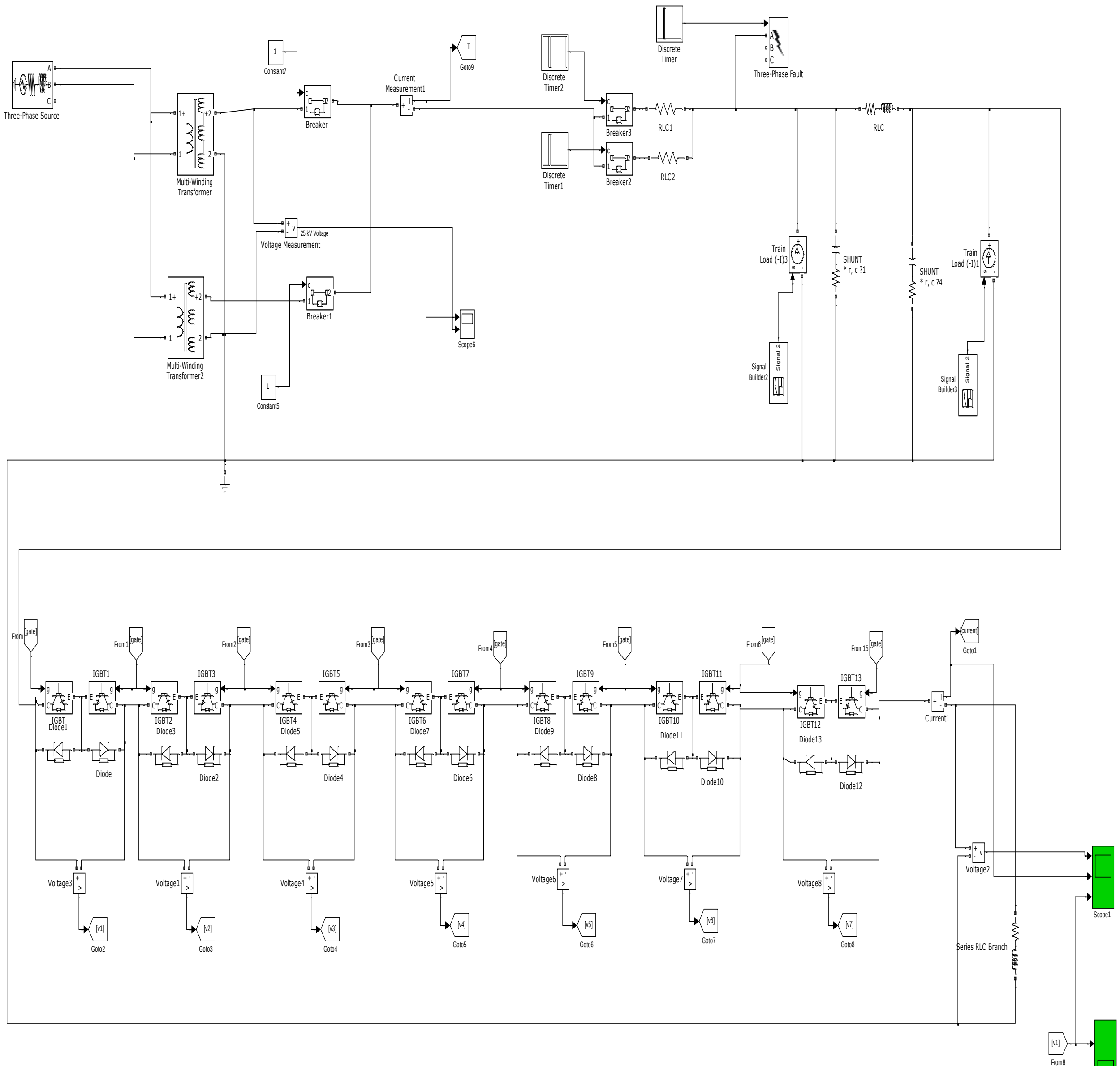


Fig.3.8: Matlab simulation of ASNS

3.7 Gate Control Circuit of Matlab

Basic considerations in designing gate control circuit is as follows :

a) During normal conditions, IGBT switch should be ON condition.

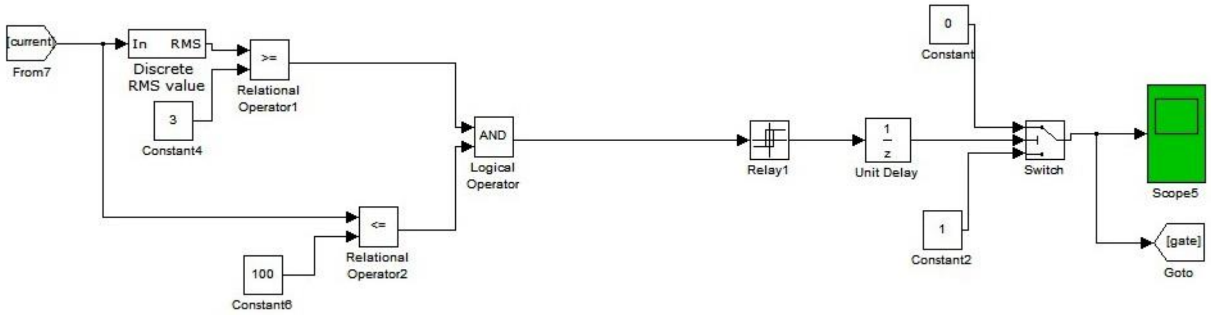


Fig.3.9: Gate Control Circuit of Matlab

b) When train comes in the zone of first section insulator, appreciable value of current is measured by current transformer due to withdrawal of load current by train through IGBT switch as shown in fig.3.2. But instantaneous opening of IGBT switch is avoided so as to ascertain crossing of section insulator otherwise it would cause flashing at first section insulator as shown in fig.3.3. Hence a delay of 01 sec is kept in opening of IGBT switch after current is sensed by current transformer.

Train may enter neutral section in coasting mode or motoring mode with current intake of 3Amps to 50 Amps respectively. So sensing circuit should be configure in the range of 3 A to 50A.

c) As soon as train crosses SCNS zone and comes in the zone of neutral section, current sensed by current transformer becomes zero. Hence IGBT switch should be switched ON for next operation.

d) Loco circuit breaker has an under voltage tripping of 2 seconds. Hence non availability of supply for less than 02 seconds would not cause under voltage tripping of loco circuit breaker and operations of circuit breaker can be avoided.

e) The actual Neutral section is composed of two NS25 with earth in the middle (see above).Thus it has a length of 11.3 meters. To cross 11.3 metres within a delay of 1.5 seconds, permissible train speed is 7.5 m/sec or 27 Km/hrs.

f) There are 04 pantographs in one train. Considering maximum speed of train, second pantograph will hit the point after 02 seconds of passing the first pantograph. Hence IGBT switch should not be kept off for more than 02 seconds. When first pantograph passes the neutral section, IGBT will be switched off for current break across IGBT and switched on within a max period of 2 seconds..

Gate control circuit of IGBT controller is as shown in fig.3.8. When current sensed by current probe is in between 3Amps to 50 Amps, AND operator shown as above cause deactivation of gate signal with a time delay of 01 second to turn off the IGBT. When train crosses SCNS zone and comes in the zone of neutral section, due to zero current, gating signal is removed by gate operator to turn on the IGBT.

3.8 Experimental Results

Train logs of neutral section detection time, opening time of loco circuit breaker and closing circuit breaker taken at various speeds to tune the turn off period of IGBT switch:

S.No.	Speed	Neutral Section detection time	Opening time of loco circuit breaker	Closing time of loco circuit breaker
1	69.5	19.02.29	19.02.31	19.02.35
2	60	19.48.23	19.48.26	19.48.30
3	49	22.07.13	22.07.15	22.07.20

Simulation is carried out to check the non availability of voltage supply in the train and comes out to be 0.9 seconds (0.4 seconds and 0.5 seconds to cross 6.6m neutral section) which is far less than permissible value of 02 seconds as stipulated in point no. 3.7 d. Hence opening and closing of loco circuit breakers can be prevented when train will pass dead zone of neutral section.

Secondly, switch off period of IGBT is 0.4 seconds which is less than permissible value of 2 seconds as stipulated in point no. 3.7 f.

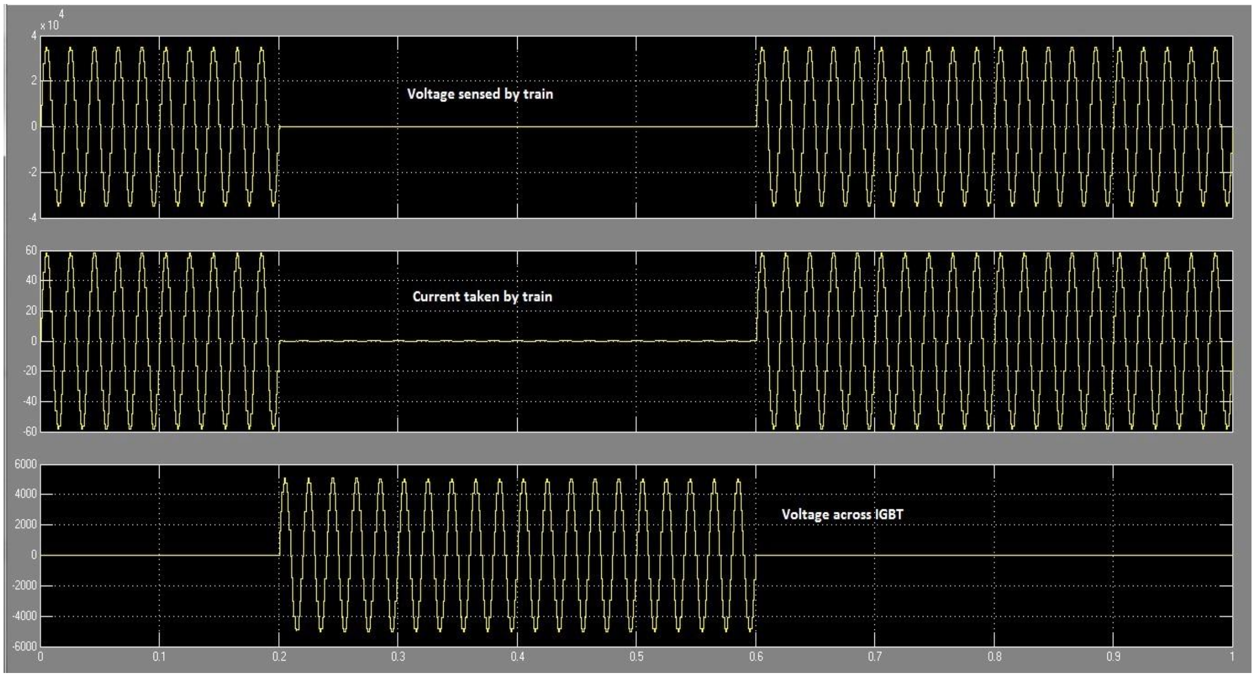


Fig.3.10: Experimental Results

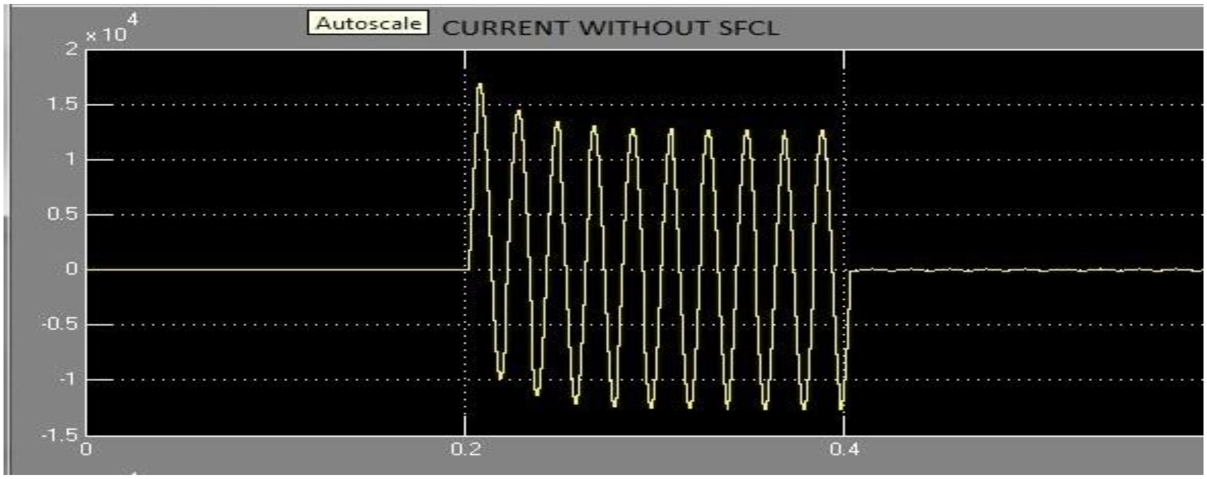


Fig.3.11: Current without SFCL

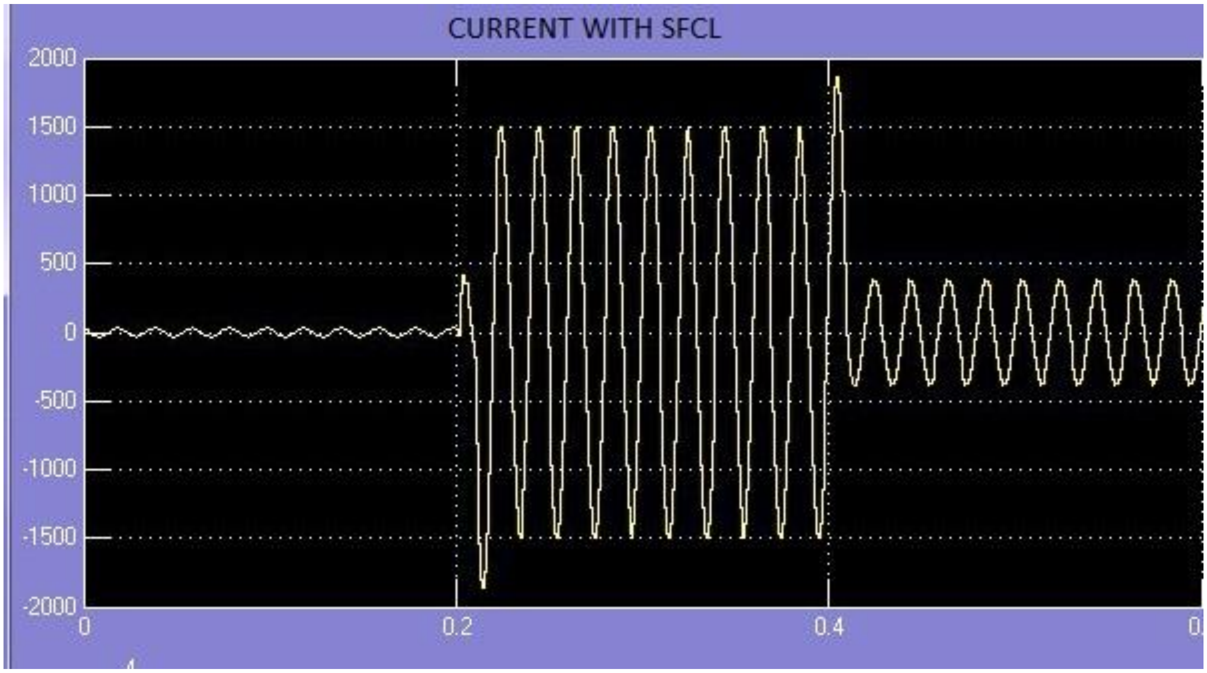


Fig.3.12: Current with SFCL

3.9 Risk assessment of Proposed arrangement and remedies:

a) Supply of IGBT switch is proposed to be fed using one auxiliary transformer of 25KV/110V AC protected by HV fuse. In case of any fault in transformer or blowing of HV fuse, supply to IGBT controller will stop working. During such scenario, if train will pass the neutral section, there will be huge flashing due to sudden current break of 50amps across OHE and pantograph and may cause severe damage to OHE.

Remedy: Following indication needs to be monitored on real time basis through SCADA :

- Status of the system
- Temperature
- Current flowing through the switch
- Voltage over the switch.

In case, status of system become faulty, information should be transmitted to operation control centre through SCADA. SCADA server shall automatically execute command message to signaling system to start opening and closing of loco circuit breakers as per old scheme.

b) In India the ambient temperature goes up to 50 degrees during summer and in fact the temperature of metallic container on sunny days during summer goes up to 70-75^{0}C, the performance of IGBT can become a critical issue.
Remedy : The switch should be composed of a GRP-housing and a sunshade and tested for ambience of 75 degree. In case, temperature of system increases more than designed limit, information should be transmitted to operation control centre through SCADA to alert maintenance team.

CHAPTER-4

SCADA SECURITY REMEDIES

A test setup as shown in fig 4.1 consisting of RTU, signal simulator, communication unit, firewall and SCADA MTU (server) is prepared to check the transmission of logs. Softwares RTUtil, CTTP6.0 and COMPROT is used to analyze the messages. Firewall of CISCO model no. ASA 5510 is used between RTU and server to prevent unauthorized access.

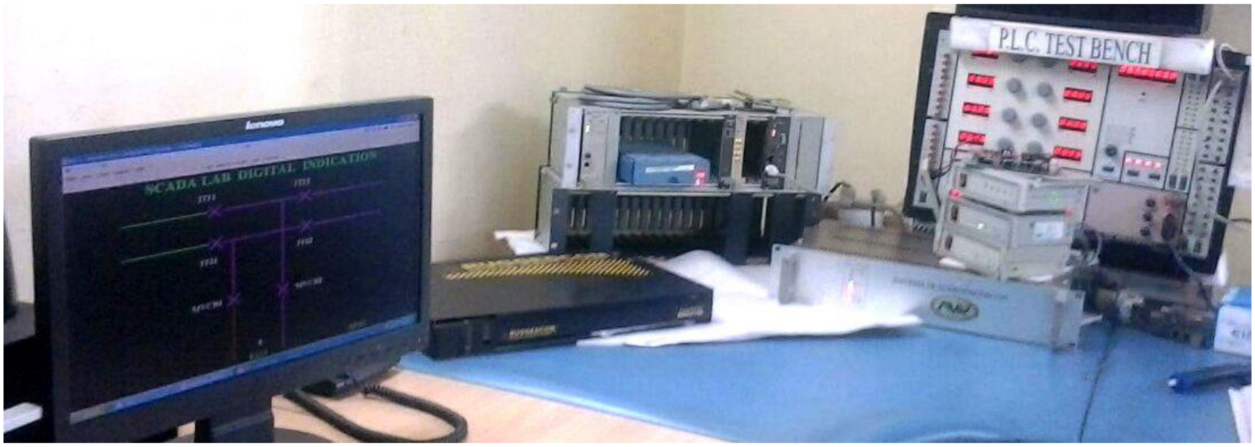


Fig.4.1: Test Setup to check/simulate SCADA message

A. Firewall at RTU level

Providing secure protection just before the substation equipments i.e. at RTU/PLC end is an effective solution to prevent unauthorized access. A firewall is a device or software capability designed to allow or deny network transmissions based upon a set of rules. The protocol-based whitelist method is related to the application layer (up to layer 7) and deals with various SCADA protocols, such as Modbus, DNP3, IEC 60870-5 series, ICCP, IEC 61850 and proprietary protocols [17]. Firewall configuration should support specific protocol used for RTU so that communication other than master slave communication is not permitted and an alert message is generated. Some of the utilities make use of engineering work-station to configure RTU/PLC/IED remotely. Where remote access is used, Remote access should be available to specific engineering work-station of configured IP address as well as Mcaddress in firewall so that no access is given other than engineering work-station.

Typical configuration (relevant settings shown below) of firewall involves defining IP address as well as Mcaddress of servers installed in control centre.

```
outside 173.18.0.122             0004.a52a.15e5 181
```

```
        outside 173.18.0.114                0004.a52a.1507 241
```

Above configuration ensures that attacker trying to change RTU configuration using same IP will be denied access due to different Mc address.

B. Exploit Management

Exploits are malformed data file designed specifically for a software or protocol to deteriorate its performance. Hence in addition to antivirus and antispyware signatures, software should be able to detect and block exploits. For this, frequent patching of system is essential.

C. Patch Management

Patch Management should be part of regular maintenance activities. This includes patching of Operating system, DBMS application software and upgradation of RTU software. A tie- up should be done with software provider to give security patches on regular basis. Patches should be examined on standalone system before installing in to real systems.

D. Antivirus Management

Even if the system is isolated from other networks, it is essential to provide antivirus software in each computer. Rather than taking online updates, it is better to update offline by using CD. CD should be scanned in a standalone system before installing virus definitions in the SCADA computer. Launching of unwanted software should be blocked by antivirus software.

E. Physical Access

Locking system is provided in RTUs to prevent unauthorized access. Door Opening alarm should be available in RTU's to improve security of SCADA system further. CCTV surveillance should be provided for all equipment rooms to prevent internal attack.

F. Use of safety Instrumented system (SIS) for highly critical applications

As a second line of safety, SIS should be introduced at the equipment level for critical equipments. SIS are independent of SCADA control circuits and can override the SCADA command which may cause unsafe situation so as to maintain failsafe condition. For example, electrical/mechanical interlocks may be deployed in command circuit of SCADA. If any unsafe command is received from SCADA, interlocks shall come in to picture.

G. Set user interface restrictions

It is necessary to restrict user actions performed via Windows interface. It is required to disable such hotkeys as Ctr+Alt+Del, Alt+Esc, Alt+Tab, Ctl+Esc [17].

H. Password Management

Search engines used by hackers get access of device easily which are still operating on factory settings, with generic passwords and login details. Default passwords of OEM should be changed. All the operators and maintenance engineers should be asked to replace their password on regular basis for which password change reminder may be set [5]. User-IDs of Ex-employees should be deleted.

I. Configuration logs of RTU/PLC/BCU

With the introduction of communication network, it has become possible to access configuration data of field devices from remote without actually visiting the site. Any modification in configuration can be communicated to control centre. System administrator should keep a watch on any changes in the configuration file. If any unexpected change is noticed, the respective device should be taken out of service immediately till further investigation.

J. Compliance to security standards

The software and hardware should atleast meet the NCSC class C-2 rating.VPN protocols (PPTP, IPSec, L2TP) should be considered for communication and substation RTUs and IEDs [13].

Software should be validated from National cyber security organization.

K. Disable unused ports and services

Unused USB ports and CD-ROMs should be disabled to prevent any intrusion due to usage of pen-drives.

L. Application control mechanism

Application control mechanism includes

- Start-up and control of applications as per blacklisting policy
- Control of application access to operating system resources : files, folders, system registry etc
- Control all types of executable that run in a windows environment, including: exe, dll, ocx ,drivers, scripts, command line interpreters and kerenel mode drivers.
- Update application reputation data

M. Ensure safe custody of design documents:-

Design documents, Input/ Output list, RTU configuration should be kept in safe custody. Old backups kept in CD/DVD/tape drive/hard disks etc should also be kept in safe custody. Online upkeep of records should be avoided.

N. Use of third party software

Softwares other than SCADA and DBMS software should not be kept on MTUs and operator work-stations. This will prevent malicious activity in MTUs to a great extent.

O. Anamoly detection

Even after taking preventive steps, SCADA administrator should monitor the system for any unauthorized activity. Anomaly detection requires a detailed analysis of data logs and correlation of detected anomalies events. Intrusion detection techniques are developed for the identification of unauthorized activities and event correlation based on data and information [18].

Algorithms should be developed in SCADA software so that any change in system configuration should create a log which should be monitored by security team round the clock. Any change in RTU/PLC/BCU configuration should send an alarm to control centre for security team. If any unauthorized activity is noticed, respective RTU/PLC/BCU should be taken out of service.

P. Implement frequent audits

Security Audit should be conducted at an appropriate frequency. Third party audits are recommended for security controls and its effectiveness. Use of automated tools is recommended in audits. Audits should include application and network security vulnerability assessments with penetration testing. IBM App scan , web inspect, qualysguard and nessus are some of the world class tolls for testing. Conduct regular VAPT (Vulnerability assessments and penetration test) using capable tools and ensure that systems are immune to known attacks like network sniffing replay, denial of service (DoS), man in the middle attack and remote code execution [11]. Security events that are logged include individual user log-in, log-out, change of parameters or configurations, and updates to software or firmware. For each event, date and time, user, event ID, outcome and source of event are logged. Access to the audit trail is available to authorized users only [19].

Q. Firewall at RTU communication interface of server room

This will address the security issues of communication interface between RTU and server. Firewall should support respective protocols of SCADA network with a sole purpose to prevent any third party system in to control centre network.

Firewalls are available from leading vendors which are compatible to SCADA protocols. Typical configuration (relevant settings shown below) of firewall involves defining RTU address communicating on IEC-104 protocol :

```
access-list Soft extended permit 104 any any        (To permit RTUs of IEC-104 protocol)

access-list Allow19 extended permit 38 any any    (RTU address – 38)
```

R. Firewall at interface point of corporate network and SCADA network

Firewall should be placed at interface point of corporate network and SCADA network.

Firewalls properly configured, can protest passwords, IP addresses, files and more. However without a hardened operating system, hackers can directly penetrate private internal networks or create a denial of service (DOS) condition, rendering the firewall useless [21].

Logs generated by firewall should be analyzed. A typical log generated by firewall under test setup is as below :

```
ICMP echo request from outside:173.18.0.7 to inside:173.18.0.30 ID=512 seq=5766 len=32
ICMP echo reply from inside:173.18.0.30 to outside:173.18.0.7 ID=512 seq=5766 len=32
ICMP echo request from outside:173.18.0.7 to inside:173.18.0.30 ID=512 seq=6022 len=32
ICMP echo reply from inside:173.18.0.30 to outside:173.18.0.7 ID=512 seq=6022 len=32
ICMP echo request from outside:173.18.0.7 to inside:173.18.0.30 ID=512 seq=6278 len=32
ICMP echo reply from inside:173.18.0.30 to outside:173.18.0.7 ID=512 seq=6278 len=32
ICMP echo request from outside:173.18.0.7 to inside:173.18.0.30 ID=512 seq=6534 len=32
ICMP echo reply from inside:173.18.0.30 to outside:173.18.0.7 ID=512 seq=6534 len=32
ICMP echo request from outside:173.18.0.7 to inside:173.18.0.30 ID=512 seq=6790 len=32
ICMP echo reply from inside:173.18.0.30 to outside:173.18.0.7 ID=512 seq=6790 len=32
ICMP echo request from outside:173.18.0.7 to inside:173.18.0.30 ID=512 seq=7046 len=32
ICMP echo reply from inside:173.18.0.30 to outside:173.18.0.7 ID=512 seq=7046 len=32
ICMP echo request from outside:173.18.0.7 to inside:173.18.0.30 ID=512 seq=7302 len=32
ICMP echo reply from inside:173.18.0.30 to outside:173.18.0.7 ID=512 seq=7302 len=32
ICMP echo request from outside:173.18.0.7 to inside:173.18.0.30 ID=512 seq=7558 len=32
ICMP echo reply from inside:173.18.0.30 to outside:173.18.0.7 ID=512 seq=7558 len=32
ICMP echo request from outside:173.18.0.7 to inside:173.18.0.30 ID=512 seq=7814 len=32
ICMP echo reply from inside:173.18.0.30 to outside:173.18.0.7 ID=512 seq=7814 len=32
ICMP echo request from outside:173.18.0.7 to inside:173.18.0.30 ID=512 seq=8070 len=32
ICMP echo reply from inside:173.18.0.30 to outside:173.18.0.7 ID=512 seq=8070 len=32
```

S. Policies and procedures:-

Different interests and compliance with legislative and contractual requirements could make it necessary to define a security policy structure using different security domains inside the power utility [20].

There should be a strong cyber security policy covering all aspects. Responsibility of each team member should be clearly defined in policy.

T. Remote access

Remote access is generally given to OEM to troubleshoot the problem in the software. It should be ensured that remote access should be given using secured gateway. Wherever possible, use of internet in SCADA network should be restricted to prevent any intrusion/hack attempt through web.

U. Wireless communication between RTU and OCC

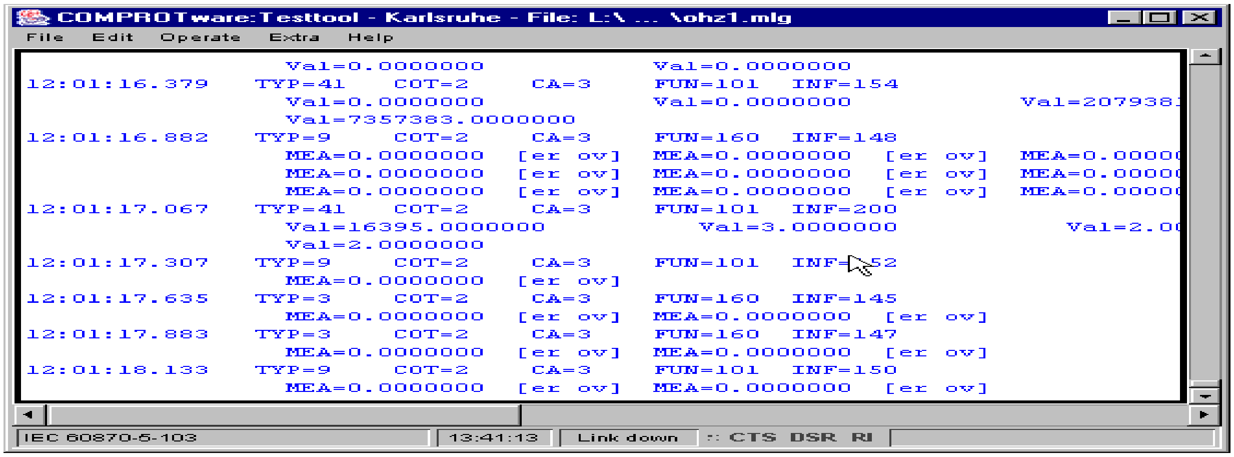
In case of wireless networks, deploy measures to restrict the access: Disabling of service, set identifier broadcast, Change of default passwords, turning on of Wi-Fi protected access, use of secure wireless routers, control of transmitter power, and turning off network when not in use [21].

V. Software Upgradation

There are some SCADA applications which are still running on older operating systems like Win XP, Win 2000. Security patches from these OS are no longer available. Hence, timely upgradation of OS is also essential.

VIII. RESULTS AND DISCUSSIONS

Protocol stacks of open protocol are publicly available. Fig.4.2 shows protocol messages of IEC-60870-103 protocol. If communication access become available to intruders, it will not be much difficult for them to manipulate messages.

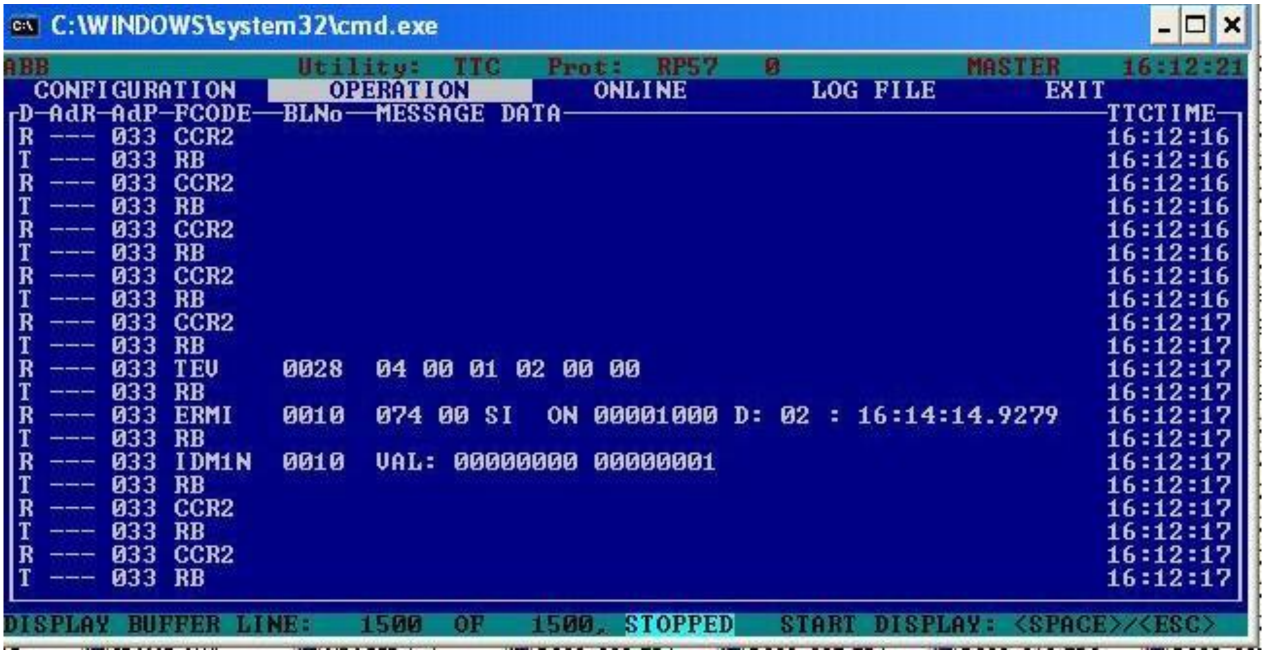


```
                        Val=0.0000000                      Val=0.0000000
12:01:16.379        TYP=41      COT=2       CA=3       FUN=101    INF=154
                        Val=0.0000000                      Val=0.0000000                      Val=2079381
                        Val=7357383.0000000
12:01:16.882        TYP=9       COT=2       CA=3       FUN=160    INF=148
                        MEA=0.0000000   [er ov]   MEA=0.0000000   [er ov]   MEA=0.00000
                        MEA=0.0000000   [er ov]   MEA=0.0000000   [er ov]   MEA=0.00000
                        MEA=0.0000000   [er ov]   MEA=0.0000000   [er ov]   MEA=0.00000
12:01:17.067        TYP=41      COT=2       CA=3       FUN=101    INF=200
                        Val=16395.0000000                     Val=3.0000000                      Val=2.00
                        Val=2.0000000
12:01:17.307        TYP=9       COT=2       CA=3       FUN=101    INF=152
                        MEA=0.0000000   [er ov]
12:01:17.635        TYP=3       COT=2       CA=3       FUN=160    INF=145
                        MEA=0.0000000   [er ov]   MEA=0.0000000   [er ov]
12:01:17.883        TYP=3       COT=2       CA=3       FUN=160    INF=147
                        MEA=0.0000000   [er ov]   MEA=0.0000000   [er ov]
12:01:18.133        TYP=9       COT=2       CA=3       FUN=101    INF=150
                        MEA=0.0000000   [er ov]   MEA=0.0000000   [er ov]
```

```
IEC 60870-5-103 | 13:41:13 | Link down | :: CTS DSR RI
```

Fig.4.2: Results and Discussions

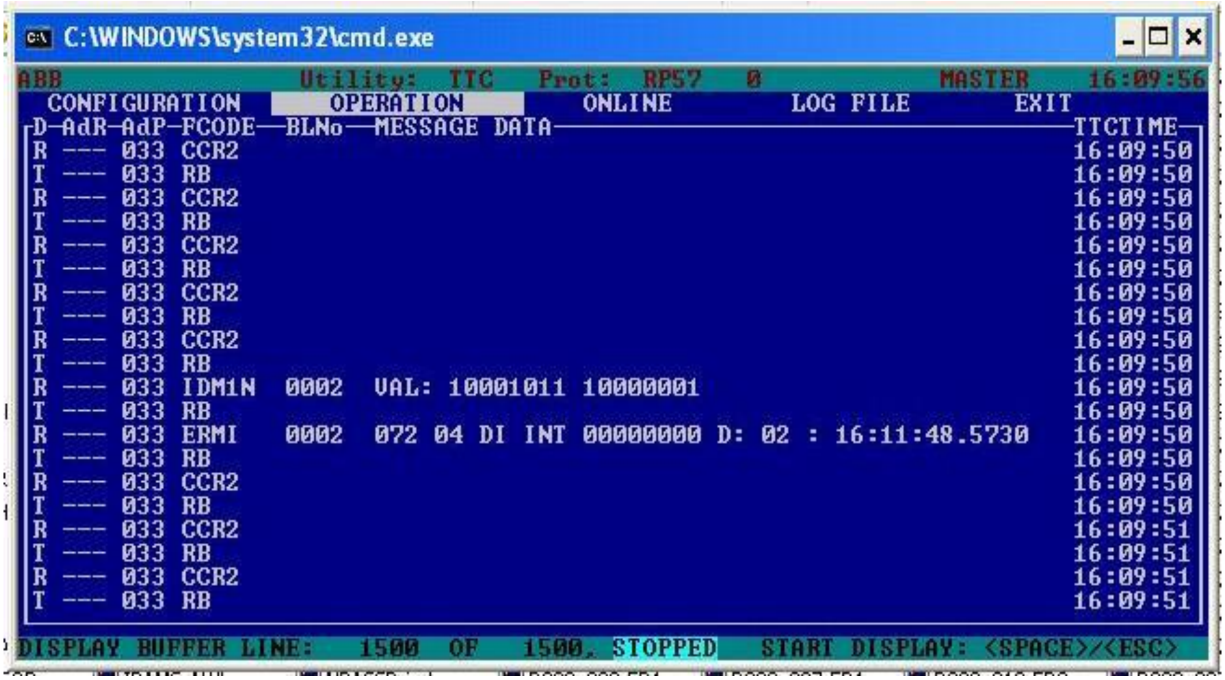
Fig.4.3 shows transmission logs of RTUs of ABB make analyzed by RTUtil software. Fig.4.3 shows transmission of logs when command for opening of 25KV breaker is executed from control centre :



```
ABB              Utility:  TTC    Prot:  RP57   0              MASTER    16:12:21
D-AdR-AdP-FCODE--BLNo--MESSAGE DATA--------------------------------------TTCTIME-
R ---- 033 CCR2                                                          16:12:16
T ---- 033 RB                                                            16:12:16
R ---- 033 CCR2                                                          16:12:16
T ---- 033 RB                                                            16:12:16
R ---- 033 CCR2                                                          16:12:16
T ---- 033 RB                                                            16:12:16
R ---- 033 CCR2                                                          16:12:16
T ---- 033 RB                                                            16:12:16
R ---- 033 CCR2                                                          16:12:17
T ---- 033 RB                                                            16:12:17
R ---- 033 TEV     0028   04 00 01 02 00 00                              16:12:17
T ---- 033 RB                                                            16:12:17
R ---- 033 ERMI    0010   074 00 SI   ON 00001000 D: 02 : 16:14:14.9279  16:12:17
T ---- 033 RB                                                            16:12:17
R ---- 033 IDM1N   0010   VAL: 00000000 00000001                         16:12:17
T ---- 033 RB                                                            16:12:17
R ---- 033 CCR2                                                          16:12:17
T ---- 033 RB                                                            16:12:17
R ---- 033 CCR2                                                          16:12:17
T ---- 033 RB                                                            16:12:17
DISPLAY BUFFER LINE:    1500   OF    1500, STOPPED    START DISPLAY: <SPACE>/<ESC>
```

Fig.4.3: Transmission logs of RTUs

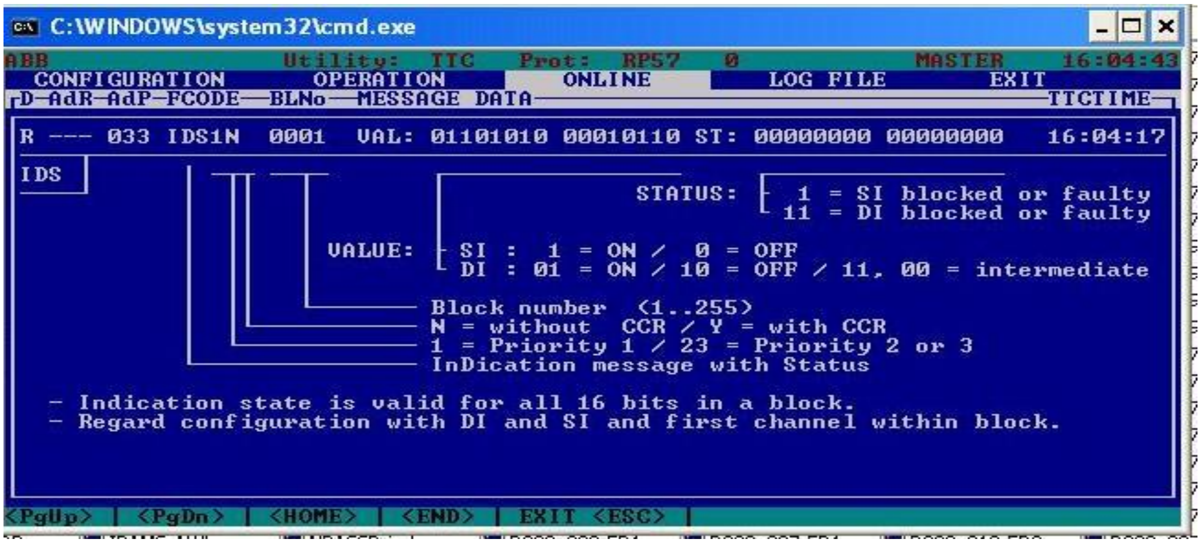
When indication changes from Operated to Normal, following message as shown in fig.4.4 is transmitted to control centre :



```
C:\WINDOWS\system32\cmd.exe
ABB              Utility:  TTC    Prot:  RP57   0              MASTER    16:09:56
   CONFIGURATION       OPERATION         ONLINE          LOG FILE          EXIT
D-AdR-AdP-FCODE--BLNo--MESSAGE DATA---------------------------------------TTCTIME
R --- 033 CCR2                                                             16:09:50
T --- 033 RB                                                               16:09:50
R --- 033 CCR2                                                             16:09:50
T --- 033 RB                                                               16:09:50
R --- 033 CCR2                                                             16:09:50
T --- 033 RB                                                               16:09:50
R --- 033 CCR2                                                             16:09:50
T --- 033 RB                                                               16:09:50
R --- 033 CCR2                                                             16:09:50
T --- 033 RB                                                               16:09:50
R --- 033 IDM1N  0002  VAL: 10001011 10000001                              16:09:50
T --- 033 RB                                                               16:09:50
R --- 033 ERMI   0002  072 04 DI INT 00000000 D: 02 : 16:11:48.5730        16:09:50
T --- 033 RB                                                               16:09:50
R --- 033 CCR2                                                             16:09:50
T --- 033 RB                                                               16:09:50
R --- 033 CCR2                                                             16:09:51
T --- 033 RB                                                               16:09:51
R --- 033 CCR2                                                             16:09:51
T --- 033 RB                                                               16:09:51
DISPLAY BUFFER LINE:    1500  OF   1500, STOPPED   START DISPLAY: <SPACE>/<ESC>
```

Fig.4.4: Transmission logs of RTUs

Interpretation of above message is shown in fig.4.5



```
C:\WINDOWS\system32\cmd.exe
ABB              Utility:  TTC    Prot:  RP57   0             MASTER    16:04:43
  CONFIGURATION       OPERATION         ONLINE         LOG FILE        EXIT
D-AdR-AdP-FCODE--BLNo--MESSAGE DATA-------------------------------------TTCTIME-

R --- 033 IDS1N  0001  VAL: 01101010 00010110 ST: 00000000 00000000   16:04:17

IDS                                         STATUS:   1 = SI blocked or faulty
                                                     11 = DI blocked or faulty

                          VALUE:  SI :  1 = ON /  0 = OFF
                                  DI : 01 = ON / 10 = OFF / 11, 00 = intermediate
                                  Block number  (1..255)
                                  N = without  CCR / Y = with CCR
                                  1 = Priority 1 / 23 = Priority 2 or 3
                                  InDication message with Status

  - Indication state is valid for all 16 bits in a block.
  - Regard configuration with DI and SI and first channel within block.

<PgUp> | <PgDn> | <HOME> | <END> | EXIT <ESC> |
```

Fig.4.5: Transmission logs of RTUs

Fig.4.6 shows layout message as per protocol format IEEEc37.10.

Synch	Remote address	Function	Internal address	Modifier
8 bits	8 bits	8bits	8 bits	8bits

Special Orders	Data	CRC
16 bits	0-192 bits	16 bits

Fig.4.6: layout message as per protocol format

Telecontrol protocols available in market do not have any mechanism to check integrity and authentication of messages received by master terminal unit (MTU) at control centre or remote terminal unit (RTU) at sub-station end [14]. These shortcomings are used by cyber attackers

- to manipulate command execution message between RTU and MTU to congest the network by creating spurious messages or by changing the configuration of network devices Matlab program has been prepared to simulate the message as per format IEEEC37.10

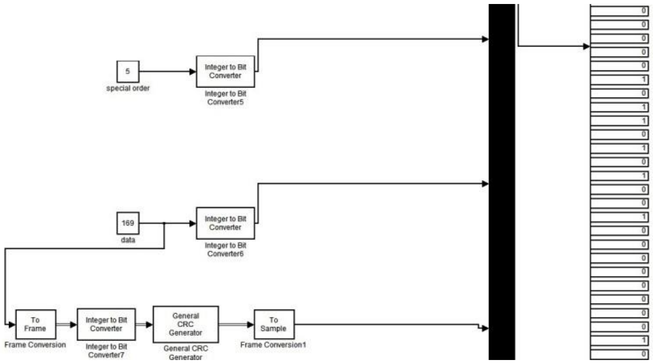


Fig.4.7: IEEEC37.10 message format simulation

Protocol analyzers and protocol gateway tools are easily available on internet which can be used to analyze and manipulate messages. Hence, unauthorized and unintended access to communication network has to be prevented.

To prevent the above, Firewall Management is analyzed. First, laptop with IP address as that of RTU series is added in the network and tried to access main server database and found to be successful.

Then following settings of IEC 104 protocol added in the firewall.

```
Access-list Soft extended permit 104 any any          (To permit RTUs of IEC-104 protocol)

Access-list Allow19 extended permit 38 any any      (RTU address – 38)
```

After implementing above settings, only RTUs communicating on IEC 104 protocol are allowed access to the server network while other systems are denied access.

Secondly, it was tried to access downwards i.e. RTU after entering communication channel using same IP address as that of server. Simulated messages through CTTP software sent to RTU and execution found successful. Then second firewall installed at RTU level with IP address and Mcaddress of server :

```
outside 173.18.0.122                  0004.a52a.15g5 181

outside 173.18.0.114                 0004.a52a.15z7 241
```

Above analysis suggests that firewall should be compatible with SCADA protocol and placed at both ends i.e. RTU/PLC/IED end as well as server or MTU end at operation control centre.

Preventive actions to avoid unauthorized access have been discussed in this paper. SCADA security administrator should be deployed by utility to check security logs of firewall and other intrusion detection systems as discussed above. He should work under management and independent of operation and maintenance teams of SCADA.

However to prevent system from internal attacks, it is also necessary to strengthen physical security policy including access control system, CCTV surveillance, cubicle opening alarm of sub-station, control centre and communication room. If any change in SCADA configuration is required by maintenance team, this should be authorized by granting of permit to work by security administrator as well as SCADA administrator.

CHAPTER-5

Summary and Conclusions

5.1 General

In this report, power supply issues and SCADA security issues of 25KV AC traction system is discussed and remedies are suggested to make the system more reliable, secure, minimal maintenance and flexible enough to cater additional load during peak conditions or multiple substation failures. SCNS-system with fault limiter is simulated. This device is based on semiconductors as switching elements and designed to cater traction power supply changeover requirement at neutral section without any involvement of frequent operations of loco circuit breakers.

In summary the main benefits if the SCNS in comparison to the conventional neutral section are the following:

- High reliability due to the application of semiconductors
- Current capability of several kA
- Minimum operation current: 3 A
- Adjustable turn-off time
- Lifetime: > 2 Million cycles
- Additional measurement capabilities (e. g. current, voltage)
- Real-time monitoring of the SCNS-status

SCNS is a breakthrough technology in the area of automatic switched neutral section. SCNS provides the possibility to supervise the status of the switch continuously and to intervene quickly by remote control. SCNS system in integration with SCADA system provides fail safe mechanism of power supply transfer across neutral section.

SCADA software from leading vendors are vulnerable to exploits that are now freely available on the internet. With the help of test set up, messages between sensors, RTUs and control centre has been analyzed and simulated. Firewall setting analysis for IEC-104 protocol has been analyzed. Different security aspects related to database level, Operating system level, operational level, Physical security, RTU/IED/PLC security, Application security, Firewall Management has been discussed in this report.

Further, in addition to firewall security, physical security and audits are equally important, Proactive approach for patch management of all SCADA components should be planned in design stage.

The above analysis suggests that achieving better quality and more secure SCADA control systems is a high priority. Improvement is a continuous process. Timely updation of security measures with technology advancement is also essential.

5.2 Future scope of work

1. Due to increase in number of passengers day by day, Enhancement of transformer capacity and introduction of new neutral sections will be required. Hence, study is required to use CI unit for 66/25KV at source. This CI unit will inject the current in phase with adjacent RSS which needs practically no neutral section. With the enhancement of load, more number of CI units can be connected in parallel as and when required. This will
   c) Remove the neutral sections from OHE
   d) Effective load management
   e) Promote power quality
   f) No imbalance on the grid side due to use of three phase to single phase converter.

2. Review of SCADA protocols for security is required so as to include following features in SCADA protocol :
   a) Password Encryption of command messages issued by user at receiving end so as to implement digital signing of command
   b) Configuration change message
   c) Compatibility of Firewalls installed at RTU level or communication level with SCADA protocols needs to be evolved.
   d) Standardardization of security features at database level, Operating system level, operational level, Physical security, RTU/IED/PLC security, Application security, Firewall Management specific to SCADA protocols.

REFERENCES

[1] Research on auto passing neutral section by CHEN LI, Yo Hong, MA Lingzhi, IEEE, 2013

[2] AC 25KV 50HZ Electrification Supply design, Dr. Roger D. White, 2013

[3] DMRC AC Traction Manual Vol-1, 2015

[4] DMRC AC Traction Manual Vol-2, 2015

[5] Rolling Stock Manual of RS-1, M/s Alstom, 2003

[6] Novel Voltage balancing Technique for series connection of IGBTs, Ruchira Withanage, 2005

[7] High voltage Switch using series connected IGBTs sing auxiliary circuit, J.W. Baek, D.W. Yoo, H.G. Kim, 2000

[8] A novel Approach to determine the optimal location of SFCL in electrical power grid to improve power system stability, G. Didier, Jean Leveque and Adberajjaq Rezoug, IEEE, 2013

[9] Analysis of IGBTs based Super conducting fault current limiter, Hu, You, Jian Xun Jin, IEEE, 2015

[10] Application of SFCL in automatic power changeover switch system of electrical railways, Hee-Shang Shin, Sung Min cho, Jae Sun Hu, Jae-chul Kim and Dong jin Kweon, IEEE, 2012

[11] en.wikipedia.org, 2016.

[12] Cyber security for SCADA systems by Thales, 2012.

[13] Kaspersky industrial cyber security : Components overview 2016.

[14] Sh. Edward Chikuni, Maxwell Dondo : Investigating the Security of Electrical Power Systems SCADA, 2004.

[15] A Trust System Architecture for SCADA Network Security Gregory M. Coates, Kenneth M. Hopkinson, Member, IEEE, Scott R. Graham, Member, IEEE, and Stuart H. Kurkowski, Member, IEEE

[16] securityincidence.net, 2010

[17] Multiattribute SCADA-Specific Intrusion Detection System for Power Networks by Y. Yang, K. McLaughlin, S. Sezer, Member, IEEE, T. Littler, E. G. Im, Member, IEEE, B. Pranggono, Member, IEEE, and H. F. Wang, Senior Member, IEEE, 2014

[18] Siemens SImatic WInCC 7.X SCADA security hardening guide

[19] Intruders in the grid published in IEEE magazine Feb 2012.

[20] Cyber security for sub-station automation products and systems of ABB, 2012

[21] Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure by Goran N. Ericsson, Senior Member, IEEE, 2010.

[22] Sh. Suhas Rautmare : SCADA System Security Challenges and Recommendations, 2009

[23] www. realthoughts.com, cptt software log file, 2016.Critical state based filtering system for securing SCADA network protocols by Igor Nai fovino