ADDIS ABABA INSTITUTE OF TECHNOLOGY
SCHOOL OF GRADUATE STUDIES
SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING

INVESTIGATING INTO REMOTE MONITORING LEVELCROSING SAFETYUSING SCADA SYSTEM:IN CASE OF AALRT

By
Mesfin Abate
Advisor: Abebe Teklu
Co-Advisor: Abi Abate
Aug: 2016

A Thesis

Submitted to

Addis Ababa Institute of Technology

Addis Ababa University

In Partial Fulfillment

of the requirements for the Degree

Master of Science in Electrical Engineering for Railway Systems

ADDIS ABABA UNIVERSITY

SCHOOL OF GRADUATE STUDIES

ADDIS ABABA INSTITUTE OF TECHNOLOGY

SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING

INVESTIGATING INTO REMOTE MONITORING LEVELCROSING SAFETYUSING SCADA SYSTEM:IN CASE OF AALRT

By

Mesfin Abate

Approval by Board of Examiners

_____

Chairman, School of Graduate StudiesSignature

Mr. **Abebe Teklu** _____
AdvisorSignature

Mr.**Abi Abate** _____
Co- AdvisorSignature

Internal Examiner _____

_____ **Signature**

External Examiner _____

_____ **Signature**

Declaration

I, the undersigned, declare that this thesis is my original work, has not been presented for a degree in this or any other university, and all sources of materials used for the thesis have been fully acknowledged.

Mesfin Abate _____

Name Signature

Place: Addis Ababa

Date of Submission: _____

This thesis has been submitted for examination with my approval as a university advisor.

Mr. Abebe Teklu _____

Advisor Signature

Mr. Abi Abate _____

Co-Advisor Signature

Abstract

Safety plays a prime importance in all aspects of life, especially in railway level crossings. Because accidents at level crossing contribute large portion on train accidents which costs human life and economical crisis. Moreover, the accident occur cause train delay and operational interruption. To tackle this problem and to assure safety by reducing accident at level crossing using various equipments used for this purpose. But existing warning device, and crossing barrier are simple train-oriented protection equipments. In this thesis, remote monitoring of level crossing to reduce those accidents to a minimum level to achieve safety at level crossing using wireless-SCADA System is proposed.

SCADA system is employed to monitor level crossings. The system employed encompasses collecting of data from a number of remote terminal unit's (RTU's) and operator terminal ,and transferring it back to the traffic control center, carrying out any necessary analysis and control and then displaying that information on a number of operator screens or displays. The required control actions are then conveyed back to the process for taking action.

In general, the SCADA system consists of two major parts, remote control center (RCC) and remote terminal unit's (RTU's).The RCC does the work of the a supervisor and controls the activities of a network through RTUs.

Keywords: SCADA, Remote, warning device, crossing barrier, RTU, RCC

Acknowledgment

The success that I have had in my educational endeavors I owe to my wife Menbere Genanu, my daughter Saron Mesfin and My newly born kid Natanyem Mesfin.

This thesis would not have been possible without the dedication and commitment of my advisor,

Mr.Abebe Teklu and Abi Abate. They have been providing me guidance throughout my research and mygraduate studies. My appreciation and support extended to Mr. Birhanu Reesom. I cannot imagine working with anyone more understanding or supportive.

I thank the Ethiopian Railway Corporation for sponsoring this graduate study.

Finally, and most significantly, I thank God, most beneficent and kindhearted

Table of Content

Table of Figures

List of Table

Chapter One

Introduction

Background and Motivation

Level crossing is part of the railway track where it intersected with road traffic and imposes a constant set of risk on safety as well as transportation capacity. Hence, the transportation bottlenecks are observed in the existence of level crossing. Accidents occurred at level crossings are with severe consequences of danger specificities to both traffic modes. In modern times, the requirement for increasing train speed is prevailing and also road vehicles are increasing which intern results in increase of accidents [1].Generally, safety is the primary attribute of any society and assuring safety at the level crossings is the priority concept while designing railway transportation infrastructure.

In recent years, light railway transit (LRT) system is becoming a means of modernizing cities and establishing new urban areas to eases the life style of the society. This is because of its ability to operate in a broad range of environments, availability, frequency of operation and capacity [2, 3]. The LRT allows smooth, comfortable, environmental friendly and quiet travel around town. In addition, LRT's can extend into the city downtown which enhances the character of downtown areas. Thus, LRT provides comfortable ride and easy reach to market center as it can make sharp turns. However, LRT level crossings are more prevalent in urban settings and it is imperative that these locations must be carefully analyzed and designed such that this mode of transportation operates in synchronization with on-street automobile and pedestrian traffic [4, 9].

Currently, Ethiopia is constructing railway lines linking different regions that will bring economical advantage to the country [1]. Addis Ababa Light Railway Transit (AALRT) (refer fig1 below) is one of the most recent which is believed to reduce the existing transportation problem. AALRT already starts operation since March 2016 and proves to be the solution for shortage of transportation system in Addis Ababa [3]. AALRT has a total of 12level crossings of which 6 of them are from North-South (Menelik II square-to-Kality) and the remaining are to East-west (Hayat-to-Tor Hayloch) [1, 7].

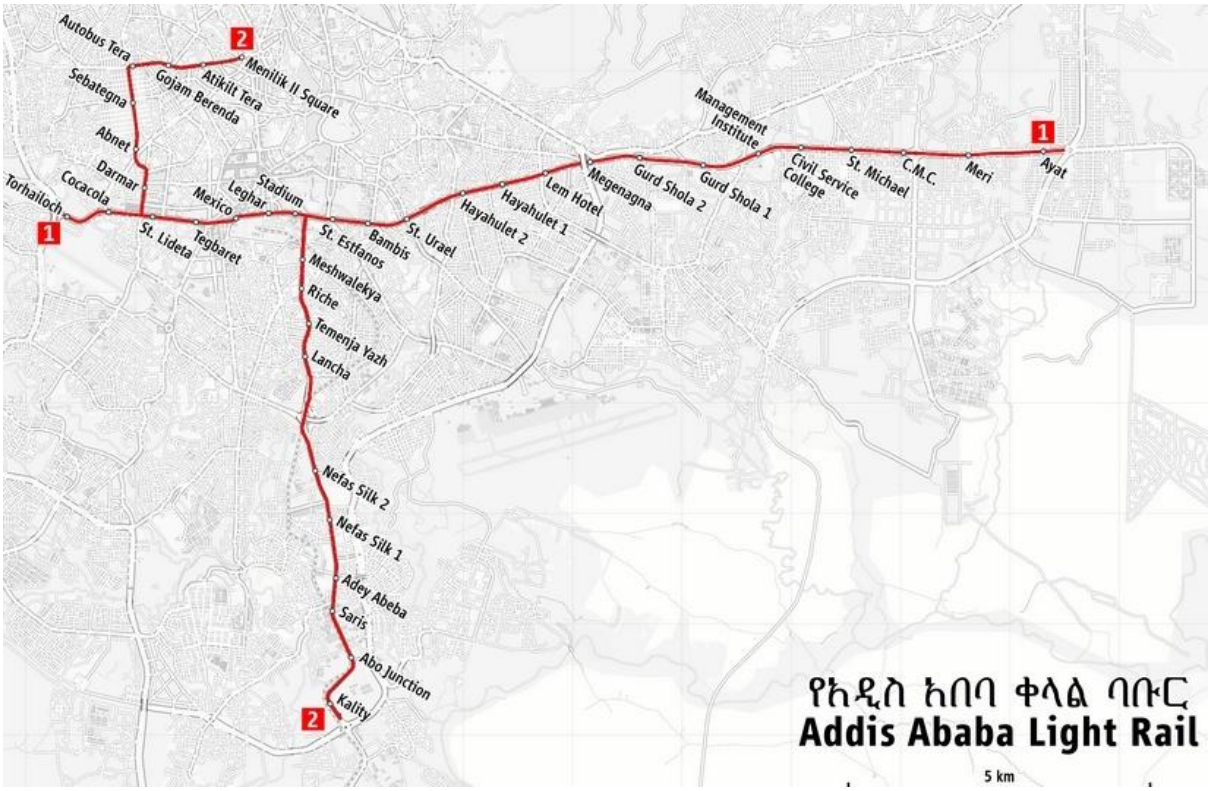


Fig1.AALRT line graph

Railway level crossing can be compared to a highway intersection with two conflicting streams of traffic, but the train always has the right-of-way. A train moves along a fixed path, and its operating characteristics prevent the operator from braking quickly to avoid a collision. Another most challenging traffic control issues associated with level crossings involves the close proximity of signalized intersections. Safety concerns occur when a train arrives and traffic from the signalized intersection has queued back onto the tracks. Similarly, traffic flow issues arise when traffic queued for a train arrival spills back onto the intersection. To alleviate both safety and operational issues associated with signalized intersections that are in close proximity to a level crossing, it is necessary to coordinate or "interconnect" railway road signals with traffic signals at nearby intersections. This coordination is often performed using a special signal "preemption" strategy which transfers the traffic signal from the normal operational mode to a special control mode upon detection of an arriving train [6].

The need for preemption arises due to the differences in the right-of-way assignment principles between roadway and railway road signals (i.e., approaching trains always have the right-of-way, while roadway signals alternately assign right-of-way based on time or

actuation). Due to these differences, adjacent roadway traffic signals must be preempted by an arriving train, to give it priority over all other movements. The objective of a preempt is to take control of the nearby traffic signal to provide for the safe passage of a train, no matter what the status of the normal traffic signal operation at the time the preemption occurs. Successful traffic signal preemption provides two functions:

1. Initially clears the tracks of any queued vehicles and
2. Does not allow any movements that would intersect the tracks, as traffic may spill back into the intersection.

Methods for adding preemption routines depend on the traffic signal controller. Most modern traffic signal controllers allow for several default and user-programmable preemption routines including those for railway-road crossings [2]. Nowadays level crossings are protected using different technologically invented devices [13, 14, and 17].

In the signaling preliminary design for the Addis Ababa LRT there is, actually a system of detecting an obstacle to prevent an accident, but it is not as technically good as that of the existing, al event or fact [13,15].Thus every responsibility is burdened on to the train operator who is driving on sight. But what if an obstacle is there on the level crossing, what if he couldn't see farther because it is fogy, night…etc. To solve this problem the "Remote Monitoring of Level crossing using SCADA System" is going to be analyzed and examined for its detection performance, reliability, longevity and cost effectiveness.

In the signaling preliminary design for the Addis Ababa LRT, there is a system of detecting an obstacle to prevent an accident, but it is not as technically good as the existing demanding for assuring safety to its customer .[2,13,15]. Thus every responsibility is burdened on to the train operator. But what if an obstacle is there on the level crossing, what if he couldn't see farther because it is fogy, night….etc. To solve this problem the "Remote Monitoring of Level crossing using SCADA System" is happened to the solution for such a problem. Hence, in this thesis, we analyzed and examined the SCADA application for its detection performance, reliability, longevity and cost effectiveness.

1.2. Problem Statement

As shown in fig 1.AALRT has two lines stretching from East to West and North to South. The East to West rail line which accounts 17.4Km is stretching from Ayat village to Tor Hailoch passing through Megenagna, Legehar and Mexico. On the hand, the North to South direction accounts 16.9Km rail track and pass through Menelik Square, Merkato, Lideta, Legehar, Meskel Square, Gotera and Kality. The two directions will have a common track of about 2.8Km. According to the train operation plan of LRT project in Addis Ababa, a train is passing the level crossing every 1.27 minutes on average in long-term daily service time from (5:00 AM ~11:00 PM) with maximum running speed of not more than 70 km/hr and 41 trains in service, including 21 trains for E-W line and 20 trains for N-S line [2].

Level crossing safety is an old and persistent problem, an unpleasant hangover from an era when rail and road traffic were far slower and less frequent than they are today [7].The way of solving the transportation problem of the residents is quiet acceptable; however, safety mechanisms must be given a space so as to sustain and provide confidence in using the vehicle.

Figure 2:Road and Rail crossings

Figure 3:Moment all together at level crossings

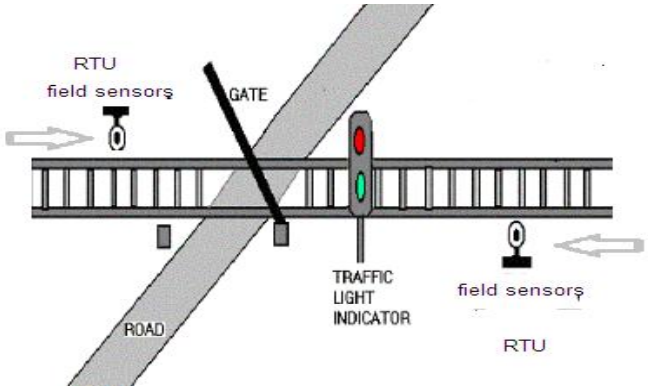


Figure 4: Crossing of road and rail[1]

As it is new and the resident has not prior knowledge practically on how and when to cross the intersection and lack of formal training about the meaning of the devices and the required course of action, makes the LRT crossing an especially vulnerable location for pedestrians (and bicyclists) accident. Level crossing control devices and systems intended to communicate with the pedestrian should not only transmit the intended message clearly, but should also indicate the required action and the increased level of risk associated with violating the crossing control device. [2]

All safety concerns at LRT systems are exacerbated by the failure of some crossing users to accurately perceive and obey crossing control devices and warning systems. With LRTs approaching level crossing at speeds up to 30 kilometer per hour (Km/hr), based on the alignment type, there is little opportunity for crossing users to err (making mistake) and recover safely for operators to avoid collisions. Therefore, adequate perception of crossing control devices and warning systems by crossing users is critical to the overall safety of LRT operations [2].

The other critical one is about car drivers, who engage in numerous action and emotion at crossings that may increase the risk of an accident. For example, the driver disregarded a stop sign, failed to look for a train, distracted, and had a judgment error involved roadway conditions that limited the drivers' ability to see the crossing or train. In addition, the most important issue in level crossing is traffic queues which have potential impact for extending across nearby crossings. Safety concerns occur when traffic queued back on to intersection. Similarly, traffic flow issues arise when traffic queued for a train arrival spills back onto the intersection [3, 5]. So level crossing is more important issue in transportation because it cause serious damage and cause more accidents.

Many attempts have been implemented, including CCTV camera System [9], to reduce the catastrophes happening at level crossings. To this end, this thesis investigated on level crossing control used for AALRT and identifies the bottlenecks, the use of Supervisory Control and Data Acquisition (SCADA) system for level crossing control and suggests suitable communication architecture to monitor railway level crossing for safe train operation.

1.3. Objectives

1.3.1. General Objective

The general objective of this thesis is to investigate the use of Supervisory Control and Data Acquisition (SCADA) system to monitor railway level crossing operation remotely for safe train operation.

1.3.2. Specific Objectives

Specifically; the aim of this thesis is to:

- Perform an in-depth investigation on conventional level crossing accident prevention techniques and analyze their role in railway transport.
- Investigate on future level crossing applications capacity demand
- Investigate on how to reduce effects of accidents before and/or after its occurrence.
- Investigate the various communication architectures for supporting remote monitoring of railway level crossing operation.
- Performance Comparison of the proposed SCADA architecture against the existing one.

1.4. Methodology:

The method used for this thesis includes:

- ✓ **Literature review**: looking thoroughly of different research papers, works, journals, any publication and materials which encircles railway level crossing accident prevention and related topics are conducted. Having brief understanding of the problem, collection of necessary information which is essential to achieve the objective of this thesis is done. Even though information collection is not completed due to unavailability of the required documents; assumptions and information from different thesis, papers and books are used.
- ✓ **System Designing**: in this step, the components that are highly involved to contribute for the level crossing accident prevention system are studied and designed to come up with a model.
- ✓ **Performance comparison and Analysis**: finally, the performances obtained are analyzed; interpreted and possible suggestions are done.

1.5. Scope of the Thesis

The scope of this thesis is:

- ✓ Cramming current status of traffic condition in Addis Ababa light railway transient (AALRT) and suggest essential point that are helpful in reducing accident on level-crossing.
- ✓ Present statistics, indicators, technology and problems relating to the systems adopted for level-crossing protection.
- ✓ Analyze various alternative systems for level-crossing protection and Make recommendations pertaining to the selection of cost-effective protection systems.

1.6. Expected Output

The main issue of this thesis is to optimize traffic flow on level crossing and to minimize risk. The output of this work:-

- ➢ Traffic queue of vehicles near level crossing will be reduced.
- ➢ Enhances non- conflict movement of Pedestrian on level crossing
- ➢ Conducting efficient and effective operation of traffic over level crossing so as to attain wellbeing of its customer.
- ➢ Minimize traffic delay reduction on level crossing
- ➢ Appropriately harmonize the movement's vehicles, trains, and pedestrians on level crossing
- ➢ Decrease accident and any kind of catastrophes that occur on level crossing.

Thesis organization

This thesis is organized in Six chapters.

The first chapter describes about the introduction of this thesis. It provides clear information about the background work, the problem investigated, objective of thesis and methodologies used to achieve the stated objective.

Chapter two is named as literature review as it goes from the AALRT's level crossing system to the SCADA application for level crossing control. This section provides clear understanding of level crossing accident prevention system. In addition, it provides clear information about the SCADA application along with AALRT's accident prevention method.

Chapter three is modeling of the proposed system State-of-the Art: Train model, Signal model, and System flow chart.

Chapter four: Compare and contrasting the existing system against the proposed SCADA system under different operational scenarios are considered.. Hardware and Software Components of the SCADA system.

Chapter five is recommendation and conclusion. Here, the work would be concluded based on the result discussed and obtained in chapter five. Further recommendation for the development of new model or improvement would be suggested.

1.8. Thesis Limitation

Even though the investigating work is carried out in an effective manner, but it does not include any software simulation activity. As I have seen and tried ,it would have been better if it were simulated using suitable software.

Much has been tried to include the simulation activity, however, fail to get the suitable simulating software because it is not available in an open source. Even the trial version they provide has got very much limited expiry date. For instance IGSS20(2 days),RRAuto (30 minutes), Scram(one Day).

Thus to make use of those software it is expected to spent $10,000 to $20,000 (200,000-400,000 Eth birr).Which is too much costly.

Chapter Two

2.1. Existing Level crossing System at AALRT

One of the problems, which arise during the railway operation, is a problem of providing safety at the railway crossings. This problem is of actual value for all the countries with railway transportation service. The problem arises owing to the fact that railway crossings are not equipped well and the installed equipment got out of date. [1, 4, 5]

Problems with railway crossings lead to the unproductive stoppages of the railway and automobile transport, faults in train schedule and accidents which includes traffic fatality. The most characteristic problems in railway crossing operation is lack of required amount of road signs, traffic light and sound signaling, lightning and poor visibility of the train.

Modernization of the railway crossing automation or development of the new warning and control automatic system (traffic lights, traffic control barriers with audio announcement) are intended for improving safety of crossing both serviceable and non-serviceable railway crossings.[35]

Here in Ethiopia the problem mentioned above exists since the Emperor MenilikII regime at the railway transportation stretching from Djibouti-Diredawa-Addis Ababa. And now the most modernized that has never been exists in the country built in different areas. One among the many projects is the AALRT. [2, 35, 36]

The Addis Ababa Light Railway Train uses DX-lw LX system for controlling the level crossing system .The system consists of the following equipments:

1. Main Control cabinet(MCC):
2. Barrier Control Box
3. Barrier and Road signal
4. Audible alarm device.

Each component contributes its part for securing safety .For instance, the MCC consists of main control unit, outdoor equipment interface board and power module. While

The DX-IW control system composed of the following main components.

1. Main control cabinet (MCC)-this is the main control system having main control unit, outdoor equipment interface board and power module.

2. The Control and Indication control panel-CIP which is an integrated on the face plate of the control cabinet and LCD screen for indicating the status of the LX equipment.

3. Barrier control box is used for the crossing operator to control the barrier. two Sets of lifting /lowering buttons are arranged in each barrier control box and one set of lifting/lowering buttons may be shared by two opposite barrier .

4. Outdoor Equipments: this comprises of the barrier machine and the road signal.

With all the above equipments and operator (a guard) that the level crossing duty is handled.

The main function of LX sub system with the DX-IW is to give approaching alarm notice and controlling road signal as well as the barrier.[2]

In this regard, the information of approaching train at the level crossing from any direction is provided by the Interlocking system that will be displayed on the relay interface for the operator. The LX subsystem then send the control information to the indoor and outdoor train approaching alarm notices.

There are three kinds of alarm notice used by LX subsystem. The first one is buzzer alarm which is adopted for the indoor train approaching alarm notice ; the second one is Audible and visual alarm indication of signal dedicated to provide information to pedestrian and the vehicle and the third one is the audible alarm used by the outdoor which installed at the top road signal post with horn loudspeaker.

If the train approaching to the level crossing at any direction, the LX subsystem is able to send the alarm notice to every equipments that is dedicated to carry out this duty. But the indoor alarm signal is cancelled by the guard.[2, 9]

The barrier control is again the part of LX subsystem participating in the level crossing control system which operated in three modes.

- ✓ Automatic operating mode(automatic lifting and manual lowering)
- ✓ All manual operating modes.
- ✓ On-site manual mode

The automatic operation mode or all-manual operation mode will be set after system initialization and modified as required. Under normal condition, after train clearing out of the crossing area, the barrier will be lifted up. When the barrier is lifted, it should be judged that the train is approaching in either direction determined by the interlocking system and when the train leaves that area the route at the axle-counter section will be released.

The Lx subsystem will stop the outdoor train approaching alarm and lifted the barrier when the interlocking system sends that the train leaves the crossing. But if the condition for lifting is not working perfectly, the barrier will remain in the status of lowering and controlled by the guard.

If the train approaching the crossing which is requested by the interlocking, he will press the lowering button after being checking that anything is available in between. On the other hand, he will press the barrier by-pass switch on the control and indication panel, if the interlocking is not able to get status information about the status of level crossing barrier.

In the case where power is failed or mal function of the system, either the barrier is lifted manually by the hand crank at the site operated by the guard or the barrier will stop and stay at the current position and again operated by the guard.

Regarding the road signal, it is controlled by the control cabinet. It has two aspect color (light indications). Under normal condition Green light is displayed, where every pedestrians, vehicles and cyclists are allowed to cross. But if the train approaching information is send by the interlocking system, then the light will be turned to Red after the green light flickering for 5 seconds. When the crossing area is cleared and the system barrier should be lifted manually and the Green light will get glow.

Table Among the technical parameters. The following are taken for this case

Table 1: Status of level crossing equipments and there duration at Saris

No	Status	Duration
1	Crossing Barrier action time.	Barrier lifting <7s,barrier lowering <10s
2	Length of the cross barrier arm	10m.Maximum
3	View distance of road signal	>=200m
4	MTBF	• Barrier machine: operation times no less than 50,000. • Service life of road signal is 50000hr. • The Electrical endurance of buttons is not less than 500,000 times.

- Here the level crossing control mechanism relies on the interlocking system. In other words it is the interlocking system along with the guard that facilitates the controlling phenomena of the level crossing.
- The duration that takes for closing and opening of the barrier is long.

- The lowering (closing) and lifting (opening) time varies having 3s difference, which is huge figure.
- The view distance is less.

Practical observation at the site during operation:

What I have seen and exactly there at the site is Barrier (gate) which is opened and closing automatically and traffic policeman who are working as a guard.

There is also alarm system.

And there also light indicating lumps working together with the level crossing to assure safety. But the signal aspect the theoretical one (document) and the practical one is total different and one is the inverse of the other.

2.2. Level Crossing Control System

2.2.1. Introduction to Level Crossing Safety

Level Crossings are a critical interface between the railway and roadway, which require regular maintenance and testing to ensure safety. Therefore, level crossing protection is employed to oversee the safe operation of both railway and roadways. Although railway and road transports are different entities with entirely different responsibilities, domains and performances; both will come together and converge for a single cause of providing a facility to the transport user at level crossings. This prevail the possibility of risks at intersection. Even during normal operating condition, there exist possibilities of observing transportation accidents which may cause extremely high rate of risk. Usually such a situation my happen due to negligence of the operation procedures [1, 7].

The potential for accidents is made higher as the railways control only half the problem. The other half, meanwhile, cannot really be said to be controlled by one entity, as even though traffic rules and road design standards supposedly exist, the movements of road users are not organized and monitored by one specific entity as rigidly as rail movements. The railway systems of Asia and the Pacific are no exception to this. Each year, accidents at level crossings not only cause fatalities or serious injuries to many thousands of road users and railway passengers, but also impose a heavy financial burden in terms of disruptions of railway and road services and damages to railway and road vehicles as well as properties. A very high number of these collisions are caused by the negligence,

incompetence or incapacity of road vehicle drivers, who by and large operate their vehicles in environments in which safety consciousness is practically non-existent. Since it is the railway which must bear the responsibility for ensuring that, it is protected from the transgressions by road users (despite the fact that in many countries the law gives it priority of passage over road users), it is the railway which also has to shoulder most of the financial burden of providing this protection. Similarly, it is the railway, which has most of the responsibility for educating road users on the safe use of its level crossings. Notwithstanding this, it appears that in many regions, railways are ill-equipped to be in a position to monitor level crossing safety effectively and to take both corrective and pro-active measures to improve the safety of their level crossing installations [4, 6].

2.2.2. Level Crossing Types

According to European Railway Agency (ERA), level crossings (LC) are classified into two groups:

- ✓ Group A (Active LCs)
- ✓ Group B (Passive LCs)

The active LC is where the crossing users are warned from the approaching train by the activation of devices when it is unsafe for the user to cross the LC; whereas the passive LCs are equipped with any warning signs, plates, devices, or any other protection equipment, which is permanent and independent of any traffic situation.

The first analysis of operational LC risk was carried out on the basis of the active and passive LC types as defined per the ERA for the purpose of defining Common Safety Indicators (CSI). As a basis for comparison, seven basic LC types defined per ERA were taken into account. The individual risk for road LC user was compared as per the different LC types. However, only five of these types could be identified (the A1.1 and A2.2 were not clearly identified) when analyzing the 66 collected national level crossing types of countries involved in SELCAT project. Risks considering the accidents, fatalities or injuries at LC of a particular type are covered deeply in [12].

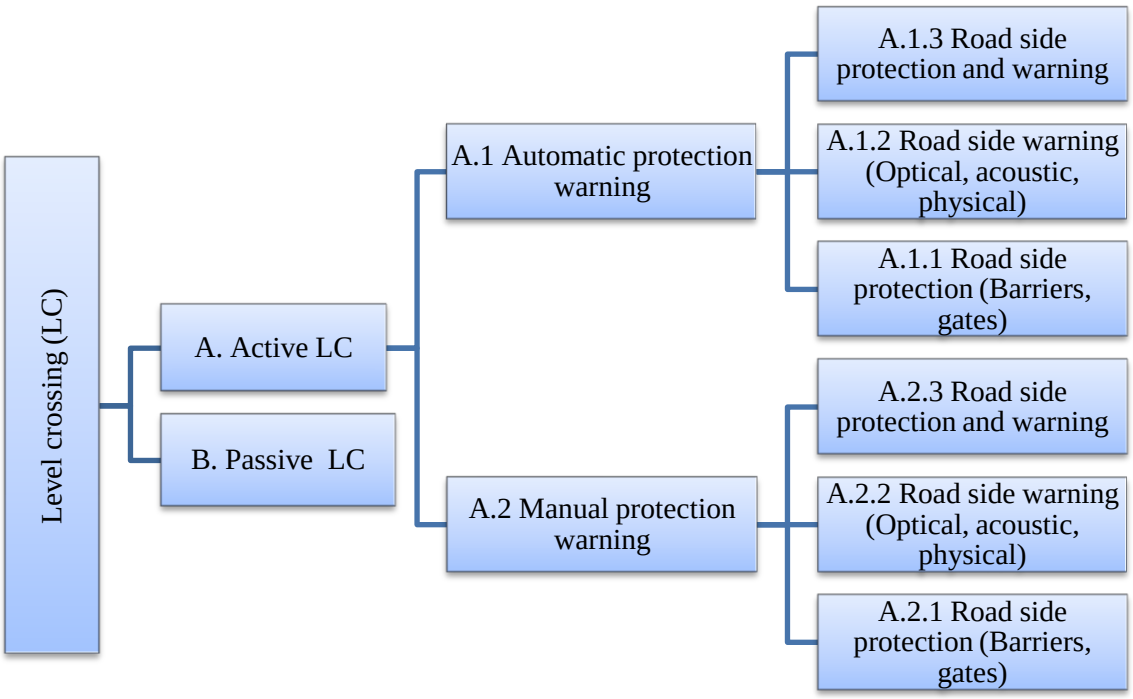


Figure 5: Level crossing (LC) types classified by European Road Authority (ERA)

2.3 SCADA System

2.3.1. Introduction to SCADA

New technologies have become increasingly important in our lives and can be used in more and more different areas. One of the most important questions is how to observe remote events, which are located several hundreds or thousands meters away, and how to quickly and timely respond to system changes. For such data monitoring and collection, SCADA systems were designed. These systems may be implemented in various fields – from industry to housing. The main purpose of such systems is to monitor, gather and analyze data. The system processes the received data all the time and then takes appropriate measure based on the information processed; for example, to send specific tasks to controllers or inform relevant people or instances about the situation when deviations are noticed. In general, Supervisory Control and Data Acquisition (SCADA) system is used for remote monitoring and control in the delivery of essential services products such as electricity, natural gas, water, waste treatment and transportation [3, 15]. If we consider water level control system using SCADA, when the water level exceeds a preset threshold, the application activates the pump system to pump water to tanks with low water level. Beyond this, transit authority's uses SCADA system to regulate

electricity to subways, trams and trolleys and to automate traffic signals for rail systems, to track and locate trains and to control railroad crossing gates [16].

A SCADA system can monitor and control a lot of input-output points. It assists in the operation and management by providing a computer-based technology that offers flexibility in operational efforts, easiness in gathering and maintaining data, and its ability to reports on a timely basis [33]. Moreover, a SCADA control center performs centralized monitoring and control for field sites over long-distance communications networks, including monitoring alarms and processing status data. Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices. On the other hand, field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

It is uses a common automation system to gather data from sensors and instruments located at remote sites and to transmit and display this data at a central site for either control or monitoring purposes. The collected data is usually viewed on one or more SCADA host computers located at the central or master site. In a railway system, these devices can be deployed in remote locations in the field. The monitoring and control via SCADA is done at center within the Master Terminal Unit (MTU)[5, 16].

A SCADA system in its simplest form consists of a central host or master computer Master Terminal Unit/MTU communicating with one or more data gathering units (Remote Terminal Units / RTU) by means of one or more communications media and a collection of standard and/or custom software. A wide range of telecommunications media (i.e., land lines, public switched network, radio can be used to provide a means of communication between MTU and RTU[30].

Implementation of SCADA system saves time and money, because it is not necessary to go to remote sites for data collection or to check the functionality of the system. With the use of SCADA system real time data and system management, automatic report generation, system errors elimination and many other functions become possible [17].

2.3.2. SCADA Classification

SCADA system can be classified in different ways. For example; according to Divide Bailey [6], there are four (4) different types of SCADA systems.

1. First Generation: Monolithic or early SCADA systems are earlier SCADA systems were developed wherein the common network services were not available. Hence, this is independent systems without having any connectivity to other systems as shown in
2. Figure and is limited to monitoring sensors only.

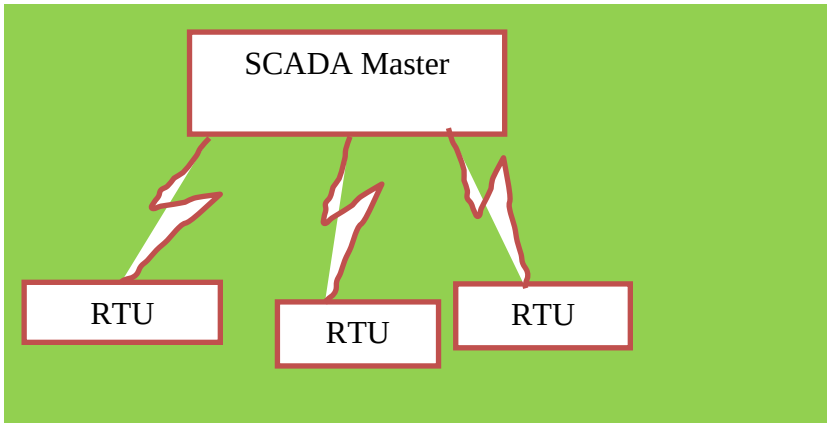


Figure 6: Monolithic or Early SCADA Systems architecture.

3. Second Generation (Distributed SCADA systems):here the sharing of control functions is distributed across the multiple systems connected to each other using Local Area Network (LAN). Hence, individual stations were used to share real-time information and command processing for performing control tasks to trip the alarm levels of possible problems.[5,6]

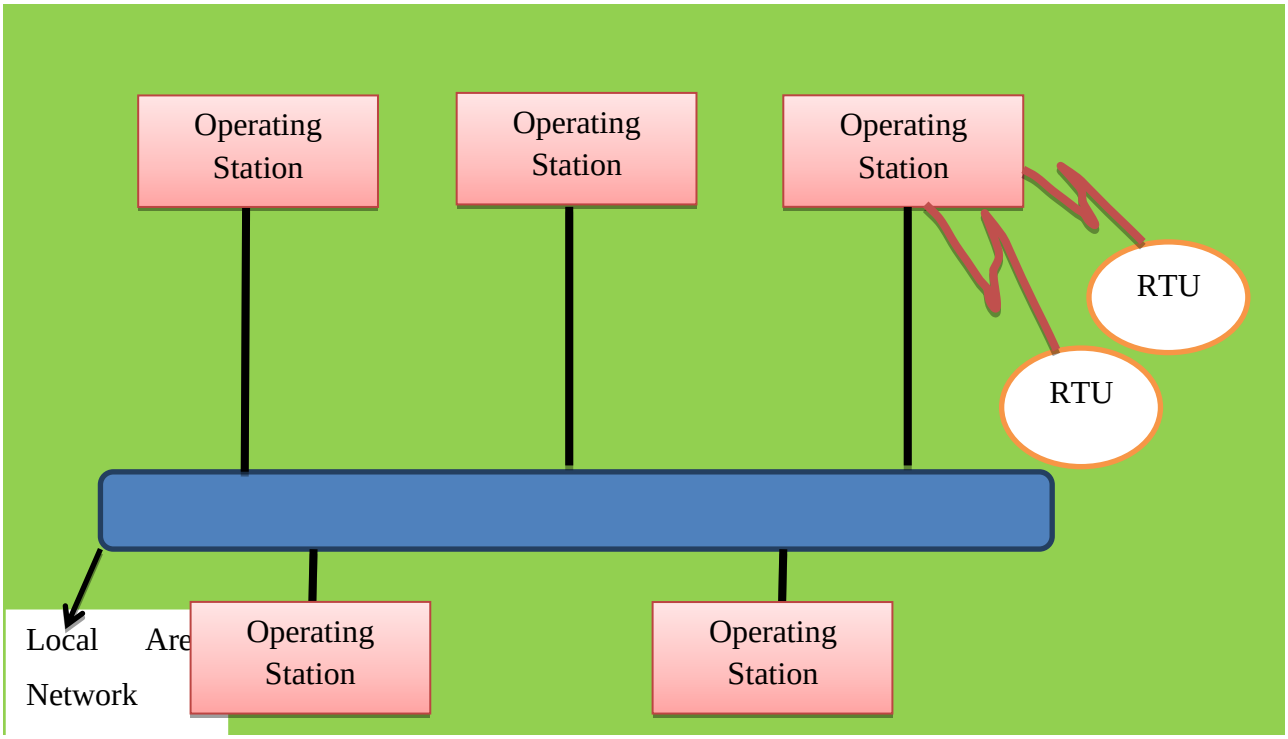


Figure 7: Distributed SCADA Systems Architecture.

The cost and size of the station were reduced compared to the first generation system, as each system of the second generation was responsible for performing a particular task with reduced size and cost. But even in the second generation systems, the network protocols were not standardized. The security of the SCADA installation was determined by a very few people beyond the developers, as the protocols were proprietary and literally the security of the SCADA installation was ignored.

4. Networked SCADA Systems: The current SCADA systems are generally networked and communicate using Wide Area Network (WAN) Systems over data lines or phone. These systems use Ethernet or Fiber Optic Connections for transmitting data between the nodes frequently.[3,5]

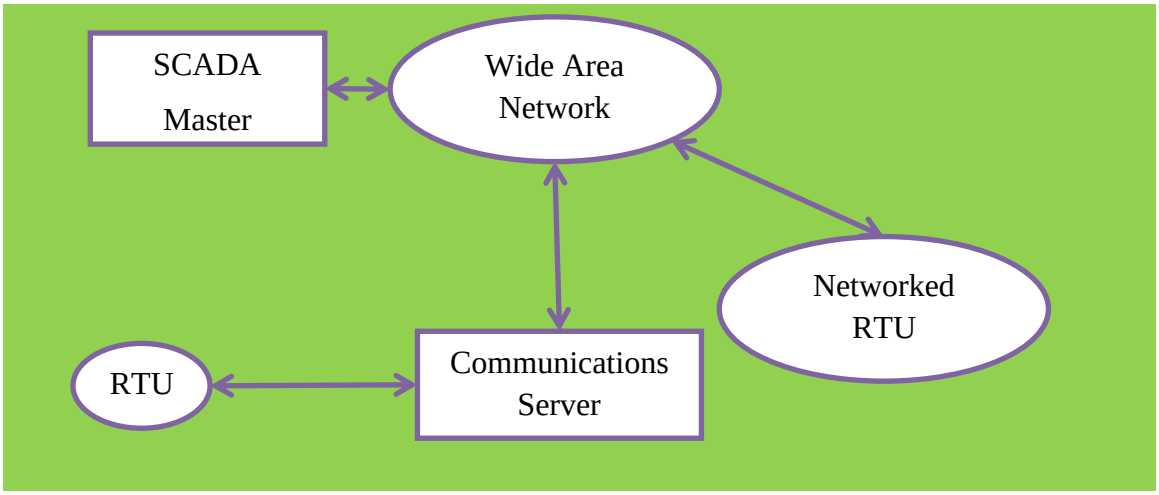


Figure 8: Networked SCADA Systems architecture.

The first and second generation SCADA systems are limited to single site networks or single building called as sealed systems. In these systems, we cannot have any risk compared to the third generation SCADA systems which are connected to the internet causing the security risks. There will be several parallel working distributed SCADA systems under a single supervisor in network architecture.

5. **Internet of Things**

In fourth generation, the infrastructure cost of the SCADA systems is reduced by adopting the internet of things technology with the commercially available cloud computing. The maintenance and integration is also very easy for the fourth generation compared to the earlier SCADA systems [5,6].

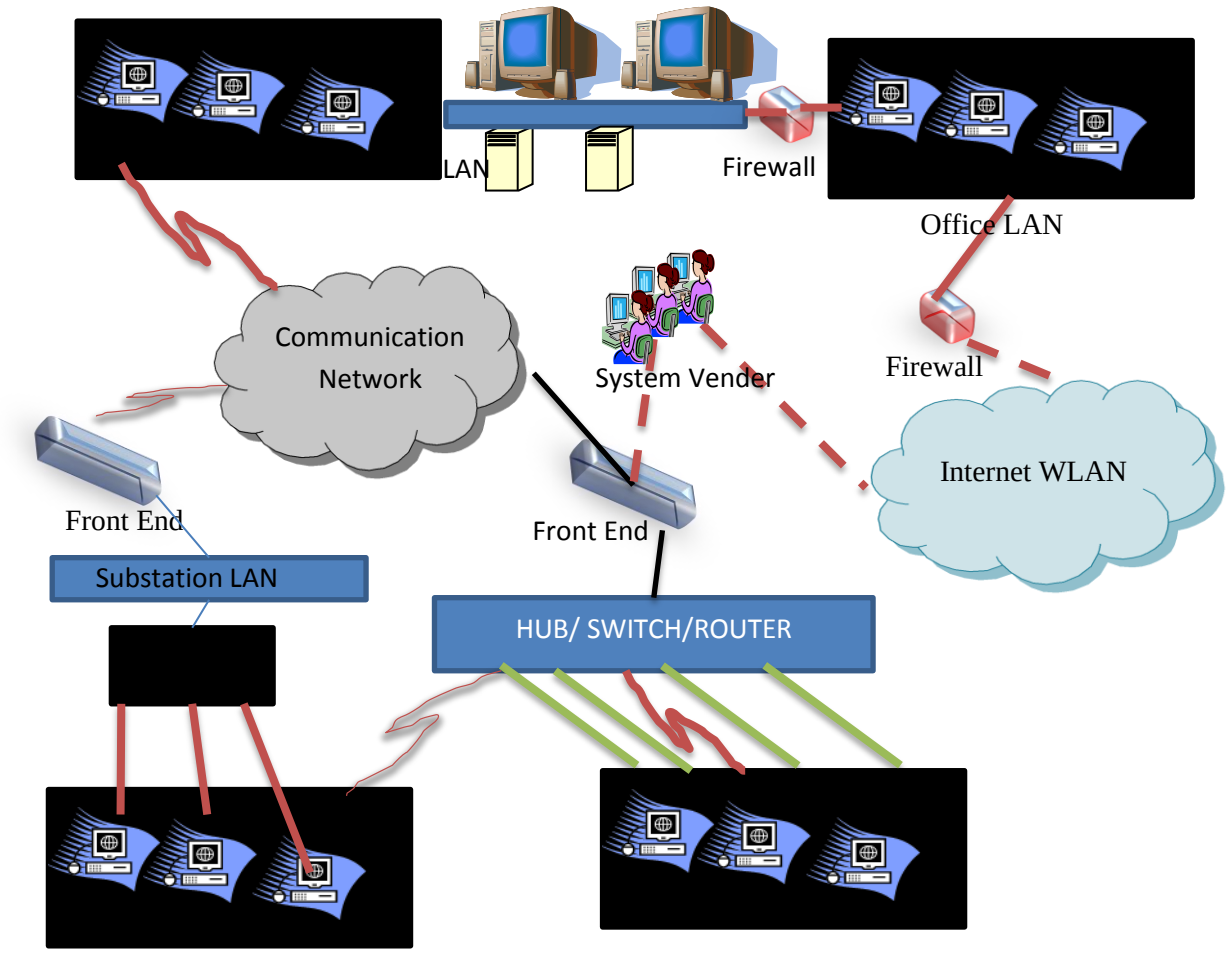


Figure 9: Internet of Things system Architecture

Of the four generation of the SCADA, this thesis used the third generation SCADA system. This is due to the technology that is able attain and implement. Regarding the fourth generation, it is based on clouding which is going to be feature work

2.3.3. The SCADA Communication System Protocols

Basically the SCADA system is based on hardware included "Master Terminal Unit (MTU), Remote Terminal Units (RTUs)" and software that provides communication interface between SCADA hardware and software. Human Machine Interface (HMI) also provides facility to visualized entire SCADA communication including controlling and monitoring. Master Terminal Unit (MTU) is located at control center or perform the services of control station and connected with one or more Remote Terminal Units (RTUs), that may geographically distributed over remote areas (wide area network) or within Local Area Network (LAN) using communication link/media such as radio

signals, telephone line, cable connection, satellite and micro waves media. In this thesis the wireless communication system is implemented. The RTUs have been collecting data/information from actuators/sensors and then process to Master Terminal Station (MTU) for monitoring and controlling the entire SCADA system [31].

Communication protocols are the rules that govern the communication between the different components within a distributed computer system. There are a number of different kinds of protocol which are used for controlling the information transmission between the MTU and RTU.In such case the MTU and RTU would be communicated as a Master(MTU)-to-Slave(RTU) way; besides, the network topology employed would also be Token ring and multiple access systems.

Initially some devices such as instruments and protective relays allowed remote communication via local RS232 connection or via dial-up modem (PSTN) link without a protocol. However, these devices also supported a protocol; the data representations sent are not identified in any fashion other than by absolute addressing. Each protocol consists of two message sets. One set forms the master protocol, containing statements for master station initiation and the other set is the RTU protocol, containing statements an RTU can initiate. The SCADA protocol between master and RTU forms a model for IED-to-RTU communications.(for more protocol see fig 110) [32.33].Of which Distributed Network protocol (DNP3) and ModBus are chosen because both are byte-oriented protocols. Both protocols are widely used over a variety of physical layers, including RS-232, RS-422, RS-485, and TCP/IP. ModBus has a separate specification to use over TCP/IP (ModBus-TCP). With DNP, the protocol encapsulated within TCP/IP. The DNP3 type protocol is chosen over the ModBus, because it is an application layer protocol, while DNP3 contains application and data Link Layers, with a pseudo-transport layer [6].
In general, the primary advantage of ModBus is for small devices and the very large range of devices that have some sort of ModBus interface. It is widely used in process control and SCADA systems.

Among the many protocols, the DNP3 has more applicable than the ModBus and other related SCADA protocols [31].The ProfiBus protocol has a robust communication ability and ease of use in hazardous applications, on the other hand, ModBus is easy to use in small applications and provides a good link between a SCADA system and data

concentrator. Moreover, ModBus protocol is used because it has the character of easy modem support and simple implementation [33].So for this thesis the ModBus protocol is selected.

DNP3 is specifically designed for use in SCADA applications. It is highly standardized, with relatively high compatibility and inter-operability between devices from different manufacturers.

Both DNP3 and ModBus have independent Technical committees that are working to ensure interoperability and create standards for new functionality. [6,8, 9]

Table 2: Comparison Summary

Feature	ModBus	ProfiBus	DNP3
Open Domain	✓	✓	✓
Active User Group	✓	✓	✓
Multiple Data Types	✓	✓	✓
Standardized data formats	X	X	✓
Time-Stamped Data	X	X	✓

The DNP3 protocol can be used reliably over media that is subject to noisy interference. This protocol uses 27 basic function codes for exchange of data between Master and RTU.Some codes enable the Master

- To request and receive status information from remote (RTU).
- To change the RTU settings

The primary advantage of ModBus is its simplicity for small devices and the very large range of devices that have some sort of ModBus interface. It is widely used in process control and SCADA systems. DNP3 is specifically designed for use in SCADA applications. It is highly standardized, with relatively high compatibility and inter-operability between devices from different manufacturers. Both DNP3 and ModBus are working to ensure interoperability and create standards for new functionality. [33]

The following points are particularly highlighted why DNP3 is selected: It supports control operations via output object groups and its output objects are also read/w rite; reading the output object and returns the output status. The actual value of the control point can be monitored via a Binary or Analog input.

1. It supports high-security two-step control operations.

2. The quality flags reported by DNP3 give important output quality status information, including whether the point is offline, if it is being controlled locally.[34]

2.3.3.1. System Structure of DNP3

DNP3 or Distributed Network Protocol Version 3.3 is a telecommunications standard that defines communications between master stations, remote telemetry units (RTUs) and other intelligent electronic devices (IEDs). [32]

System Topology

The system topology of DNP3 protocol includes the following and is explained hereafter:

- ✓ Master–Slave
- ✓ Multidrug from one master
- ✓ Hierarchical with intermediate data concentrators
- ✓ Multiple master

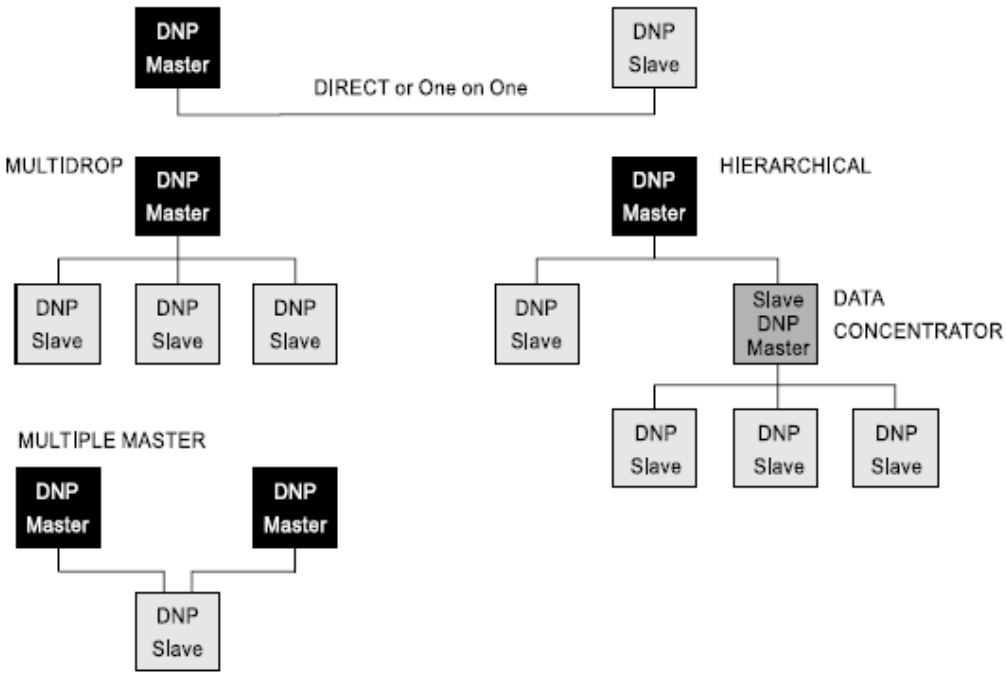


Figure 10:DNP3 Network Topologies [31]

DNP3 supports multiple-slave, peer-to-peer and multiple-master communications [30]. In this paper the Direct and Hierarchical is implemented. This is because the communication character that exists between the MTU and RTU dictates the system to use the hybrid of the network topologies.i.e. The Direct and Hierarchical.

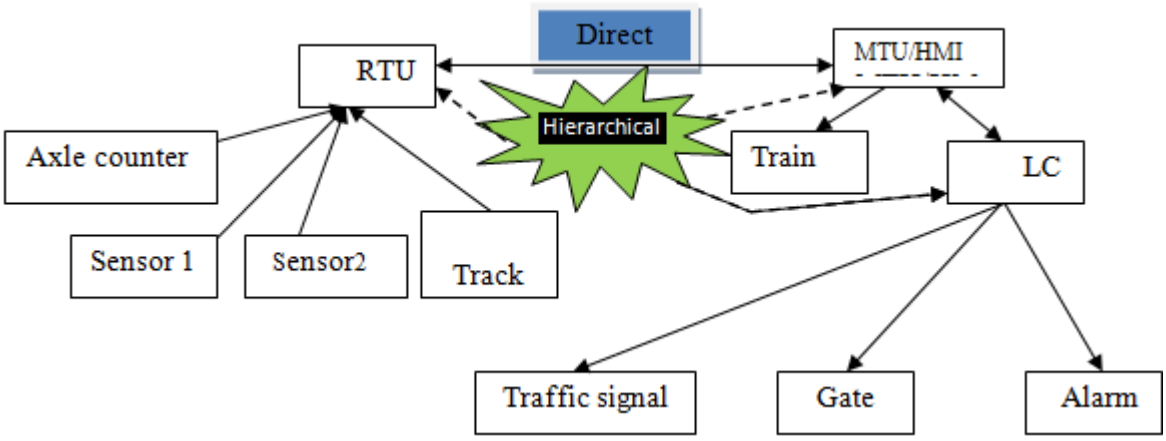


Figure 11: The Hybrid DNP3 Topology (being used by this paper)

Why use DNP3?

DNP3 is an open protocol that is gaining widespread acceptance and usage across a number of industries and countries. It is optimized for SCADA communications, and provides secure and efficient communications for the types of messages transferred by these systems.

The reasons for the adoption of DNP3 by users are primarily:[32]

- It is an open protocol
- It is optimized for SCADA communications
- It provides interoperability between different vendor's equipment
- It is supported by a substantial number of SCADA equipment manufacturers
- It will provide immediate and long-term benefits to user

Message Structure and Message Buildup

In the OSI-7 model there are seven layers, each layer of the model has its own message structure and associated message build up [29,31]. The DNP3 protocol has involved in some of the layers, namely: Application, Transportation, Data link and the Physical layers [32]. The information that has passed from the higher layer (Application Layer) and continuously adds information connected with the services performed by that respective layer. The additional information is usually added as a header, that is, in front of the original message. Thus during message assembly, the message will grow in size. It is also disassembled in the reverse way like last-in-first-out (LIFO) into smaller units of data.

Structure Model

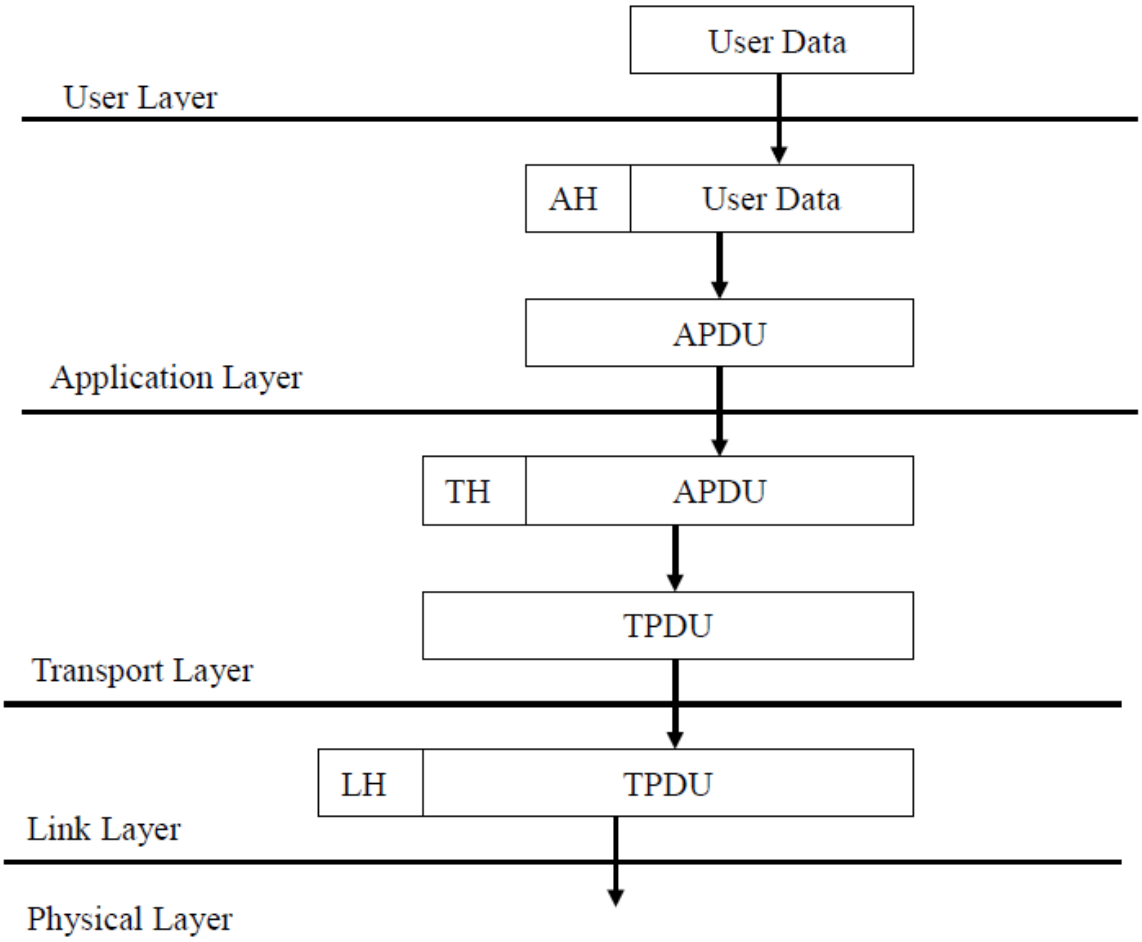


Figure 12.The Detailed Structure of DNP3 protocol

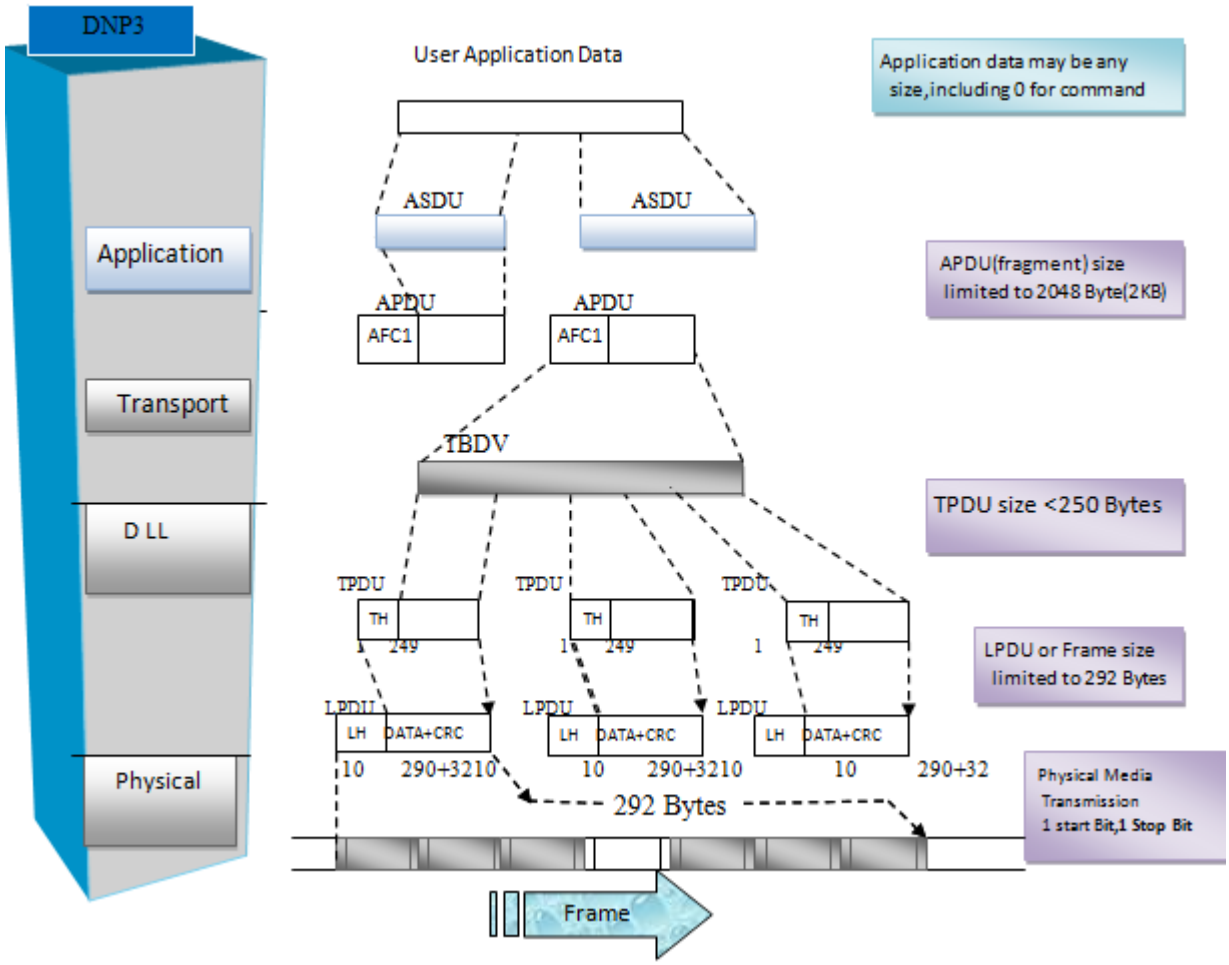


Figure 13: The Detailed Structure of DNP3 protocol

The message buildup illustrated in the drawing is now briefly described for each layer.It is described here from the highest level, the application level, downwards. This reflects the sequence of message building during sending. Of course the sequence at the other end is in reverse, as the message is passed over the physical medium, into the data link layer, and up to the application layer.

The user data is the data arising from the user application at the application layer. The user application can be visualized as a layer above the application layer, and could be a human machine interface (HMI). The data could be alarm and event data, digital status data, or even a data file such as a configuration file being passed from a master terminal unit to RTU (confirmation),Level crossing and to Train driver. On the other hand, in the case of many types of command being issued by a master terminal unit, there may be no data at all provided that no message is coming from RTU. A key point is that this data can be of any size. The total data size is not limited by the protocol. The application layer initially forms the data into manageable sized blocks. These are called application service data units or ASDUs. The application layer then creates the application protocol data unit

APDU by combining a header with the ASDU data. The application header is referred to as the application protocol control information, or APCI. This is either 2 bytes or 4 bytes in length, depending on whether the message is a request (from RTU) or a response (from MTU) or control data (from MTU).There is only a header, and no ASDU. Depending on the total size of the data to be transmitted, one or more APDUs are created. In the case that multiple APDUs are required, these are each termed fragments. Whilst the number of fragments required to represent an ASDU is not limited, the size of each fragment is limited to a maximum of 2048 bytes. 80 Practical Modern SCADA Protocols: DNP3, 60870.5 and Related systems.

The APDU from the application layer may be referred to as the transport service data unit within the pseudo-transport layer. It is interpreted purely as data to be transported by the transport layer. The transport layer breaks the TSDU down into smaller units termed transport protocol data units or TPDUs. These are made up of a one byte header, followed by a maximum of 249 bytes of data. The overall size of the TPDUs, which is 250 bytes, was determined so that each TPDU will fit within one 'frame' or LPDU at the data link layer.

Then follows the data link layer that takes the TPDUs from the transport layer and adds a 10 byte header to each. As the data link layer is also responsible for providing error detection and correction functions, error checking codes are introduced here [23].A 16-bit cyclic redundancy code (CRC) is used. Each TPDU is converted to a frame of up to 292 bytes in length. It is worth noting at this point that the frame format is known as the FT3 frame.

The physical layer converts each frame into a bit stream over the physical media. In the original DNP3 documentation, a bit-serial asynchronous physical layer is specified. It calls for 8-bit data, 1 start bit, 1 stop bit, no parity, and RS-232C voltage levels and control signals.

Description of physical layer

This is the layer where sending and receiving of packets are undergoing. The physical layer originally recommended for DNP3 has the following specification:

- Bit serial asynchronous
- 8 data bits
- 1 start bit, 1 stop bit
- No parity
- RS-232C voltage levels and control signals

- CCIT V.24 hardware protocol for DTE/DCE communications.[32]

The DNP3 Users Group Technical Committee subsequently produced a standard for transmission of DNP3 over networks. This provides an alternative definition of the physical layer for that situation. Communications in a SCADA system will generally have a structure where some stations may be identified as master stations (MTU/HMI), and others as slave stations (RTU).In a hierarchical structure (where this paper relies on), At the data link level, the terms balanced and unbalanced are used to describe whether all stations may initiate communications or not. In 'unbalanced' systems, only master stations will initiate communications but here the RTU(acting as a slave) takes the initiative. That is, the RTU will be a primary, or originating, station, and MTU will always be next to RTU. It will wait some time till the MTU/HMI confirms. The DNP3 protocol support balanced communications at the data link level. This provides greater flexibility by allowing non-master stations to initiate communications. In DNP3 any station can be an originator or primary station. .[29,30]

These concepts are illustrated in the following communication sequence diagram. The diagram below shows how these terms relate to the communication process. The diagram illustrates a request for data from a master station to a non-master station. This could be a poll for current data, a 'static' poll. The diagram illustrates the communication sequence by showing the parties on each side, with message directions shown between them. The time sequence is shown from top to bottom. .[29, 30 31]

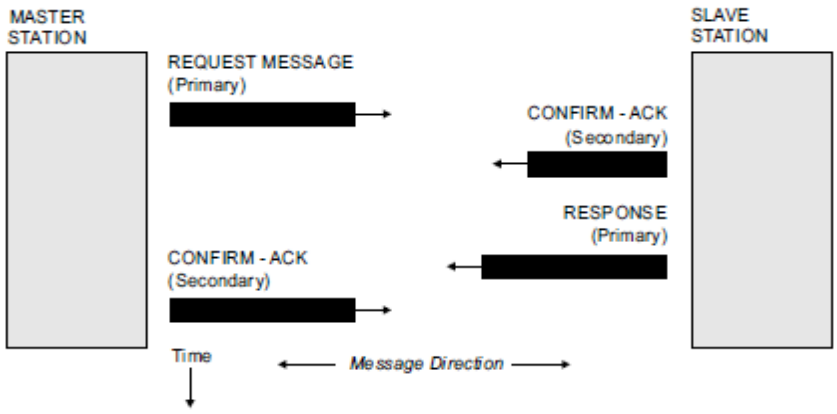


Figure 14: .Example of communication sequence diagram

In the diagram the designated master station initiates a communication with a non-master station. The request message itself is contained in the application layer information within the message. The designated master station has initiated this communication and is therefore the primary station. A response is required to this message at the data link level,

i.e. a confirmation of receipt is expected. The non-master station sends an acknowledgment. This is a secondary message, i.e. a data-link response to the primary message. Note that at the data link level, this transaction is now completed.

Because the last transaction contained an application level request for the transmission of data, the non-master station (namely RTU) then initiates a communication with the requested data. Now the non-master station is initiating the communication, and it is the primary station for this transaction. This is a new communication sequence, or transaction, at the data link level. Although it is related to the prior transaction at the application level, it is unrelated at this level. It can be seen from this example that the terms primary and secondary relate to the station initiating a transaction at the data link level, and not to whether the stations are master or non-master. Although the communications are balanced, and therefore any station can be a primary station and initiate messages, it is incorrect to believe that the terms master and non-master[28,30] have no meaning. In DNP3 stations may be defined as either master or non-master. This information is used at the link level to determine the setting of a message direction bit, the DIR bit. The direction bit is set for messages from a master, and cleared for messages from a non-master station. A final definition that is important to understand is the 'data link' or just 'link'. The link refers to the logical connection between a primary station and a secondary station. It is therefore a one-way communication path or two way communication path. But to establish two way communications between two devices, it is necessary to establish the links in each direction. The logic in this may be better understood by recognizing that a communication channel between two devices can be duplex, using two entirely separate physical media, one in each direction. The simplest example of this is of course a four-wire connection.[29,34]

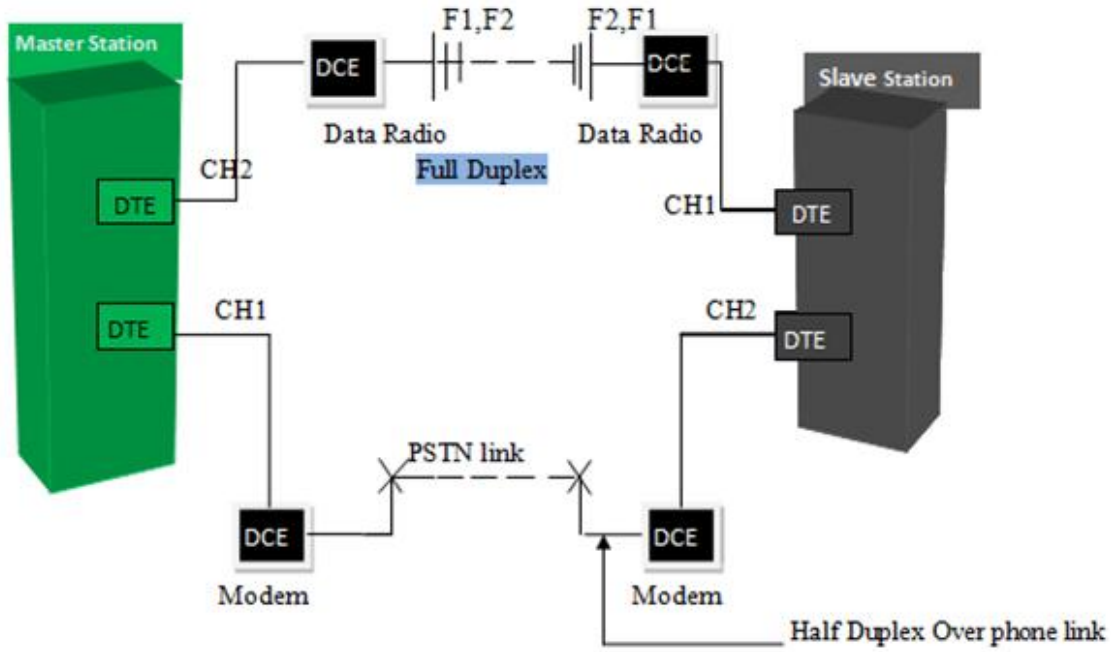


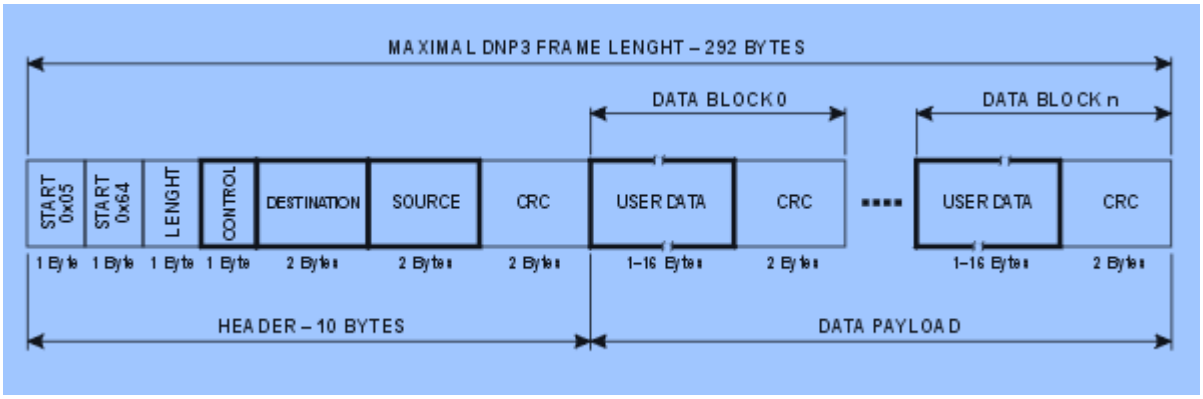
Figure 25: .Basic Communication ways

The following illustrates two communication channel between the Master unit and the non-Master (slave) one. The first channel uses that is from RTU to MTU/HMI(for this paper case) uses half duplex. But from MTU/HMI forwards uses channel two (full duplex).[29].

The DNP3 has a function of controlling transmission at the Data link layer(DLL) by using a control byte defined within the message frame[31],in this case the DNP3 must first defined a procedure that describes what action are to be taken at each during transmission and the control byte provides a coordination between them. The DNP3 is making FT3 frame format and this frame format helps to understand the structure of the message ,the meaning of the information on the control byte and the procedure.[32]

2.3.3.2. What looks the FT3 frame format?

The Link protocol data unit (LPDU) or frame format based on the FT3 format by IEC870.5-1. The IEC870.5-1 has specified four possible frame formats, Among them the FT3 is one that used by DNP3.The format specifies a 10 Byte header,16 data blocks. The overall message size is 292 bytes, which provides for a maximum data capacity of 250 bytes. [28,34]. Generally the frame consists of the header plus 16 data blocks, with the last block having 10 data bytes.



Fixed length Header=10 Bytes

Body 0-282 Bytes

Maximum 16 Blocks

Maximum Data=250 Bytes

Header 10

Body= Data=250

CRC= 32

292

Fig 16. DNP3 Frame format

N.B. Each block has a 16-bit CRC appended to it.

2.3.3.3. DNP3 Header description

SYNC [0x0564]

0x0564The Start field is 2 bytes in length. The first byte is a 05 hexadecimal and the second byte is a 64 hexadecimal too.

LENGTH

The length field is 1 byte in length and specifies the count of user bytes in the frame. The CONTROL,DESTINATION and SOURCE field sizes are included in this count. The minimum value for this field is 5 and the maximum value is 255.

The control field contains the direction of the frame, type of frame and flow control information. Figure 2 defines the fields of the control byte. Station A is defined as the designated master station. Station B is not a master station. The primary station is the originator of the message, the source of the message. The secondary station is the destination station.[33]

CONTROL

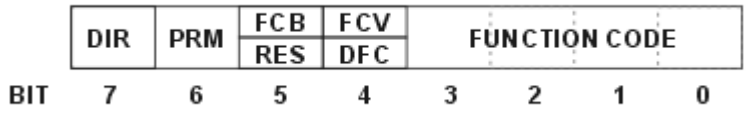


Fig. 6.3 : DNP3 CONTROL

DIR

Physical transmission direction

- 1 = station A to station B

- 0 = station B to station A

Primary Message

PRM

- 1 = frame from primary (initiating station)
- 0 = frame from secondary (responding station)

FCB — Frame count bit

Frame count bit valid

FCV

- 1 = Frame count bit is valid
- 0 = ignore frame count bit

DFC — Data flow control bit

RES — Reserved = 0

FUNCTION CODE — The function code identifies the type of frame. The definition of the values placed in this field is different between primary and secondary stations. The following tables define the implemented codes and associated FCV.

PRM = 1

Function Code	Frame Type	Service Function	FCV Bit
0	SEND – CONFIRM expected	RESET of remote link	0
1	SEND – CONFIRM expected	Reset of user process	0
2	SEND – CONFIRM expected	TEST function for link	1
3	SEND – CONFIRM expected	User Data	1
4	SEND – NO REPLY expected	Unconfirmed User Data	0
9	REQUEST – RESPOND expected	REQUEST LINK STATUS	0

Secondary — PRM = 0

Function Code	Frame Type	Service Function
0	CONFIRM	ACK – positive acknowledgement
1	CONFIRM	NACK – Message not accepted, Link busy
11	RESPOND	Status of Link (DFC = 0 or DFC = 1)

Destination address — The Destination address field is 2 bytes in size and specifies the address of the station that the frame is directed to. The first byte of the address is the low order byte and the second byte is the high order. The address 0xffff is defined as an all stations address.

Source — The source address field is 2 bytes in size and specifies the address of the station that the

address	frame originated from. The first byte of the address is the low order byte and the second byte is the high order.
HEADER CRC	A two byte cyclic redundancy check is appended to each block in a frame.
USER DATA BLOCK	The blocks following the header may contain from 1 to 16 bytes of user data. If more than 16 user data bytes follow the header (block 0), each block must contain 16 bytes of data except for the last block. The last block will contain the leftover. Each data block has a CRC appended to it. [32,33]

2.3.3.4. DNP3 Security

2.3.3.4.1. Introduction

In today's business environment, internal networks are used for all corporate communications, including SCADA. SCADA systems are therefore vulnerable to many of the same threats as any TCP/IP-based system. SCADA Administrators and Industrial Systems Analysts are often deceived into thinking that since their industrial networks are on separate systems from the corporate network, they are safe from outside attacks. PLCs and RTUs are usually polled by other 3rd party vendor-specific networks and protocols like RS-232, RS-485, MODBUS4, and DNP3, and are usually done over phone lines, leased private frame relay circuits, satellite systems, licensed and spread spectrum radios, and other token-ring bus topology systems. [39]

2.3.3.4.2. Need for Security

The SCADA System that was developed in the earlier times has not an issue of being secured because they are free from cyber attack. But nowadays, unlike the previous one today's SCADA system needs a highly secured system due to the presence of Internet connection.[20] The reason of being secured is because of the fact that the nature of SCADA system performance that carries out its critical operation on remote locations which is geographically distant from the base.[19,20] Besides to this, the DNP3 protocol was designed for SCADA communication only. DNP3 was not designed with the security in mind. Industrial Systems are nowadays exposed to new kinds of malicious threats. This resulted into severe cyber-attacks on a SCADA network where DNP3 haplessly failed to the malicious intent of attackers without protection. Several scientific works [20] have showed how SCADA i.e. the systems which control industrial installations, are exposed

to cyber-attacks. These, due to the intrinsic nature of SCADA systems, cannot be avoided by using traditional Information and Communication Technology (ICT) security measures. [20].

Nowadays, the system in general and the protocol in particular exposed to new malicious threats [20, 36, and 37] which results to sever cyber attacks on the SCADA networks where DNP3 haplessly failed to the malicious intent of attackers without any protection.SCADA system, by its intrinsic nature, is mostly exposed to such attacks and this issue cannot be addressed and avoided by using traditional Information Communication Technology (ICT) security measures.

Modern Critical Infrastructures which are making use of SCADA like Rail ways, are still largely dependent on ICT to harness new features and carry out operations. In particular, according to a relatively new trend, several of the maintenance and management operations related to such installations, are conducted remotely taking advantage of public networks i.e. Internet. This has contributed by making the process fast and efficient but on the other hand it has exposed such critical operations to new sources of possible threats. In fact, connecting together the critical systems by using the Internet have opened new virtual gates to those interested in damaging such critical infrastructures. The ICT security measures like firewalls, antivirus or intrusion detection is simply not sufficient enough and proves to be too cumbersome to maintain.
The flow of data in every SCADA system is totally dependent on the communication protocol (e.g. ModBus, DNP3 etc.). By using these protocols it is possible perform any operation. [20]

2.3.3.4.3. Security Problems arise at DNP3

DNP3 cannot address the following issues with regard to security
i). Master and slave do not authenticate each other. This scenario is extremely dangerous, since, an attacker could take the control of the critical installation.

ii). an attacker could send to the master fake slave reply packets, with false information about the state of the system. In this case, the attacker will be able to eventually hide state of the system

2.3.3.4.4. Possible Solutions To the problem

To improve DNP3 security

The approaches that can be examined to improve the DNP3 security enhancements in SCADA communications to reduce the vulnerability of cyber attacks are
a). Altering DNP3 fundamentally [35]b). Wrap the DNP3 protocols without making changes to the protocols.[34].

a) Solutions that alter DNP3 fundamentally

The security issue of protocols should not be an additional overhead issue and must not affect the overall performance of the system. This approach examines changing the protocol internally by adding an authentication mechanism in its application layer. The main objective of altering the DNP3 protocol internally is to provide authentication.

The protocol model when this mechanism is added will serve the following: A DNP3 outstation can use to unambiguously determine it is communicating with a user who is authorized to access the services of the outstation.

A DNP3 master can use to unambiguously determine that it is communicating with the correct outstation. [37]

b). Solutions that wrap DNP3 into external secure protocol

I) SSL/TLS

This is an approach which is exactly opposite of the previous approach. As mentioned earlier this approach does not change the protocol internally but tries to run it on a secured medium. SSL (Secured Socket Layer) /TLS (Transaction Layer Security) secures the communication channel to carry out traffic over the TCP-IP. This mechanism secures the communication channels in order to carry out reliable communication over DNP3 and is in use for about a decade providing private network for the Internet users. SSL/TLS secures communication between a client and a server by allowing mutual authentication and provides integrity by using digital signatures and privacy via encryption.
How SSL works with DNP3.
The secured socket layer is placed between a reliable connection dependent protocol like a TCP-IP and DNP3 packets are sent over it. This mechanism provides a secure communication between a remote DNP3 Master and a SCADA DNP3 outstation. Security techniques like mutual authentication, digital signatures and encryption are achieved automatically with this technique at a low cost as they come with SSL-TLS itself. The

protocol is also designed for specific algorithms used for cryptography, digests and digital signatures. [38]

SSL Session Establishment

The SSL session is established when a handshake sequence happens between a client and server as shown in Figure 44.

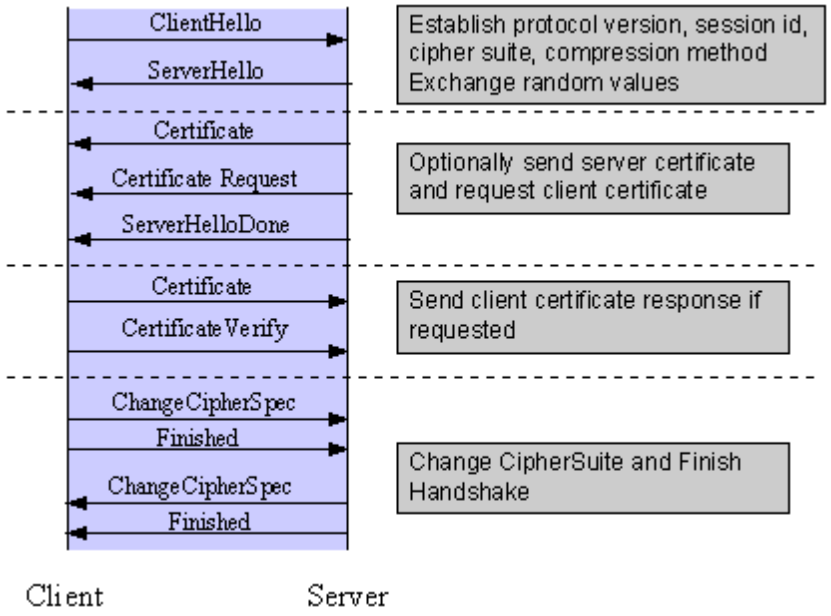


Figure 17 SSL handshake sequence [38]

The steps in authentication are:

1. Negotiate the Cipher Suite to be used during the transfer
2. Establish and share a session key between communicating entities
3. Authenticate the server to the client and vice versa. [38]

2.3.3.4.5. Improvements obtained

The following security threats are successfully defended with this approach.

- **Spoofing** –a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. [14]

- **Modification-**Here there are two kinds of attacks namely; Active and passive. The active attacker removes a message from network traffic, alters it, and reinserts it,

because it involves an attempts to change information; in comparison, a passive attacker, such as password sniffing, seeks information but does not itself modify the valid information, although it may be used in conjunction with an active form of attack for various purposes." [38]

- **Replay-** A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an opponent who intercepts the data and retransmits it, possibly as part of a deception attack by IP packet substitution [38].

- **Eavesdropping-** The attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. [17]

- **Non repudiation-**Non-repudiation refers to a state of affairs where the purported maker of a statement will not be able to successfully challenge the validity of the statement. [18]

2.4. Review of Related Work

Safety is the prime consideration for public transport systems, and that includes level crossings. Because a level crossing affects both railways and roadways, accident is there common opponent. In order to prevent or control this hazardous effect, sectors involved in this area have tried their best and implement different mechanisms to control the problem. Due to this, so many researches were conducted to achieve optimum accident prevention, but the problem still exists all over the world [45]. This is due to the fact that none of them can provide appropriate solution to alleviate the problem considering nearly all operational constraints. Here, seven paper works on the issue of level crossing accident preventing mechanisms are discussed.

Reference [5]: This paper aimed at explaining system configuration, philosophy of system designing, and short distance track circuit for level crossing using computerized system. The reason why the paper introduced a computerized system, as it explains, is using track circuit system alone can't alleviate the problem. This is because of the fact that track circuits fail to detect an obstacle at the level crossing. On the contrary, the computerized system of level crossing is cheap and can make it standardized easily;

besides to this, it has an advantage of fail-safe, high reliability and easy construction and maintenance. It doesn't provide remote monitoring and control of the level crossing system.

Reference [6]: This paper describes and explains about intelligent railway crossing control system for multiple tracks that features a controller which receives messages from incoming and outgoing trains by sensors. These messages contain detail information including the direction and identity of a train. The objective of this paper is on how to reduce accidents at level crossing by controlling railway crossing gate automatically using radio link. This system can be implemented both on single and multiple tracks. The main facility of this system is that it can be merged with the existing system. The initial cost of the system is high but maintenance cost is very low. Power consumption of the system is low.

Reference [7]: This paper discussed about how level crossing accidents is going to be controlled using unmanned level crossings system using sensors. It begins with explaining about the lateness of the area that fruitful steps have not been yet taken so far. It targets to fill the gap of accident prevention using automatic railway gate operation at a level crossing replacing the former method of gates operated by the gatekeepers. Its focuses on two things:

1. It deals with the reduction of time for which the gate is being kept closed and
2. To provide safety to the road users by reducing the accidents.
3. By employing the automatic railway gate control at the level crossing, the arrival of the train is detected by the sensors placed near to the gate. Hence, the time for which it is closed is less compared to the manually operated gates. The operation is automatic; error due to manual operation is prevented. Automatic railway gate control is highly microcontroller based arrangements, designed for use in almost all the unmanned level crossing in the train. But the truth is, it is very much distance limited. But the SCADA system can facilitate the controlling mechanism with distance much better. [6]

Reference [8]: The paper starts with describing about the existing crossing barrier and warning devices that are simple train-oriented protection equipment which cannot take measure accordingly. To solve this problem, it proposes "intelligent level crossing system", that dreams to improve the overall level crossing control technology and reduce the accident drastically. The system uses wireless transceiver that can be applied to train-ground communication for control command transmission, and the image processing and

train tracking algorithm are also used for train detection and control. But here, the image processing is time taking and depends on the weather condition. But the SCADA system able to control the level crossing without performing such processes.[10,19]

Reference [9]: Level crossing gates are operated manually by a gatekeeper. In this regard, the gatekeeper will operate the railway gate after receiving the information about the train's arrival. When a train starts to leave a station, stationmaster of the particular station delivers the information to the nearby gate. This paper proposes developing automatic railway gate operation to prevent accidents at unmanned gate and automatic closure of unmanned gate; moreover, the system has equipped with a fail proof system to avoid such accidents. The unmanned level crossing is fitted with obstacle sensor and automatic gate closing mechanisms and Zigbee. The PC in the master control room will receive information via Zigbee from the train and continuously estimate the distance between the train and the unmanned gate. But here the distance is known due to the placement of the sensors.[10,32]

Reference [10]: Unlike the present day, previously the level crossing railway gate is operated normally by a gatekeeper. It gets information about the status of the train from the station master and act accordingly. To improve this highly backward way of controlling the gate at level crossing, it proposed a microprocessor based controlling mechanism that would implement together with sensors and communication equipment. But the communication system they implemented was Public Switched Transmission Network (PSTN) (fully wired.).But here it implements wireless communication.[10]

Chapter Three

Modeling of the proposed system state-of-the art

3.1. Proposed Intelligent Accident Prevention System

3.1.1. Intelligent system introduction

The term “accident", in general, is an unplanned, unexpected, and un designed (not purposefully caused) event which occurs suddenly and causes injury or loss and decrease in value of the resources, or an increase in liabilities[21]. Such accident scenarios are very common in any transportation system.

The ever increasing number of newly fabricated vehicles with the existence of much narrowed highways can be taken as one of the primary case in transportation system accident. As a result, it led to heavy traffic congestion which further results an increase in the number of car accidents besides, violating the level crossing regulations contributes the occurrence of serious accident at level crossings.

Many researchers have been proposing and trying to implement different schemes to prevent level crossing accidents; in spite of this, the problem still exists and this implies that advanced technology in this area is highly required to prevent accidents at level crossings.

The main aim of writing this paper is to implement new accident prevention techniques that will highly reduce the amount of accidents occurred at LC.Figure shows the proposed system architecture that employs an intelligent system at level crossings. The intelligent level crossing accident prevention system provides warning information to train and roadside traffic adjacent to a level crossing, using a wireless two-way communication link in Slave-Master approach, for the purpose of preventing accidents and reducing damage. Level crossing events (like warning messages) and wayside-equipment information about obstacles on the crossing (vehicles and pedestrians, etc.) are transmitted to a train from the level crossing, and information related to the train (direction, velocity, distance, etc.) is processed and the traffic lights to the vehicles and pedestrians is controlled.

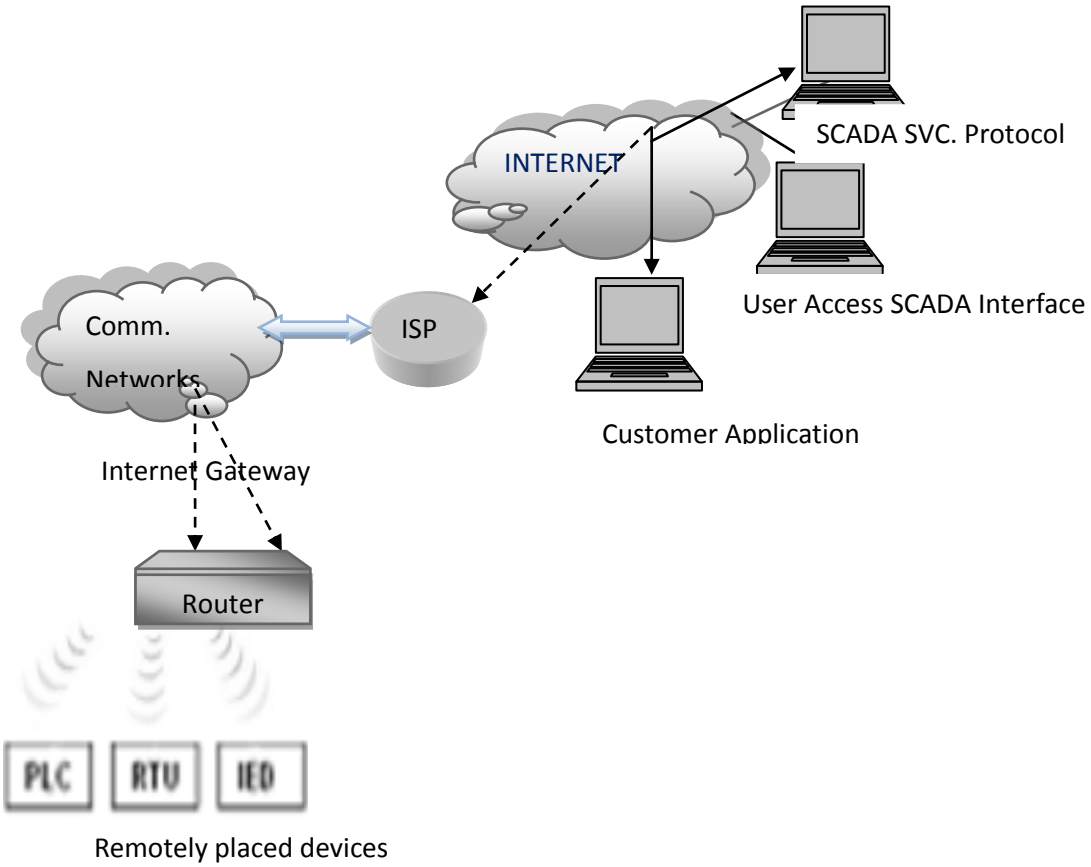


Figure 18: Wireless SCADA Architecture

3.2. Models of the System Model

3.2.1. Component of the system model

This section introduces our intelligent level crossing control system components.

1. Train model in AALRT case

The following data were obtained from AALRT:.

- The total length of N-S line is 16.674 km long and has 22 stations.
- The minimum interval between two stations is .435Km and maximum is 1.161Km
- Kality Depot is set near to the terminal point of the N-S line.
- The total length of E-W line is 16.998 km long and has 17 stations.
- Ayat Depot is set near to the terminal point of the E-W line.
- The common rail section2.61km and the average interval between stations is 0.798 km.
- The common control center for the E-W and N-S lines is provided in the Kality Depot.

- A train is passing the level crossing every 1.27 minutes for N-S line [22]. Maximum running speed of not more than 70 km/hr [22].

Terminologies

A Train is characterized by its maximum permissible speed (70Km per hr.For this particular case),its deceleration rate(-1m/s2), the time delay for the deceleration rate to become effective, its length and its permission to exceed certain classes of track speed restrictions.

ATP – (Automatic Train Protection) is a predictive enforcement system which continuously monitors the speed of a train in relation to either a target speed, which for a Limit of Authority would be zero, or a target distance, and intervenes such that the train is prevented from passing a Limit of Authority or exceeding a speed limit.

Braking Distance is the distance travelled by a train between the point at which the driver initiates a brake application and the point at which the train eventually comes to rest. A train travels along a rail line obey all speed limits at every location of the line. In this case, the initial and final speed must be calculated. At initial time the locomotive must reach to the initial running point and at final time it must reach to the destination point [21].

Emergency Braking Distance is the braking distance for a train when it has been subjected to an "emergency" brake application. Emergency Braking Distance may be used in determining the minimum overlap distance to be provided beyond a stop signal [21].

A Typical Grade Crossing Analysis

The area in front of the train can contain a number of targets with different target and release speeds. Suppose initial speed is 0 m/s

A train is passing the level crossing every 1.27 minutes (90 sec) for N-S line [22].When compared to other modes of ground transportation trains have some unique characteristics that require special analytical consideration. The length of a train and its associated pneumatic brake systems, determining the train weight and calculating brake force are all variables that appear in stopping distance calculations. While running steel wheels on steel tracks greatly increases a train's load-carrying capability, these materials limit the ground forces available so that velocity changes in trains occur relatively slowly.

Calculate the braking distance

In general

$AV(0,0) = V(d,T) = 0; X(T) = d, X(0) = 0 - - - - - - (1)$ Under normal condition

From Equation (1), it is possible to have

$$S = V * T - - - - - - - - - - - - - - (2)$$

Where S= Distance, V=Speed, T=time

First let's determine the reaction distance using an average crossing time of 1.27min (0.025hr).

Since.Speed $= 70 \frac{Km}{hr}$ or $19.44 m/sec$

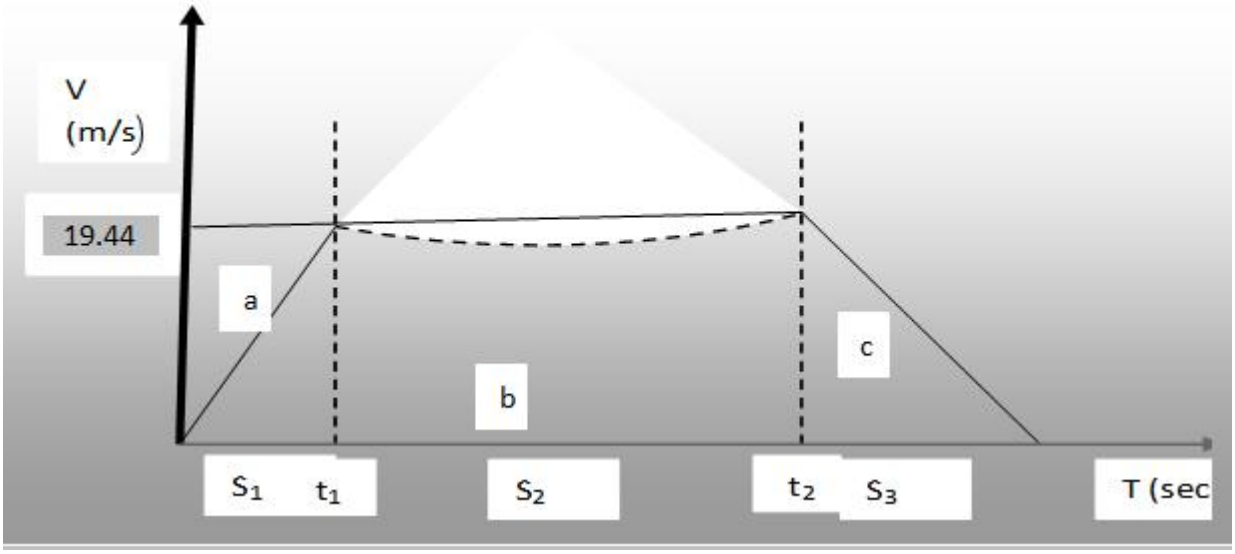


Fig 19 Train Speed profile frame work

From Newton First law of motion

Where S: distance travelled by a body.

a:accelarationS $= \frac{V_f{}^2 - V_i{}^2}{2a} - - - - - - - - - - - - (3)$

Vf: Final speed and Vi: initial speed

$$\left\{ \begin{array}{c} S_T = S_1 + S_2 + S_3 \\ S1 = \frac{Vf^2 - Vi^2}{2a} \end{array} \right\} - - - - - - - - - - (4)$$

Thus

Since the final velocity is 70km/hr. (19.44m/s), the initial velocity is 0m/sec. and acceleration is

$$a = \frac{1\text{m}}{\text{s}^2}, \quad S_1 = \frac{19.44 * 2}{2}\text{m}, \quad \text{thus} \quad S_1 = 189\text{m} = 0.189\text{Km}$$

$$S_3 = \frac{Vf^2 - Vi^2}{-2a} - - - - - - - - - - (5)$$

$$S_3 = -(19.44) * 2/(-2)$$

To calculate the distance S2.

The distance connecting the two lines is not straight, has curvilinear motion.

The Truck geometry is a crucial fact for top speed and having sharp curves. The circular curves have characteristics of having curvature resistance. For calculating the traction force Ft.

$$M_e * a = F_t - F_r - F_g - F_e - - - - - - - - - (6)$$

Where Me is effective mass (Kg)

a=acceleration in m/s2

F_r=running resistance force

F_g=Gravitational resistance force

Here, the Curvature resistance force need to be calculated by the formula given by $Fc = Me * g * (1/1000) * (700/R)$. Where R is curve resistance.(It is standardized value is 22.125).[9]

Where F_c=Curvature resistance force

And from Newton 2nd law of motion $F=M_e*a$.

Thus

$$M_e * a = M_e * g * (\frac{1}{1000} * \frac{700}{R}$$

$$a = g * \frac{1}{1000} * \frac{700}{R}$$

Here Me cancels out and g=10 m/s2

$$a = 10 * \frac{1}{1000} * \frac{700}{R}$$

$$a = \frac{7}{R}$$

$$S_2 = \frac{R * Vf^2}{14} - - - - - - - - - - (7)$$

$$S_2 = 0.5974\text{Km}$$

Therefore $S_T = S_1 + S_2 + S_3$

$$S_T = .1895 + .1895 + .5984$$

$$S_T = 0.9774\text{Km}$$

b) But when considering influencing factors. The Braking distance depends on

- The speed of the train
- Deceleration rate/acceleration (±a) depends on the coefficient of friction between wheels and rail.
- Brake delay time: time between commanded and acted.
- Geography of the track.
- The mass of the train

The locomotive that AALRT (ERC) has rated power of 130KW with rated speed of 1800rpm and maximum speed of 4377rpm [32]. Maximum torque is obtained during maximum power. Speed of the motor for maximum torque must be lower than synchronous speed [32].

$$T_R = \frac{P_A}{W_R} - - - - - - - - - (8)$$

Where: T_R=Rated Torque W_R=Rated Speed

$$T_M = \frac{1300w}{1800R_{PM}} = 72.22ws$$

P_M =Maximum Power W=Maximum Speed

But to achieve the stability $\frac{T_M}{T_R}$ is 2:3; however, stability is better if the ratio is>=1.6 [33].

Thus➔T_M=1.6TR

$$T_M = \frac{P_M}{W} = 116ws$$

But from Stephen chapmen (4th edition) TM is occurred at (20-30) % of slip.

Let us consider 6 poles as used by AALRT with a frequency of 71hz [22] and get the operating speed of the train for the maximum torque

$W = W(1-s) * W_{Synchronization}$ but $W_{synchronization}$=(71/6)*120= 1420rpm.

But Synchronization<W_{rated} (1420<1477).But if the number of poles are reduced to 4; $W_{Synchronization}$=(71/4)*120= 2130rpm.In this case

The maximum torque happened at 25% of slip.=2130(1-1/4)=1597.5rpm

Thus $P_{Max} = 116 * 1597.5\text{rpm} = 184.6\text{kw}$

The maximum tractive force that can be developed at the rail is equal to the weight on drivers multiplied by the adhesion (coefficient of friction) of the wheels on the rail. And adhesion is affected by the wheels on the rail condition and speed.[33]

Calculating the tractive force (F_{tr}).

$F_{tr} * V_{base} = P_{Max} *$ number of polesbut Vbase=41km/hr

$$F_{tr} = (184.6\text{Kw} * 4)/(41\text{km/hr}) = 64.83\text{KN}$$

❖ The normal (speed) brake must be applied at a distance 1.26 Km from the level crossing to the point of axle counter [23].

The train braking distance can be calculated from parameters like type of train and the gradient of the track. But to compensate those factors (15 to 20) % is usually added.[23] .

The theoretical braking distance can be found by determining the work required to dissipate the vehicle's kinetic energy

The kinetic energy **E** is given by the formula:

$$E = \frac{MV^2}{2} - (9)$$

Where **M** is the vehicle's mass and v is the speed at the start of braking.

The work **W** done by braking is given by:

$$W = \mu MgD - - - - - - - - - - (10)$$

Where **μ** is the coefficient of friction between the road surface and the tires, g is the gravity of Earth, and d is the distance travelled.

The braking distance (which is commonly measured as the skid length) given an initial driving speed v is then found by putting W = E, from which it follows that

$$d = \frac{v^2}{2\mu g} - - - - - - - - - - - - - - - - - - (11)$$

. The maximum speed given an available braking distance d is given by:

$$v = \sqrt{2\mu g} - - - - - - - - - - - - - - - - - (12)$$

❖ **EmergencyBrakedistance**

The maximum brake force available to the driver from his conventional braking system. The brake applies considerably more braking force than the standard full-service brake. [23].

A computer on the train is provided with inputs for grade information, axle speed, brake pipe pressure, and locomotive tractive effort. During brake applications when the train is in motion. [34].

The total stopping distance is the sum of the perception- reaction distance ($D_{p\text{-}r}$) and the braking distance ($D_{braking}$).

$$D_{Total} = D_{p-r} + D_{braking} = vt_{p-r} + \frac{v^2}{2\mu g} - - - - - - - - - - (13)$$

Known Are: μ=0.05,g=10m/s^2 and assuming $t_{p\text{-}r}$=10sec(standard perception time to react towards LC).Thus the braking distance becomes 397.53m or 0.398Km.

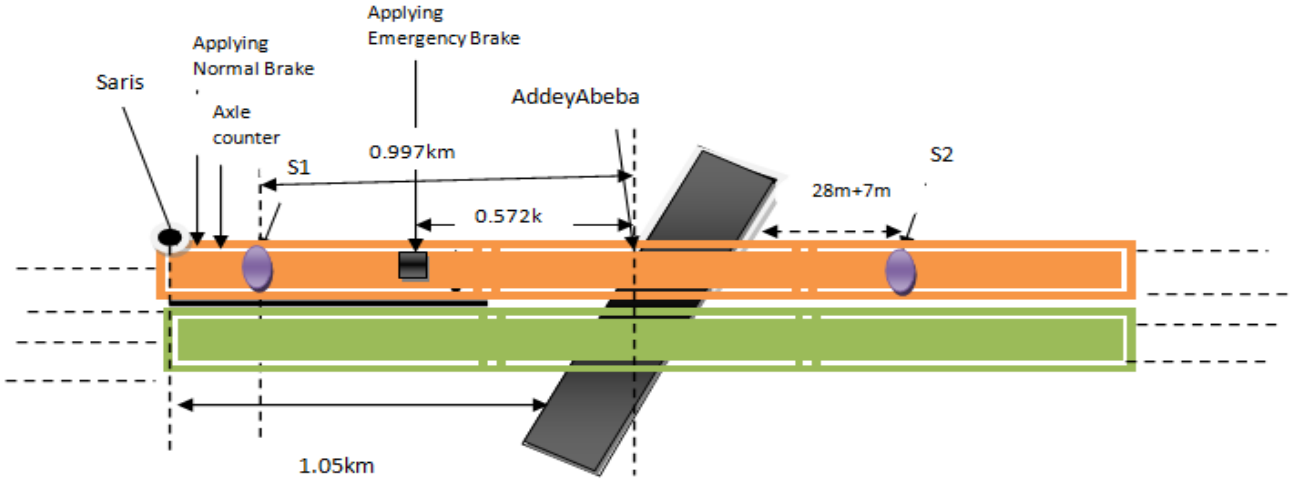


Fig. 20 showing placement of sensors

Where S1 and S2 are sensors

2. Signaling Model

The primary purposes of a signal system on a rail system are:

- **Train detection**: for providing positive location of trains;
- **Train separation**: to protect a train from a collision with a train ahead operating on the same track;
- **Train routing**: to provide protection against conflicts and to verify safety of train movements at Crossover locations or at interlocking; and
- **Movement authority**: to provide authority for the movement of trains on the right of way.

The secondary purposes of a signal system on a rail system may include:

- Positive stop enforcement;
- Broken rail detection; and
- Control of train speeds.

The primary of signaling model is to determine the signal light arrangement for both road traffic and railway traffic. In addition, it provides the working principle of the signaling component under different operational scenarios. The detail of the signaling operational scenarios can be found the next sections.

3.2. 2. Elements being considered while system modeling

When modeling a preemption system, many important items should be considered. These include

- distance between the tracks and signal,
- intersection and crossing geometry,
- approach speed of trains and vehicles,
- vehicle flow rates,
- vehicle size and classification;
- and operation of the traffic signal controller unit.

The flashing light system should be considered for traffic signals located greater than 60m from the crossing. Coordination could include, for example, queue detection that would omit some signal phases or activate variable message signs. [13].

There are cases where

- ❖ The traffic signal is green and the gate is closed to let train pass, while an obstacle exists at the level crossing. So advanced pre-emption system should be employed to tackle this kind of the problem.
- ❖ If a vehicle that wishes to cross to the level crossing should first stopped , especially if the traffic signal is green; however, there is a probability that this may not be done, due to some technical problem of the vehicle being crossing[6].To solve this kind of difficulty some additional gate delay time may be needed.
- ❖ If the traffic approaching the level crossing has got a queue, it must have a mechanism of blocking adjacent intersection to harmonize the traffic flow [13].

And the queue length (L) can be calculated as:

$$L = \begin{Bmatrix} 2q_r * (1+p) * 25, & {}^{V}/_{C} \leq 0.9 \\ (2q_r + \Delta x) * (1+p) * 25, & 0.9 \leq {}^{V}/_{C} < 1 \end{Bmatrix} - - - - - - - - - - - (14)$$

Where

- L is length of queue (in meter)
- q Vehicle flow rate(in vehicle/lane/sec.
- r effective red(red+ yellow)(in sec)
- proportion of heavy vehicle in traffic flow(as a decimal)
- Factor 2 for random arrival interval.
- Factor 25 represents the effective length of a passenger car (vehicle length space

between vehicles).

- Δx=100*(v/c-.9)
- The volume capacity ratio (v/c) of the signalized varies between 0.9 to 1.

The factor r represents effective time that the crossing would be blocked by a train and can be estimated as:

$$r = 35 + L(1.47 * V) - - - - - - - - - - -(15)$$

Where

$$L = Train\ Length - - - - - - - - - - -(15)$$

$$V = speed\ in\ Km/Hr$$

The factor 35sec is obtained by summing up time of crossing would be blocked by the gates for 25 sec before the train enters the crossing plus 10 sec after it crosses the crossing.

1.47 is a speed adjusting factor.

3.2.3. Evaluation of the System based on Reliability and Maintainability

3.3 System Overall Flowcharting

The following flow chart is describing some of the key areas that the level crossing is influenced. These are: Obstacle detection, Signal box Response, train crossing procedure, On Board Alarm Flow chart, Automatic Gate Control System, for the traffic light, for main control System. Each is described below.

Regarding Obstacle detection system, it is typically computing the position of obstacles relative to a mobile agent by using range information. Range information may be obtained from equipment at the level crossing (laser ranging) [14], sonar (sound ranging) [17, 20] or vision based techniques. The Level Crossing Obstacle Detection System, named LOD, scans the crossing area immediately after the barriers are closed to detect the presence of any obstacles can potentially cause accident, only if the area is free than the signals are cleared and the trains can pass safely at the level crossing. [9].

In dealing with level crossing, the obstacle that exists at the level crossing takes priority. That means, removing or taking the necessary action before the arrival of the train is the first duty left to the controlling system.

3.3.1. The Obstacle Detection flowchart

The flow chart below describes how obstacle is detected on level crossing. In this case, before providing the necessary output to others, it starts from the existing status of RTU which dictates the operation that flows from it. Here it checks whether there is an obstacle or not. It also has the capability to exhibit the type of obstacle exist at the LC.

In the end, before it output and stores the final appropriate information, there are cases that should be checked and evaluated incessantly showed through looping. Before a train is allowed passing the LC, it must get the appropriate information whether there is an obstacle or not.

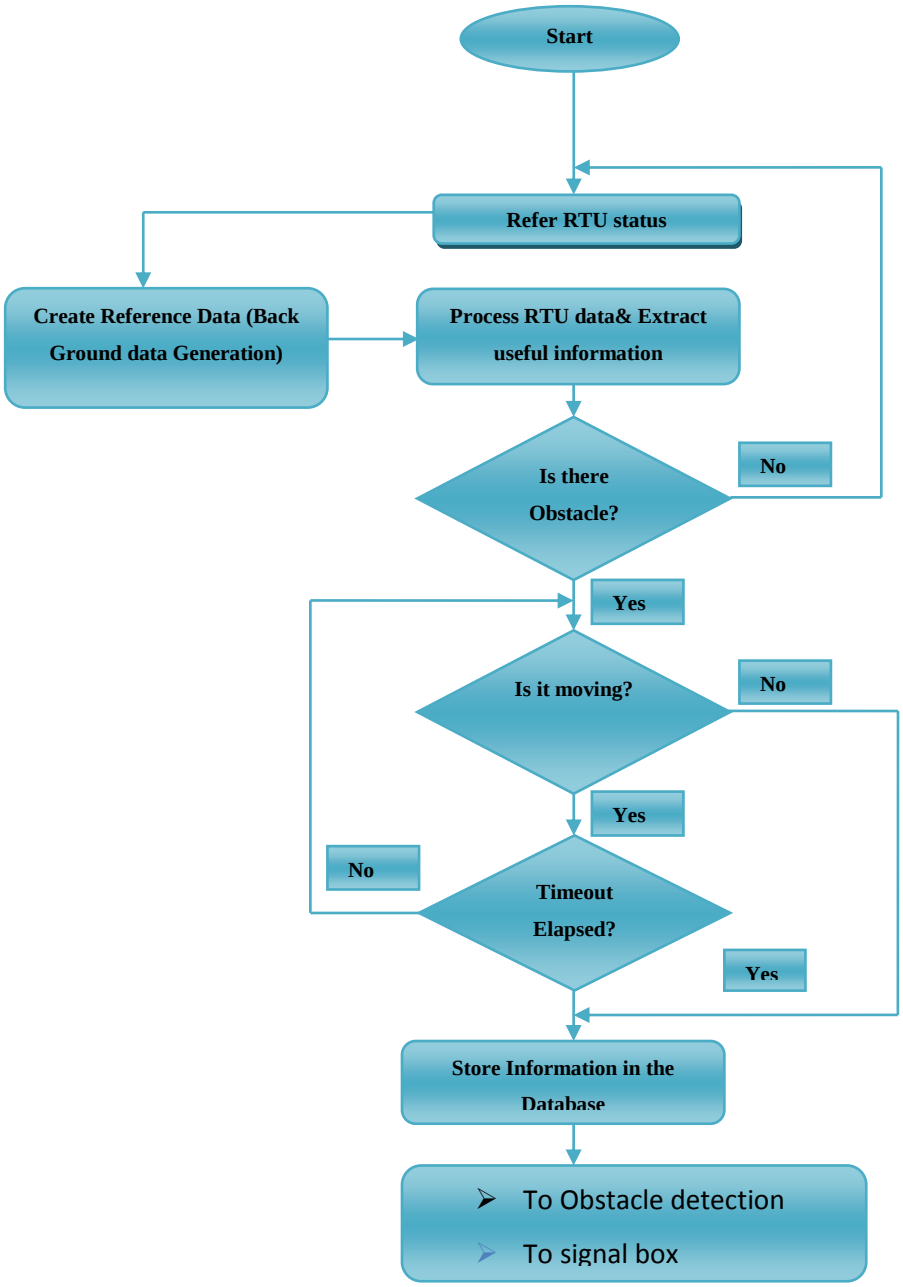


Figure 21: Flow chart for Obstacle detection

3.3.2. The Signal box Response flow chart

The signal box responding flow chart gets the necessary input data from the obstacle detecting flowchart (above).It then starts controlling the three aspect traffic signals based on the status of the level crossing with respect to the existence of an obstacle or the condition of train.

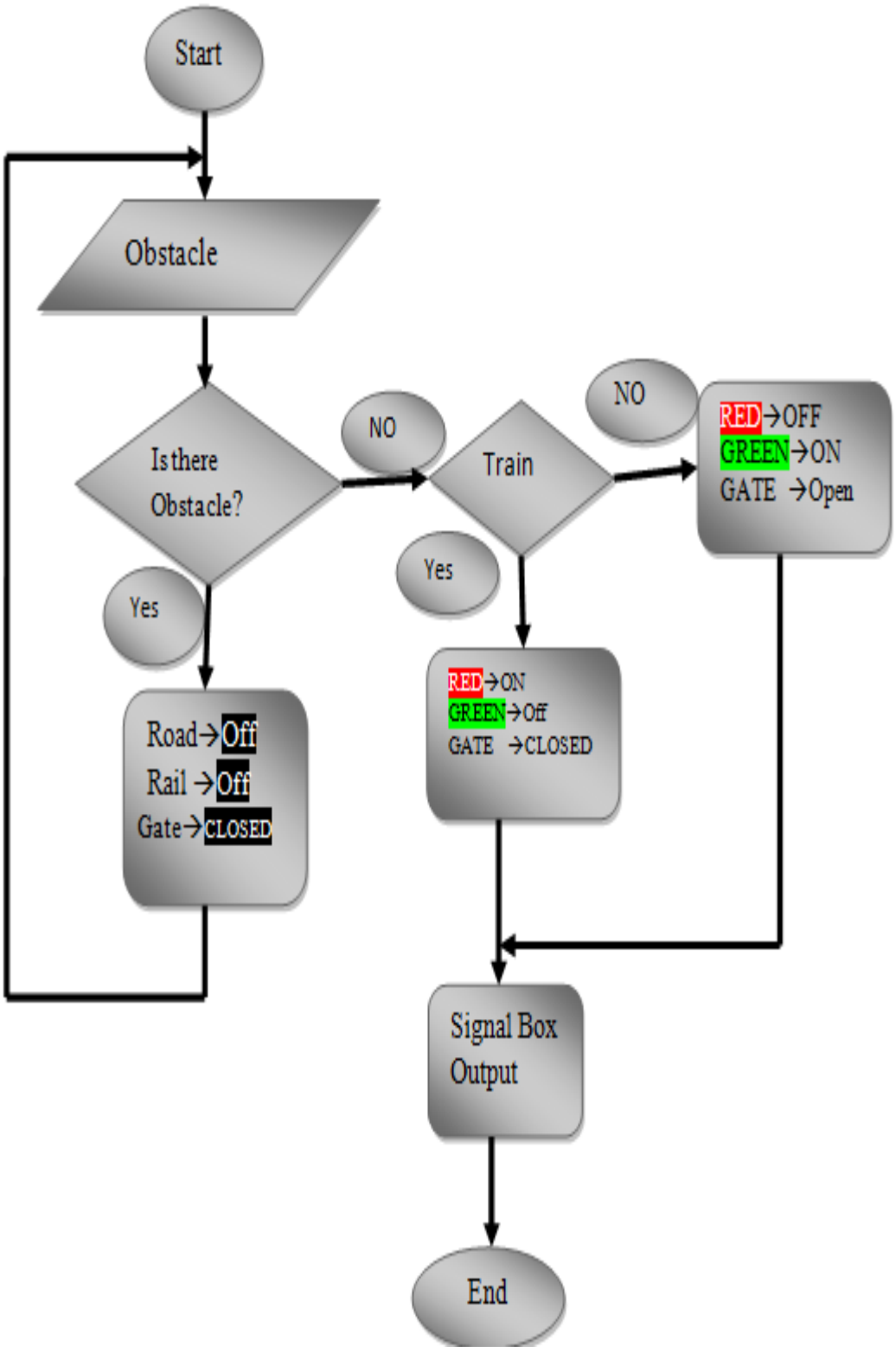


Figure 22 Signal box Response Flow chart

3.3.3. The Train Crossing Procedure Flow Chart

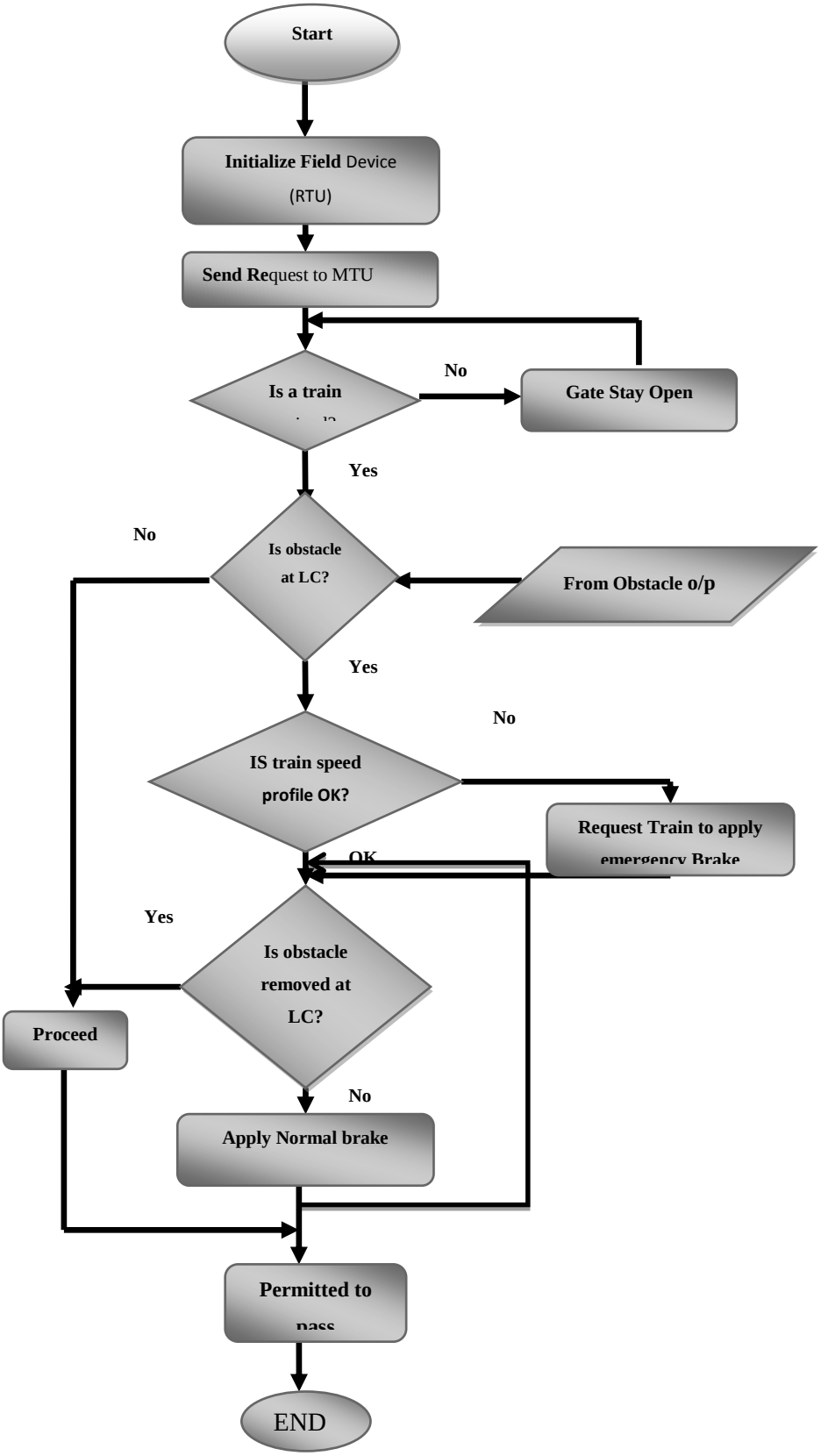


Figure 23:Flow chart for train crossing procedure

The train crossing procedure flow chart explains the course of action for allowing a train to cross the level crossing without any difficulty is based on the following steps:

1. Arrival of train
2. Checking the obstacle existence intermittently.
3. Do a Cross checking of Speed profile of the train in relation to what is in hand for the train being arriving.
4. Finally, by having the proper information, the train will get the opportunity to pass.

3.3.4. Alarm system subroutine (On board monitoring)

This subsystem is installed in the cab of the train. Warning messages and real-time information of any obstacles are provided to help the train driver notice obstacles and stop the train before the level crossing. If the train driver fails to react appropriately, this system is designed to immediately deploy the emergency brake. The alarm system subroutine includes flashing light, buzzing sound to attract the attention of the train controller and motor control to deploy automatic braking.

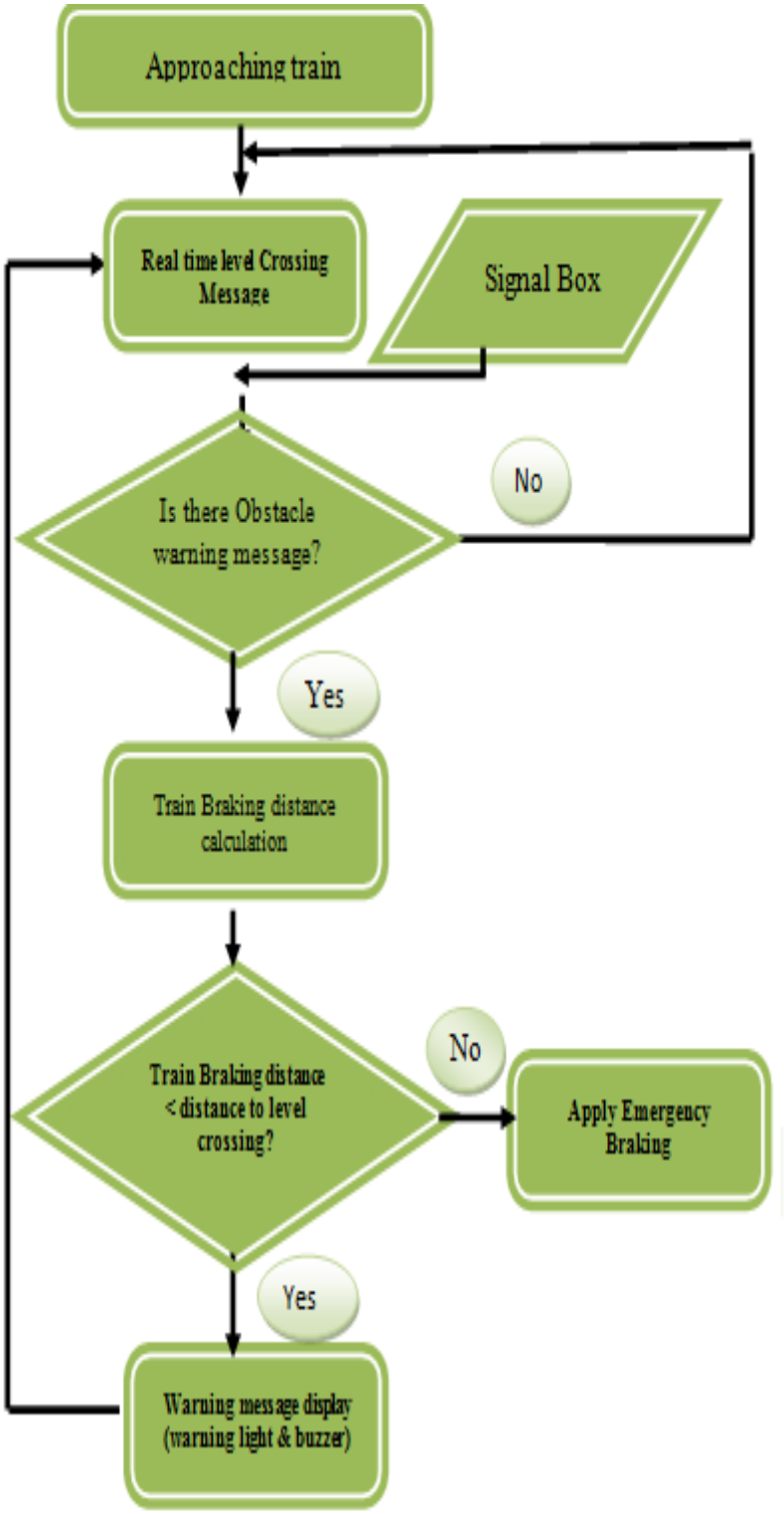


Figure 24: On board Alarm Flow chart

3.3.5. Automatic Gate Control System

This flow chart precisely describes the operation of gate control system based on the obstacle, the condition of sensors S1 and S2.

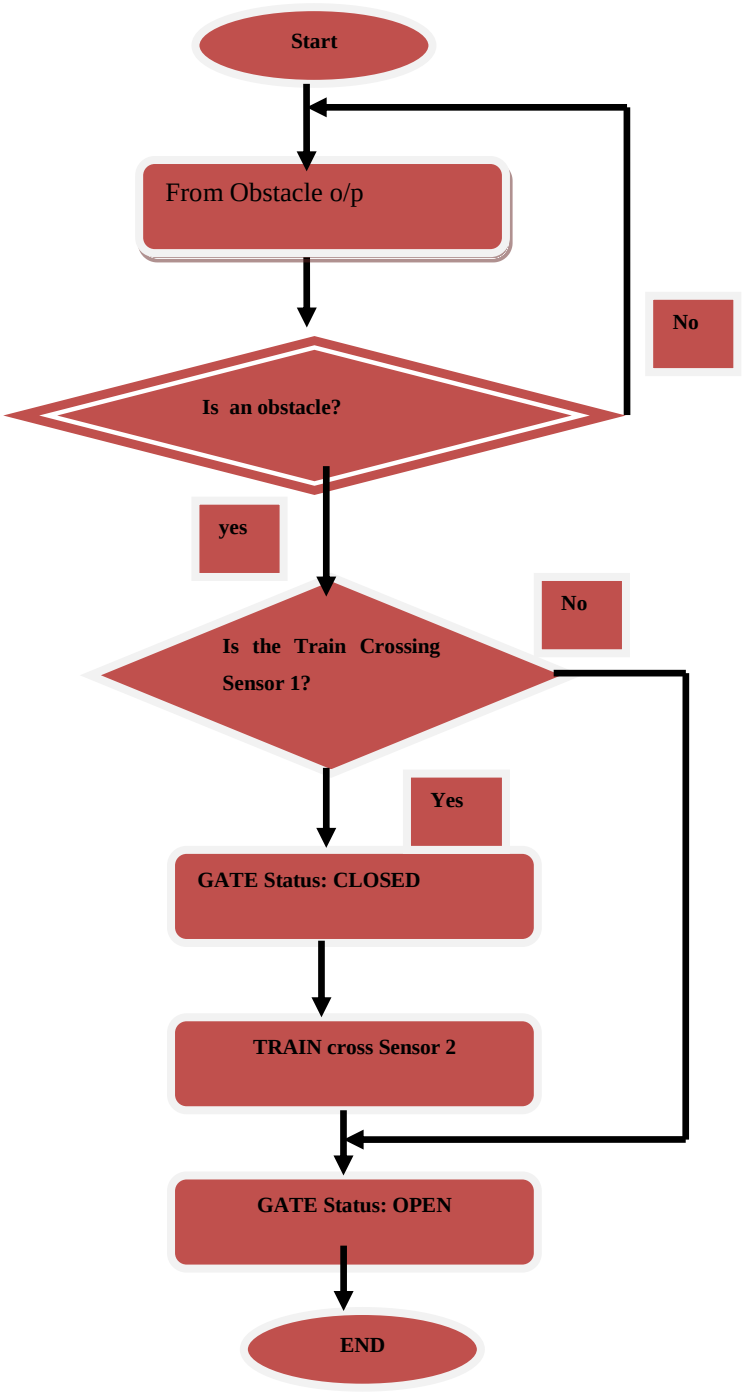


Figure 25. Automatic Gate Control System flow chart

3.3.6. Flow chart for the Traffic Light

The level crossing is a common place for the train, vehicles and pedestrians. To manage and use the level crossing effectively, integrating or synchronizing the traffic light along the road with the signal light along the rail especially, at the level crossing.

The procedure that should be followed to carry out this duty are:

1. Getting an obstacle detected information.

2. Check for obstacle.
   - ✓ If it exists both the road and rail signals will be RED, gate will be CLOSED
   - ✓ If No, Check for the status of the train and give priority to it if it is on the way to cross.
3. Check for the undetermined case. This is the case where When it is hard to determine the existence of an obstacle due to different cases such as:
   - ✓ If the instrument at Lc is fail to work.
   - ✓ Unfortunate Environmental condition

3.1 Check for sensor S1.

3.2 Condition of train whether it is passing or not. If not go to 3.1

3.3 If yes, distance from the LC is checked whether it is less than 1km.

3.3.1. Yes, "RED" signal will be glows.

3.3.2. If No, the train distance is checked (1km<R<2km)

3.3.3. 1.if yes, "Yellow" signal will be shown.

3.3.3.2. If No, "Green" signal will be displayed.

4. End.

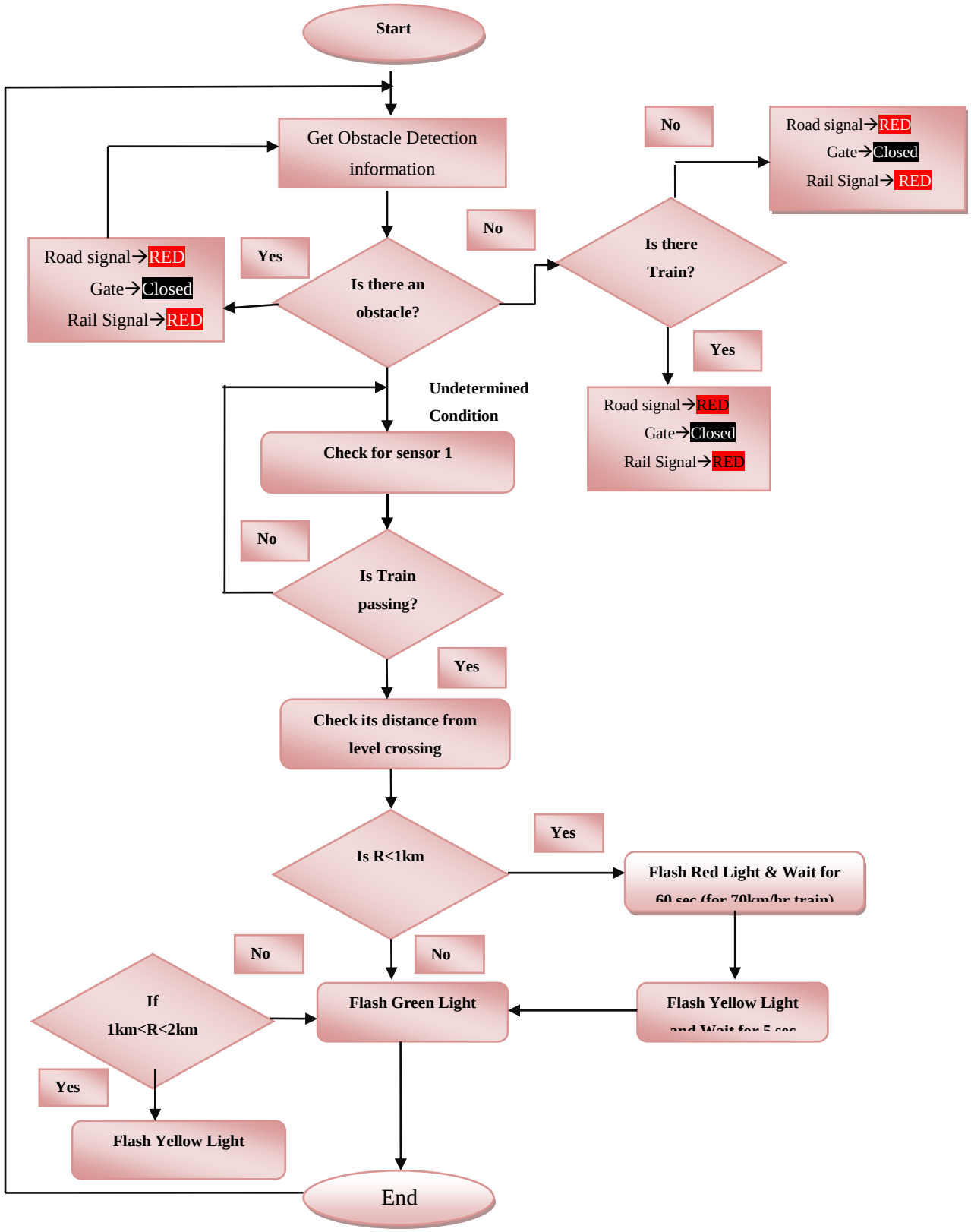


Figure 26:. Flow chart for the traffic light

3.3.7. Flow chart For Main Control System

This flow chart describes how the central system controls the overall level crossing through message exchange between the central system and the train.

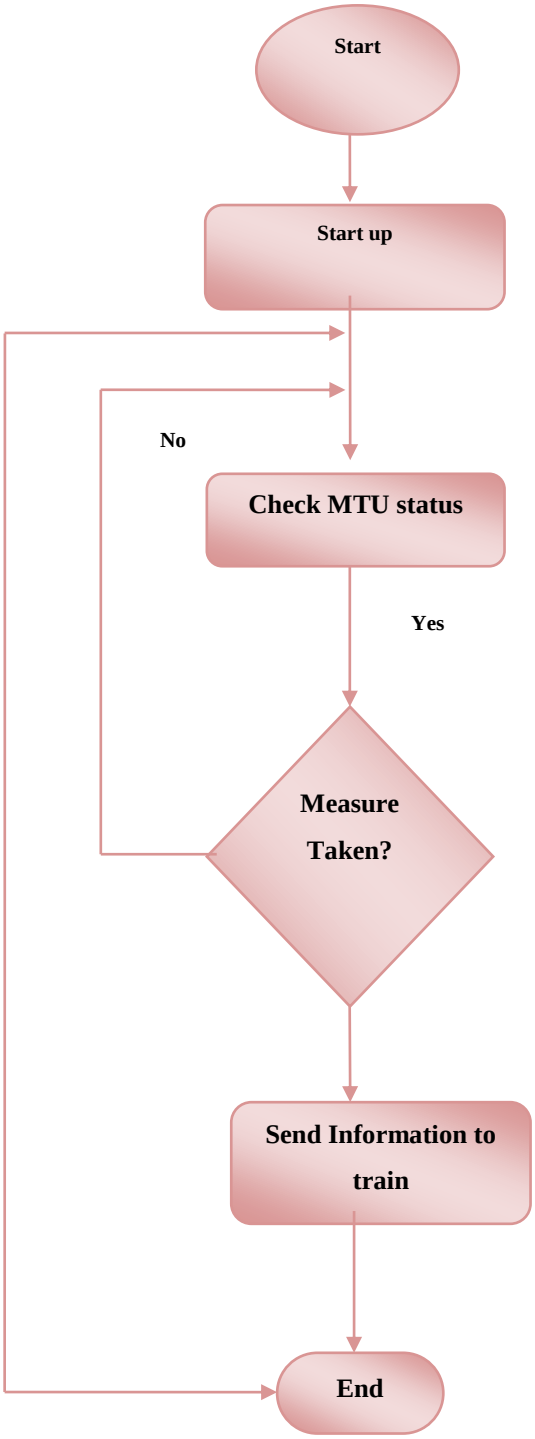


Figure 27: Flow chart for main control System

Chapter Four

4 .The Existing System versus SCADA System

Introduction

The existing system that the AALRT implement currently has been explained and discussed in chapter 2.It describes that the operation of Level crossing and interlocking system works interdependently. The overall system will not operate unless a train arrives at the switching point proximity to the level crossing. [1].In this mechanism, there lacks confidentiality to assure safety because it highly depends on speed and condition of obstacle at the level crossing.

Unlike the previous one, and as has been described earlier, the level crossing control system could be failsafe, Reliable, Maintainable and safest if SCADA system is integrated; besides to this, the remote controlling using wireless system provides more confidentiality and safest controlling output.

SCADA is a method of monitoring and controlling large processes, often scattered over along a rail way truck. It integrates data acquisition system with data transmission systems and the

Human Machine Interface (HMI) software to provide a centralized monitoring and control system. The SCADA System consists of the hardware and the software parts which are working in an integrate manner. It is used for the detection of the targets (the obstacle on the level crossing and the approaching train) so that the raw data found from it is going to be used by the Central control system.

4.1. SCADA Hardware Components

As shown in Fig.8, above. Typical hardware includes an Control part which is MTU (Master Terminal Unit) placed at a control center, communications equipment (e.g., radio, telephone line, cable, or satellite), and one or more geographically distributed field site devices consisting of RTU, which controls actuators and monitors sensors. The MTU stores and processes the information from RTU outputs, while controlling the local process at a particular site. The communication system allows the transfer of information and data back and forth between the MTU and the RTU's.

4.1.1. The Function of the SCADA Hardware components

Human Machine Interface (HMI)

1. Human Machine Interface (HMI)
   It is an interface which presents process data to a human operator, and through this, the human operator monitors and controls the process. Is a front end processor (FEP)
2. Supervisory (computer) System.
   It gathers data on the process and sending commands (or control) to the process.
3. Remote Terminal Units (RTUs).
   It connects to sensors in the process, converting sensors signal to digital data and sending digital data to the supervisory system.
4. Communication Infrastructure
   It provides connectivity to the supervisory system to the Remote Terminal Units.

The following are the components:

Each component has a well-defined function or purpose. Furthermore, each component has a specific relationship with the components that it communicates with. SCADA systems can be broken down into following major components, which form a chain. Each component communicates with the component before and after itself.

Data acquisition

The first component in the chain is data acquisition. It is not preceded by another component, but it connects to the data conversion component. Data acquisition consists of sensors, meters and field devices, such as photo sensors, pressure sensors, temperature sensors and flow sensors. Depending on the type of SCADA system these devices could be physically located hundreds of miles away from each other or could be inside the same plant. The primary function of these field devices is to sense physical parameters like light, temperature, pressure, etc., in the form of analog signals. In most cases the data which is acquired is analog. Data acquisition is also known as input output or I/O.[3]

Data conversion

Data conversion receives data generated by the acquisition component. Remote terminal unit (RTU), intelligent electronic devices (IEDs) and in some cases programmable logic controllers (PLC) are example devices that fall under this category. The functionality of

these components has evolved over the years to include analog to digital conversion, sequential relay control, process control and now even networking. An RTU monitors **the** field digital and/or analog parameters and transmits it to the central data control via the data communication component. Early PLCs were designed to replace relay logic systems and were programmed in ladder logic. Modern PLCs can even be compared to desktop PCs in regards to their power and functionality.[3,6].Data conversion has a two way communication with data presentation and control via the data communication component.

Data Communication

Data communication consists of some communication medium that transfers data back and forth between data conversion and data control. The communication medium could be wired, wireless, radio, satellite or others. The communication takes place using one of the many SCADA protocols. Some protocols are open standard while some are proprietary. Some example protocols are ModBus, DNP3, ControlNet, ProfiBus, DeviceNet, Tejas, UCA and others. [3,4].

Data presentation and control

The data presentation and control consists of devices used to monitor and control data received from various data communication channels. It may include Human Machine Interface/front end processor (HMI/FEP), which the operator uses to monitor and react to alerts and alarms. It may consist of historian databases and other support systems.[9].

4.2 SCADA Software

The Level crossing controlling system can be implemented using the SCADA software such as:IGSS families (IGSS 120,IGSS50,IGSS10) ,Winlong,profibus,etc....But all of them are not available openly. It requests the user to purchase the software online.

4.3. Equipments involved in the Level crossing System

The following are the equipments involved in the level crossing over all system that is being proposed. And the communication will be carried between HMI and these devices.

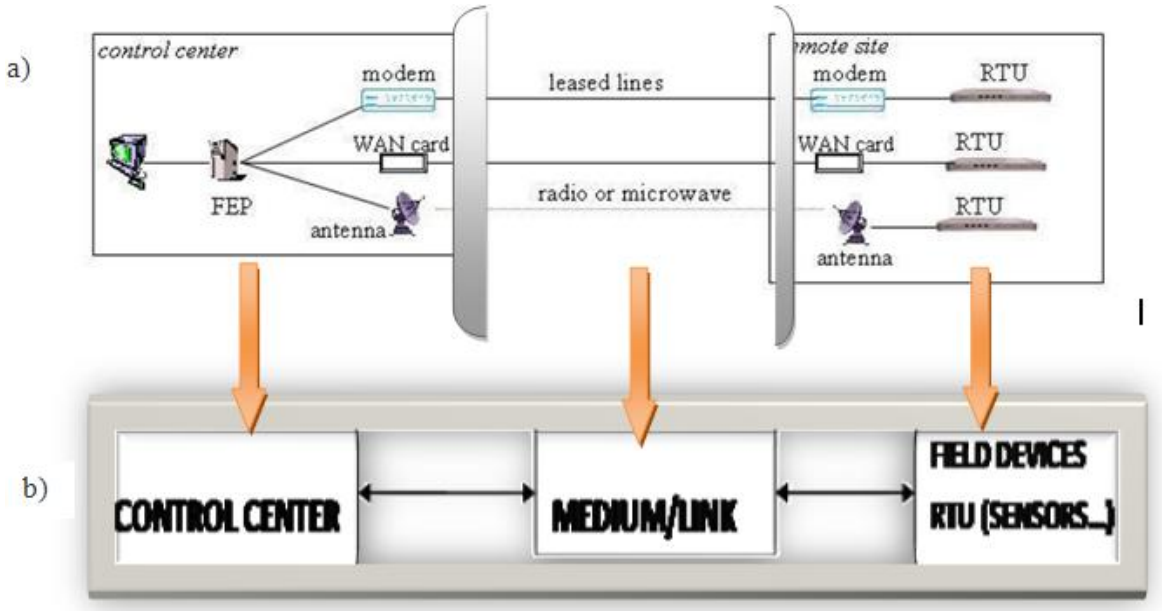


Fig 28.SCADA System a) Components and General Configuration b) Its Block diagram

The control center houses a SCADA Server (MTU) and the communications and routers. Other control center components include the HMI, engineering workstations, and the data Historian, which are all connected by a LAN. The control center collects and logs information gathered by the field sites, displays information to the HMI, and may generate actions based upon detected events. The control center is also responsible for centralized alarming, trend analyses, and reporting. The field site performs local control of actuators and monitors sensors.

Standard and proprietary communication protocols running over serial communications are used to transport information between the control center and field sites using telemetry techniques such as telephone line, cable, fiber, and radio frequency such as broadcast, microwave and satellite.

MTU-RTU communication architectures vary among implementations. The various architectures used, including point-to-point, series, series-star, and multi drop. Point-to-point is functionally the simplest type; however, it is expensive because of the individual channels needed for each connection.

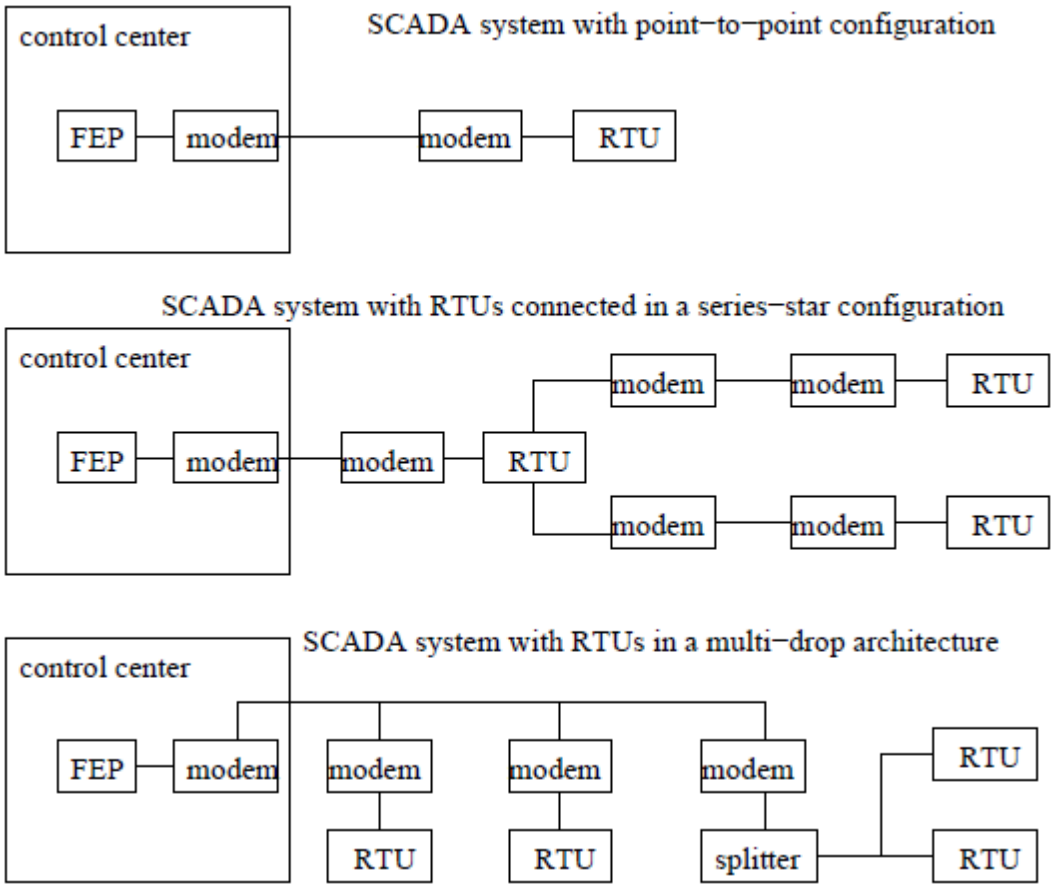


Fig 29. SCADA Communication Architecture

In a series configuration, the number of channels used is reduced; however, channel sharing has an impact on the efficiency and complexity of SCADA operations. Similarly, the series-star and multi-drop configurations ‘use of one channel per device results in decreased efficiency and increased system complexity.

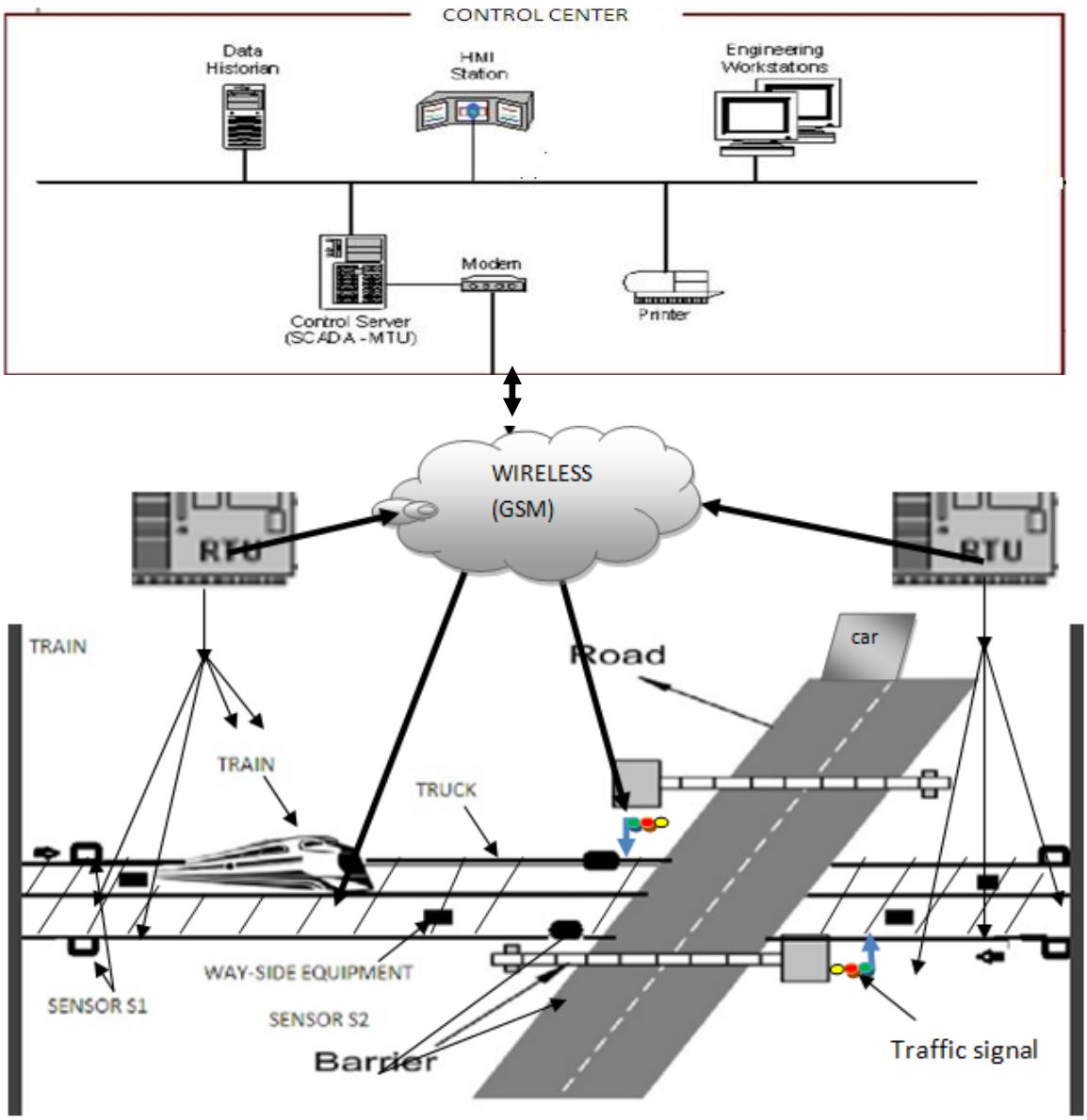


Fig 30.General frame work of SCADA, communication arena and controlled system

4.3.1. GSM modem

The Global System for Mobile Communication (GSM) is a short message service that can add values based on data packet switching provided by mobile communication using GSM Net work; besides, it has the tendency to be interconnected and roamed over a wide area due to its network ability.

The GSM Modem is selected for permanent data exchange between the approaching train and the level crossing RTU (wayside equipments). The GSM information transmitted first from the field devices (RTU) to MTU and then from MTU to level crossing controlling devices and the train which then receives the appropriate signal which is shown to the

driver so that he/she can take a measure to reduce the speed of the train or stop the train before approaching the level crossing to prevent accident.

4.3.2. Traffic Light

Is the hardware component which helps to show the Red, Yellow or Green signals for the vehicles and pedestrians interring or leaving the level crossing. This signals works according to the data sent by the MTU at the center.

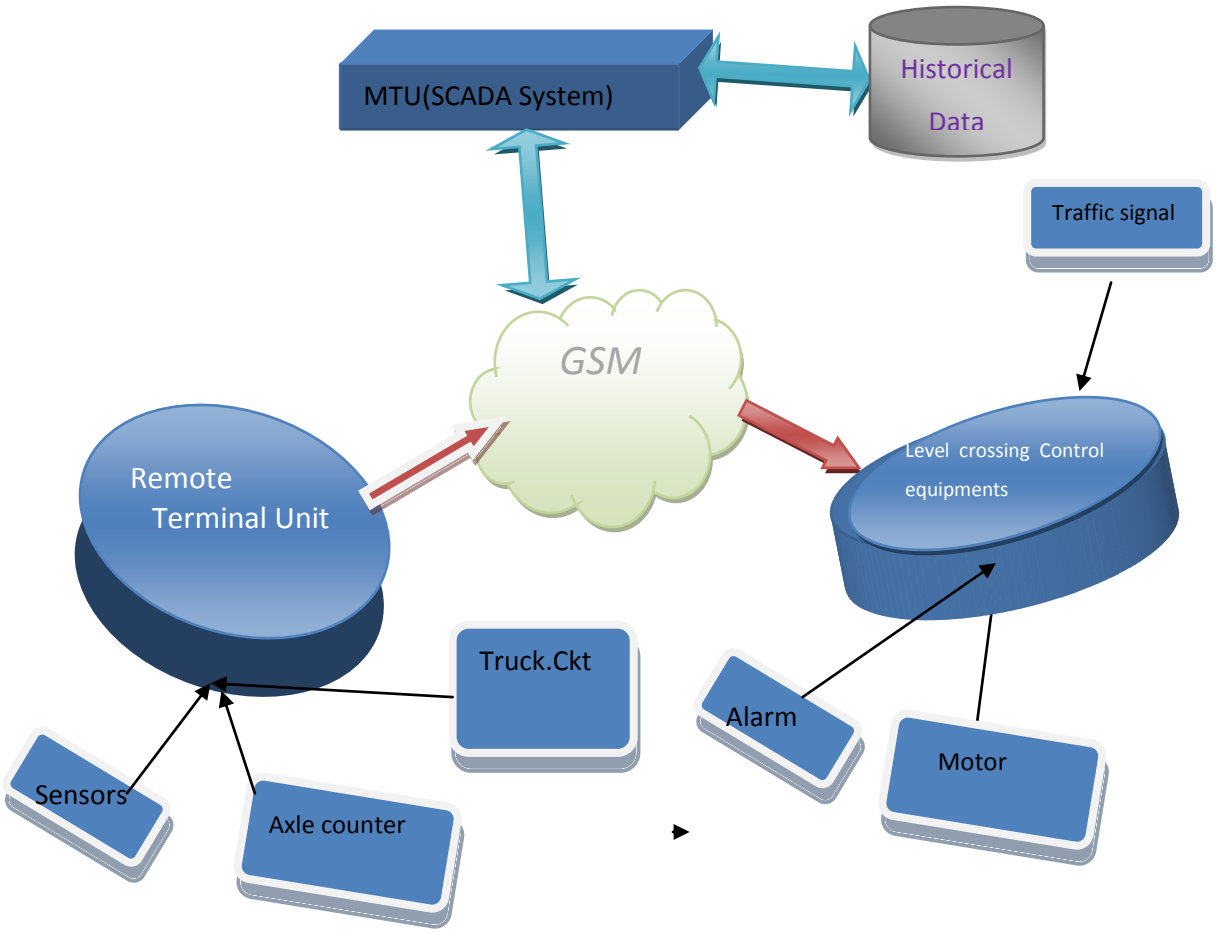


Fig 31.SCADA components, Communication (GSM) and controlled equipments

Railway level crossing system here in Ethiopia is generally a manually operated level crossing system. It is either manned or manned with unmanned [1]. The main aim is to protect pedestrians and vehicles from colliding with trains which passes at regular intervals, whereby accidents are occurred. Those accidents are happened due to human error and negligence [3].Live is lost, equipments are damaged [4, 6].

1. Level crossing Equipments

Table 3. Level crossing equipment

Relay (inductive loops)	Gate	Traffic Signal
Normally open/closed	Open/close	R/Y/G

Table 4. Field equipments/Devices (RTU)

Axle counter	Sensors	Truck Circuits
open/closed	senses	Open/short

Table 5. Train Driver front Devices

Speed Indictor(Normal)	Speed Indictor(Brake)	Speed Indictor(Emergency)
Normal	press	press

Table 6. MTU/HMI devices

Communication Link	HMI	Historic database
Wireless(GSM/wifi)	Co-ordination and Controlling	Storage previous data

4.4. The Overall Message (frame) conversation among the system component

The possible actors that participate in the proposed level crossing control system

a) RTU with Sensors
b) HMI
c) Gate

d) Driver

4.4.1. The way forward (how they interact?)

How the RTU, Obstacle detection mechanism and HMI communicate each other

The communication Event

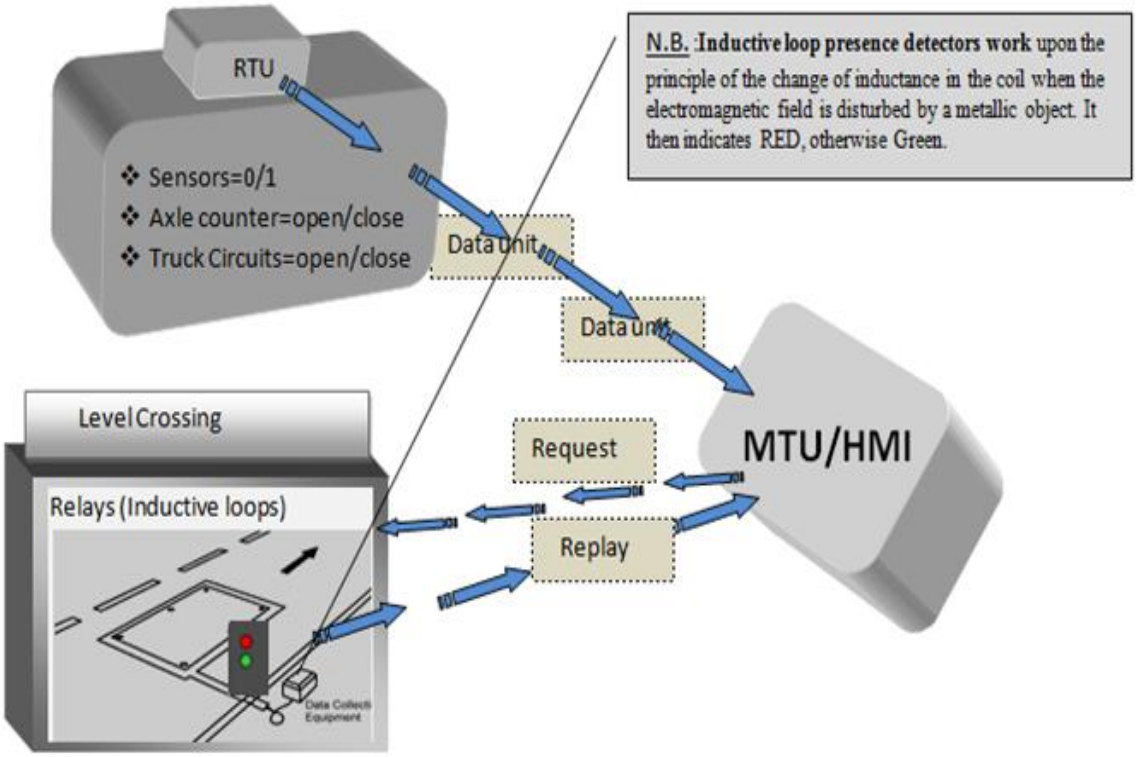


Fig 32.Communication establishment at RTU

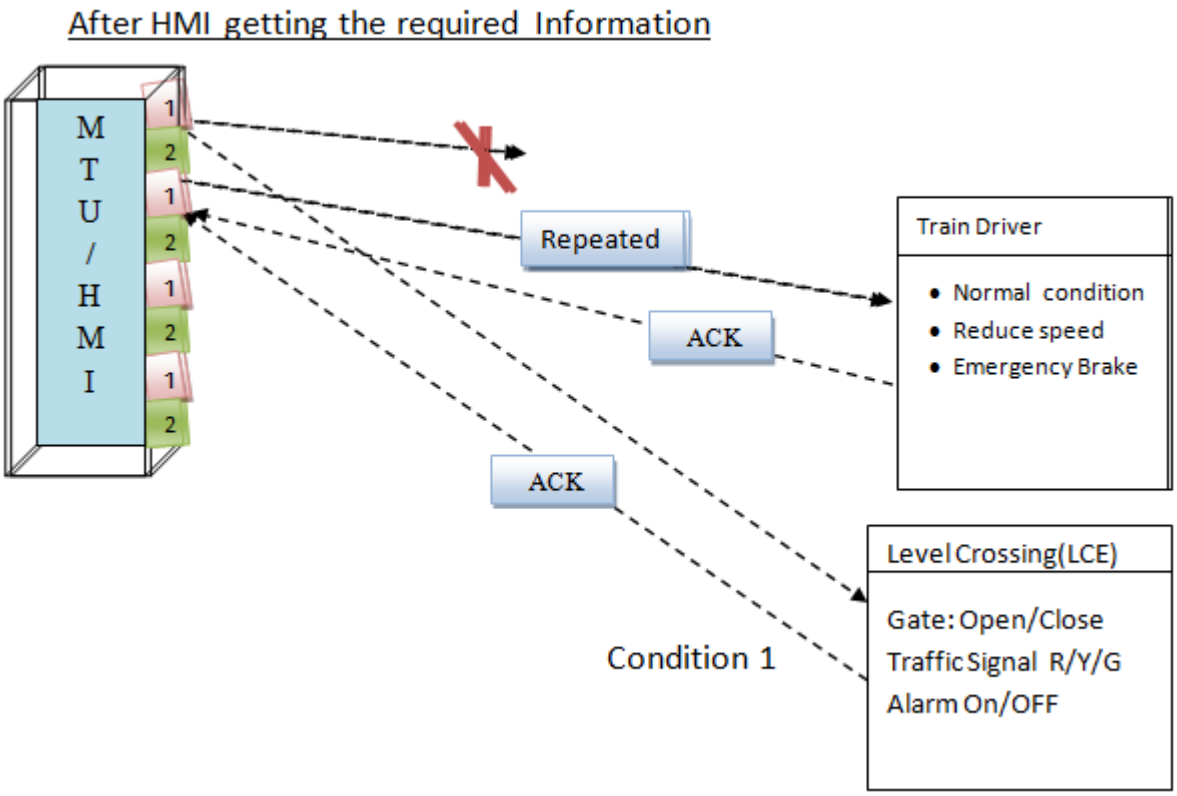


Fig 33 HMI sending control Message to Train driver(failed) and LC(successful)

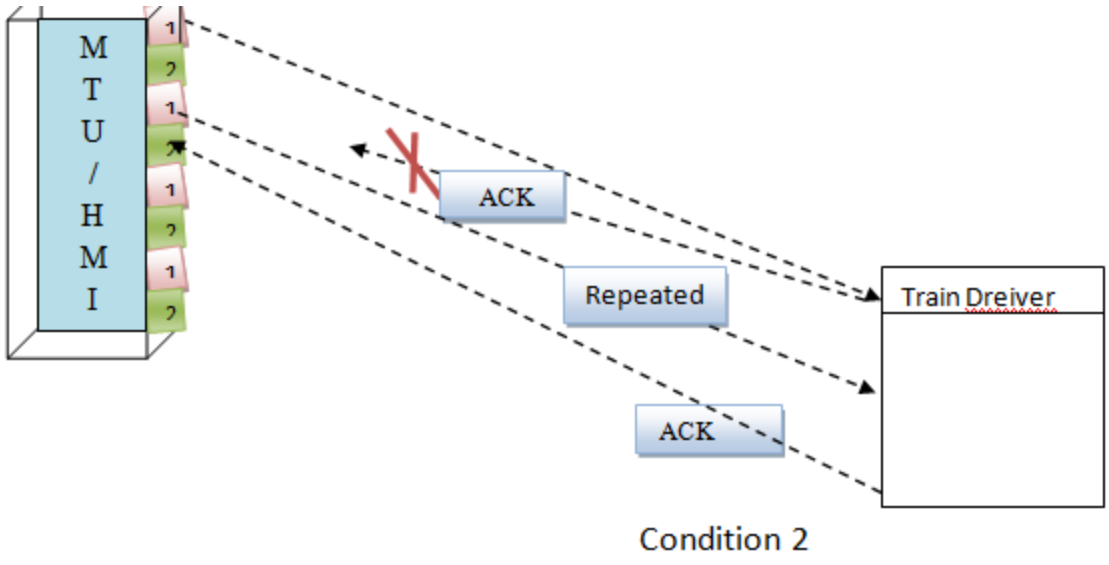


Fig 34 HMI sending control Message to Train driver(failed during Acknowledgment) and LC(successful)

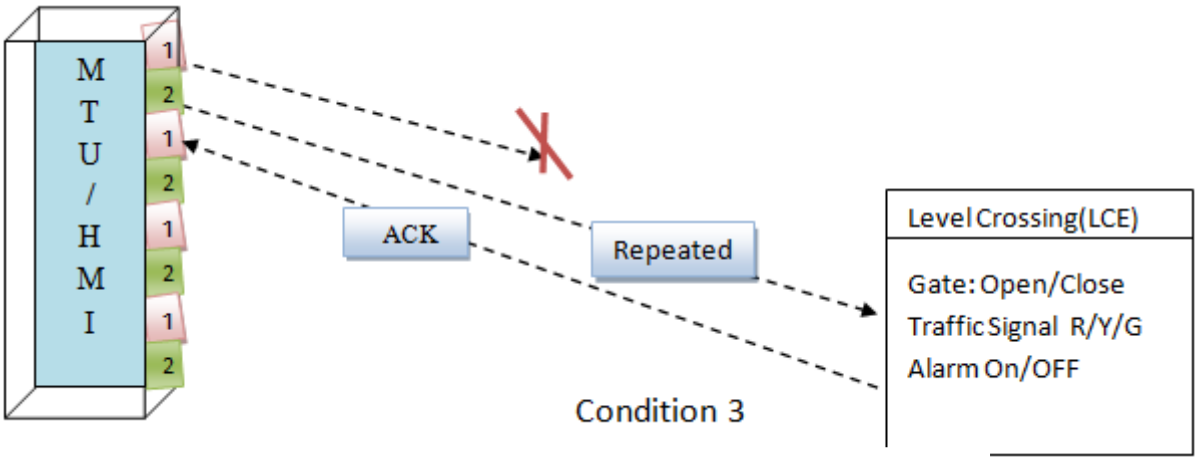


Fig 34. HMI sending control Message to Train driver(Repeated message) and Acknowledgment(successful)

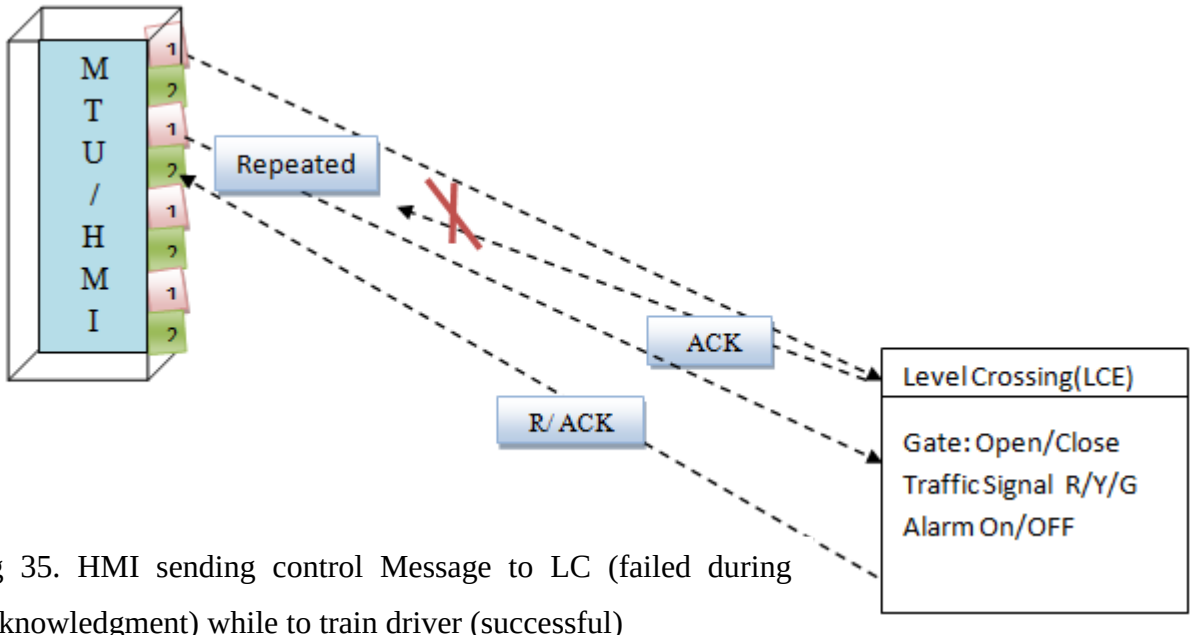


Fig 35. HMI sending control Message to LC (failed during Acknowledgment) while to train driver (successful)

After Being received a control information from the Master terminal unit, the equipments will be acted accordingly. Such as

Tasks carried out at LC EQUIPMENTS

- Gate closed
- Signal changed from Red to Green

Tasks carried out by train driver

- ❖ Making use of the speed devices at the front end
- ❖ Reduce speed accordingly

4.4.2. Condition versus Action

Table: 7. Conditions versus Action

Conditions	Failure happen at		Action taken by HMI/server
	Message	Acknowledgment	
1	Train driver		Repeat message then Acknowledged
2		Train Driver	Repeat message Then Repeat ACk'g
3	Level crossing		Repeat message then Acknowledged
4		Level crossing	Repeat message Then Repeat ACk'g

4.5. Comparison of SCADA system versus the Existing System based on Standardized Criteria

The table 3 below show, the compare and contrasting of the current system and the proposed system based on system-oriented and functionality based standard.[3,9,28 & 29].And the table 3.1 also notifying the definition and meanings of the keywords while making comparison.

Table 8. SCADA system and Lx System Comparison.

	Target	Criteria	LX-DIW	SCADA
1	Enhanced Safety	Improvident Observed/expected	Low	High
		Fail safe design	No	yes
		Provide warning	No	Yes
		Providing train information	Yes	yes
2	Cost	Installation Cost	Medium	High
		Power cost	Medium	Very high but low If solar energy
3	Instability	Un certainty presence	Medium	Used low
4	Reliability	Failsafe	Medium	High
5	Functionality	Ease of implement compatibility	need	Not needed

Key [3, 9, 11]

Table 3.1: Notifying the definition and meanings of the above keywords being used.

Performance ranges	Definition
low	Test results show compliance/no impact to motorists. Or ,the system has not tested for motorists. Reponses.
Medium	Test results show positive comment from the motorists /residents
high	Test result indicated the system is effective in warning the motorists /resident
No	The system does not detect failure. Or, no information available indicating it is fail safe.
yes	The system detect failure and activates warning
No	The system does not comply with "yes " as described below
Yes	The system activates warning device minimum of 20 s prior to arrival of train
No	The system only detects approaching train at certain distance without knowing its speed. Etc
Yes	The system detect the location, speed and direction of train ; thus possibly provide such information.
High	Installation cost.> $100,00
Medium	$50,000<installation cost<$100,000
low	Installation cost <$50,000
No	The system is not capable to operate with solar powered.
Yes	The system can be operated solely on solar powered
Development stage	The system is in development stag
System tested	The system or the prototype has been tested.
Product	The system is in revenue service or advertised as product
high	The tested system shown high failure rate. Or, no information available indicating it has no/low failure rate
Medium	The testing shown several failures.
Low	The system is in service. Or, system failure was controlled.
Hard	The implementation involves minor modification to the existing system/infrastructure.
Moderate	The implementation involves minor modification to the existing system/infrastructure.
Easy	No modification to the existing system/infrastructure is required.
Low	The system required installation of new control system/train detection system
Moderate	The system required installation of control system and warning device without hardware connection between them.
High	Existing control system /track circuit for train detection can be used and only single component (i.e ./warning devices) need to be installed.

Chapter Five

Conclusion and Recommendation

5.1 Conclusion

This paper work started with analyzing of the real problem that exists at the level crossing. And to deserve safety and smooth transportation free from any kind accidents, the SCADA System can be a currently available and resourceful solution. To manipulate, it needs to coordinate the field devices with the master terminal unit. The Architecture of SCADA, its hardware and software components has been discussed.

Next, the question of how the field devices and the Central units communicate is discussed. This was the theoretical aspects raised during the first three chapters. Hence, communication between the central unit, the level crossing devices and the field equipments is enhance using the SCADA protocol known as Distributed Network Protocol (DNP3).Which has an efficient role in SCADA communication thereby facilitate part of the transportation field with security problems are analyzed and explained.

In spite of the efforts made to have the thesis supported and explained through results and discussion, but it could not be possible and easier to get the software in an open source and it is too expensive to purchase and implement. Thus, it lacks the simulation part.

Finally, Using the SCADA with dedicated wireless link, the problem existed today can be solved; Moreover, the risk and danger, costing both Human life and property, associated with the current system would be solved and remained as history.

5.2 Recommendation

A lot can be done in this area using SCADA system. Mine is a drop. Especially considering the security system, Adapting our local language and many more.

Regarding the SCADA software and its protocol, the technology is getting advanced and changed dramatically.

On 7th February, 2012, the IEEE announced that work was proceeding to update IEEE 1815™, the standard defining the DNP3 Specification. The revisions include a significant update to the Secure Authentication section of the specification [35].

Three years later they also tried to discuses related issues, especially on the security matters [36, 39].

Thus the SCADA software getting attention by the IEEE for improving its scope of application by making more secure than ever. Therefore, it would be very useful and important to carryout research related to it, if anyone is interested to work with it.

7. Reference

1. Addis Ababa E-W & N-S (Phase I) Light Rail way Transit Project Signaling System
2. JabarAlizakeri"Safety Improvement Measures Based on Level crossing Inventories " 2004
3. By Cognitive Ergonomics Research Laboratory " A Human Factors Analysis Of Highway-Railway Grade Crossing Accidents In Canada "Prepared for Transportation Development Centre Transport Canada Department of Psychology, University of Calgary September 2002
4. http://addisababaonline.com/details-of-addis-ababa-light-rail-project/ Nov 30,2012 and Jan 22,2014
5. http://www.camerassavelives.vic.gov.au/home/cameras/camera+systems/ April 2015
6. J.Banuchandar,V.Kaliraj,P.Balasubramanian,S.Deepa,N.Thamilarasi"Automated Unmanned Railway Level Crossing System "International journey, Vol.2, Issue.1,Jan-Feb 2012.
7. Ananya Chandra, VikasBajpai, Sudhanshu Krishna Dubey " A Review on SCADA Systems in Indian Railways 2014
8. AhmerNizam Rail way road Liaison Washington State Department of Transportation Dan MacDonald, P.E. Manager Public Projects BNSF Rail way Company.
9. Highway-Rail way Level Crossing Safety & Enforcement Manual 2003
10. Dr.Aditya Goel and Ravi Shankar Mishra "Remote Data Acquisition using Wireless SCADA "International journey of Engineering(IJE),issue(1)
11. Tu-Huan Lin,Jyh-Cherng Jong,Chian Shan Suen "Evaluating the effectiveness of Traffic Signs to the drivers approaching level crossings"(2013)
12. Transactions on the Built Environment vol 16, © 1995 WIT Press, www.witpress.com, ISSN 1743-3509
13. IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 6, November 2010 ISSN (Online): 1694-0814 www.IJCSI.org
14. International Journal of Modern Engineering Research (IJMER) www.ijmer.com Vol.2, Issue.1, Jan-Feb 2012 pp-458-463.
15. IJR International Journal of Railway Vol. 3, No. 3 / September 2010, pp. 106-112
16. International Journal of Innovative Research in Science, Engineering and Technology An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014.
17. http://www.eforu.page.tl/ May 2016

18. International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 5, Special Issue 4, March 2015).
19. sSCADA: Securing SCADA Infrastructure Communications Yongge Wang and Bei-Tseng ChuDept. of SIS, UNC Charlotte,9201 University City Blvd, Charlotte, NC 28223,August 5, 2004.
20. Security considerations for SCADA protocol by James Graham [Online] Available: http://www.cs.louisville.edu/facilities/ISLab/tech%20papers/ISRL-04-01.pdf
21. Ion Boldea and Syed A. Nasser," Rhe Induction Machine Handbook", United States 0f America, CRC Pess, 2002.
22. Erwin Krayszing, "Advanced Engineering Mathematical", 10th Edition, United States Of America, Laurie Rose Tone.2011.
23. L.F Shampin, R.C Allen, Jr and S. Pruess,"Fundamental Of Numerical Computing", John Wiley & Sons, Inc., Canada, 1987.
24. Allen Jeffrey, "Advanced Engineering Mathematics" , United State Of America, HARCOURT/ Academic Press,2002
25. David A. Coley,"An Introduction To Genetic Algorithm", Singapore, World Scientific Publishing Co. Pte. Ltd, 1999.
26. Colien R. Reeves And Jonathan E. Row," GA Algorithm Principle And Perspective, A Guide To GA Theory ", United State Of America, Kluwer Academic Publishers ,2003
27. Randy L. houpt and sue Ellen houpt, "practical generic algorithm", 2nd edition, united state of America, john Wiley & sons, inc, 2004.
28. International Journal of Advanced Research in Computer and Communication Engineering. Vol. 4, Issue 3, March 2015
29. The Instrumentation, Systems and Automation Society. Presented at the ISA 2004, 5-7 October 2004, Reliant Center Houston, Texas, www.isa.org
30. http://www.automation.siemens.com/partner), March 2016
31. http://www.ni.com/white-paper/11863/en/#toc61, January 2016
32. http://www.racom.eu/eng/support/prot/dnp3/index.html, April 2016
33. IEEE journal on release of DNP3 secure authentication Version 5 by Lorene Cunningham [Online]
34. https://play.google.com/store/apps/details?id=com.YOZHStudio.RailRoad, May 2016
35. https://scadahacker.com/library/Documents/ICS_Protocols/Triangle%20Microworks May 2016

36. IEEE standard for Electric Power Communications – Distributed Networking Protocol (DNP3) June 2016

37. DNP users group online library [Online] June 2016

38. IEEE standard for Electric Power Systems Communications 1815 -DNP3 [Online] May 2016.

39. OS. A. Boyer. Supervisory Control and Data Acquisition. ISA– The Instrumentation, Systems and Automation, 1999.

8. ABBREVIATION

1. AALRT Addis Ababa Light Rail Transit
2. LRT Light Rail Transit
3. LC Level crossing
4. MTU Master Terminal Unit
5. HMI Human Machine Interface
6. LCE Level Crossing Equipments
7. SCADA Supervisory Control And Data Acquisition
8. PSTN Public Switched Transmission Network
9. DNP3 Distributed Networking Protocol
10. RTU Remote Terminal Unit
11. IED Intelligent Electronic Devices
12. TCP /IP Transmission Control Protocol /Internet Protocol
13. TLS Transaction Layer Security
14. CCTV Closed Circuit Television
15. ERA European Road Authority
16. MTBF Mean Time Between Failure
17. CSI Communication Safety Indication
18. WAN Wide Area Network
19. WLAN Wide Local Area Network
20. LOD Level Crossing Obstacle Detection
21. SELCAT: Safer European Level Crossing Appraisal and Technology:
22. FT3 Frame Format type 3
23. ICT Information Communication Technology
24. SSL Secured Socket Layer
25. IEEE Institute of Electrical and Electronics Engineers
26. IEC International Electro technical Commission
27. ASDU Application Service Data Units
28. APCI Application Protocol Control Information
29. TPDU Transport Protocol Data Units
30. LPDU Link Protocol Data Units
31. CRC Cyclic Redundancy Check
32. TSDU Transport Service Data Units
33. μ Coefficient of Friction
34. g Acceleration due to Gravity