Implementation of SCADA Communications in Long Rang Wireless using Land Mobile Radio Technology.

[1]Akshatha Kanthraj, [2]Dr.Jamuna S

[1]Student, [2]Professor
[1]Electronics and Communication Engineering ,
[1]Dayananda Sagar College of Engineering, Bangalore, India

Abstract : Radio signals are electromagnetic in nature. The process of transmission and detection occurs in straight line path as it acts like a medium. The Radio Technology plays a vital role in mission critical systems which provide benefits to the utility organizations optimizing the incident response time and reducing system downtime which gradually reduces the trunk deployment. This paper discusses various ways in which SCADA(Supervisory Control and Data Acquisition Systems) Communication can be established by using SCADA Protocols between different end points in a SCADA network spanning across wide coverage area, thereby improving the efficiency, optimizing the incident response time and reducing the system downtime. Land Mobile Radio Technology finds applicable in case of land based push-to-talk wireless communications system for critical purposes like firefighters, police, mining, utilities and other emergency response organizations.

This paper illustrates how a secure communication can be established between the SCADA Master and RTU.

Yocto Project has been used as the open embedded build system for which Bitbake is a build tool. Build tools are programs that automate the creation of executable application from source code.

***IndexTerms* - Distribution Automation, SCADA Protocols, Yocto Project, RTU, Bitbake.**

I. Introduction

Beside all the benefits for organizations using distribution automation, usage of it in the rural and suburban region becomes difficult due to expenses found in rolling out hard wired solutions, example fibre optics. Cellular coverage remains spotty in less populated areas because of no success in case of emergency or weather events. To deploy distribution automation over a wider area, electric utilities require a bearer which will always cover very long distances economically and at the same time provide mission-critical reliability. The 2-slot TDMA protocol used by SCADA systems solves this problem by creating solution which uses the mission critical trunked voice and data DMR network. This means it offers mainly excellent and extensive coverage at a low cost and also built with resiliency at its core. This being one of the most intelligent solution that some of the world’s finest networks are affording. The business benefits which can be obtained are one network for both voice and SCADA data [1], improved grid reliability and resilience, optimized network coverage and energy efficiency. It is seen that critical network managers have accepted the duplication of voice and data over the separate networks and associated costs are necessary because of the lack of alternatives. Hence the effects that can be found from any distribution automation depends on the reliability of the communication link between the devices and the SCADA system. The capacity doubling effect of 2-slot TDMA combined together with trunking resource management gives network operators new opportunities to prioritize network resources for voice or SCADA traffic, there are reserve channel resources for both voice or SCADA data so dynamic network loading does not impact the quality of essential services, interrupt the call queues which is based on priority of the call and also the network loading. Land Mobile Radio (LMR) Technology is required for utilities during time of disaster to face some constant challenges like mix of aging infrastructure, severe weather conditions like heat waves or ice storms delivering power reliably and safely for all electric distribution.

Therefore the network managers around the globe have managed various types of communications to join distribution line infrastructure and substations to their Supervisory Control and Data Acquisition systems (SCADA).

Section II discusses the Hardware and the Software Requirements.Section III discusses working of SCADA systems and Business benefits.

Section IV gives the experimental setup and results for the SCADA Communications between the SCADA Master and the RTU.

Section V summarizes the paper

II. Hardware and Software Requirements

The hardware used is the BeagleBone Black with ARM Processor AM335x 1GHz board. It is found to be less expensive, group-supported enhancement platform for builders and for also enthusiasts across the globe. It is found that the booting time for Linux is within 10 seconds and it gets rebooted within 5 minutes with a USB cable.

It is found that the memory usage is 512MB RAM 4GB 8-bit EMMC on-board flash storage along with 3D graphics accelerator and NEON floating point accelerator with 2*PRU 32-bit micro controllers. The Connectivity that can be established for this device can be through USB host along with Ethernet and HDMI and also 2*46 pin headers with USB client for power and communications. It is seen that software [2] which remains compatible for this device is the Debian, Android and Ubuntu.

The Power Supply and the USB Cable drive is also been used for booting up the hardware device and also to interface the hardware device and the Personal Computer.

Fig.1 Diagram of the Beaglebone Black as in [2]

The Beaglebone capes are the daughter-board add-on products for BeagleBone Black family and pocket Beagle family products wherein each will extend the functionality of the Beaglebone by the new exciting capabilities. The capes that are existing for the BeagleBone Black are Relay Cape, Power Cape, Proto cape and Can capes can also be used. Radio Transceivers have been used to transmit and receive data in the bi-directional form using Phoenix contact RTU which is been manufactured by the standard Phoenix Company. LTE Infra has been used in order to provide communication for long distances covering ~90 Kms.

The Software tools used mainly are the C++ Programming Language which is an object oriented type of programming language and also a general purpose programming language. It is found that it is generic in nature. The other Programming Language which can be used is Python, Shell Scripting which is open source operating system, typical operations which can be performed are file manipulation, program execution and printing text.

The code has to be encrypted properly so that transmission and reception of data occurs properly without any sort of confiscation of the data over the radio channel. There should not be any sort of noise in the carrier message.

III. WORKING OF SCADA COMMUNICATION AND ITS BUSINESS BENEFITS

SCADA Communications [4] are sent from the control application to the router, located beside the Digital Mobile Radio (DMR) Node, and then transmitted through the Basestations to Control Application Basestations which then forwards the communication to the RTU/IED located outside and wait for acknowledgement. In this process whenever the RF interference or data corruption occurs, the standard system will automatically retransmit messages to deliver highly reliable SCADA Communications, More than 60,000 basestations may be setup on the single network. The number of outstation RTUs and associated systems where outstation integrity checks are executed for every 10 minutes, operator commands are exported, executed and accompanied within less than a fraction of 1.5 seconds under both storm and also during normal operating conditions.

The Fig.2 shows the current profile for combined voice and SCADA Network. Some of the SCADA protocols used for communication are DNP3(Distributed Network Protocol), IEC 61850, Modbus RTU, Profibus, IEC 60850-5-101,IEC 60850-5-104.

IEC 60850-5 is basically collection of standards produced by the IEC. It was created as an open standard mainly for the transmission of the SCADA telemetry, control and information. The DNP3 protocol is a set of communication protocols used between components in any of the process automation systems which is mainly made up of 3 main layers such as link layer, transport layer, application layer that can sit on top of serial bus connection or TCP/IP network.

IEC 61850 is one of the standard communication protocol for intelligent electronic devices.

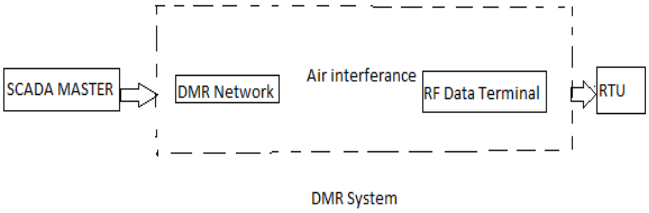


Fig.2 Combined voice and data

The DMR offers several benefits to managers, users, technicians, firstly it is an open standard which means that competition is possible between manufactures, secondly Digital Audio Quality is good over analog. Thirdly it's the data applications wherein DMR is not only capable of transmitting voice but also end-to-end applications such as text messaging, GPS, SCADA, telemetry. Fourthly, DMR is a TDMA technology which mainly offers benefits of two simultaneous and independent single talk in one single 12.5khz channel. Fifthly, DMR has been designed for easy migration from analog to digital.Sixthly, DMR has got better battery life than regular analog portables reason being greater power efficiency.

The operating systems on which the SCADA Gateway works is on the Linux[6] operating systems. The SCADA Gateway application can run on the same server as the DMR Node. Depending on the network size and redundancy requirements it may be advantageous to run the SCADA gateway on its own server hardware, separate from the DMR node. The Data Terminal in Fig.3 has been integrated with IP 40/51 enclosure which can be mounted vertically on the rails. The type of communication that occurs between the SCADA Master and the data Terminal unit is network mechanism type which consist of solicited and also the unsolicited messages. There are two different mechanism for sending messages mainly in case of solicited Messages are those messages sent by an out-station devices in response to the gateway request ,typically a poll. In this case the gateway allocates the channel resource for the outgoing message and keeps it open for the response. These types of messages are common in SCADA systems as polling stations is the usual mechanism for determining their status. Voice calls may occur on the system at the same time data calls. The control channel is shared between the voice and data which is mainly for the call setup. Hence the traffic channel can be dedicated to voice, data and also it may be even shared. Security of the system plays a major role wherein the secure system need to identify the mitigations for all significant human and system level vulnerabilities and it is also a must to consider the risk management in case of both software and hardware coverage.

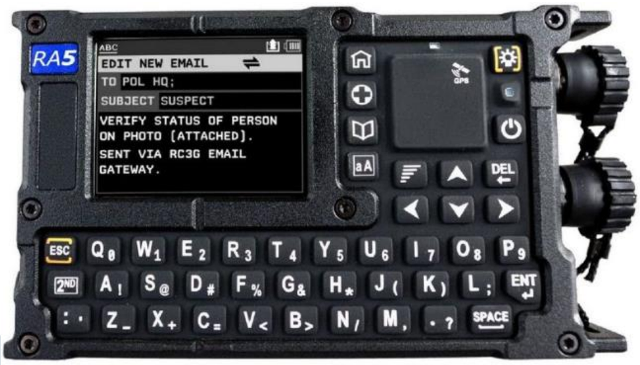


Fig 3. Data Terminal

It is seen that in the past SCADA system had a shutdown operating environment hence the system was been designed without any security functionality but in the recent years the demand for joining the SCADA System to the open network has been increased the role of key-management scheme which is necesssary for secure SCADA communications. Henceforth the study of SCADA system security plays a major role.

The SCADA network has got data acquisition systems, data transmission systems and Human Machine Interface Software which are integrated for providing the centralized monitoring and control systems for processing of data both at the outputs and inputs. SCADA networks are designed for mainly collecting the field information and then transferring it to the Central Computer facility and then displaying the information for the users either graphically or textually.

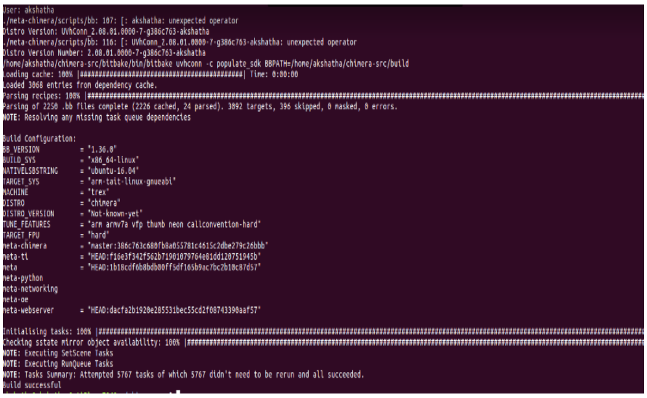
SCADA Networks typically consist of the software and hardware parts. The hardware mainly includes the Master Terminal Unit, the Sub-Master Terminal Unit, Communication Links and Equipments and also the geographically distributed field sites consisting of Remote Terminal units. But in some cases the Sub –Master Slave Unit may not be used in such cases the Master Station Unit may be directly connected to the slave station unit and RTU using the communication links.

In some situations the slave station unit provides a direct interface to control and monitor equipment and sensors. It can be seen that the Slave Station Unit may be directly polled or controlled by the Master Station Unit.

The Master Station Unit [8] mainly stores and processes the outputs and inputs information of slave station units, RTUs, while the slave station units will monitor the local process. The communication Links will always transfer the communication. Additionally software will be programmed into the SCADA network as to what and when should be monitored, what response should be initiated when parameters go outside certain acceptable values.

IV. RESULT ANALYSIS

The application has been built on the software later on ported on to the board. The simulation results for that has been analyzed and shown below in Fig.4



```
User: akshatha
./meta-chimera/scripts/bb: 107: [: akshatha: unexpected operator
Distro Version: UVhConn_2.08.01.0000-7-g386c763-akshatha
./meta-chimera/scripts/bb: 116: [: UVhConn_2.08.01.0000-7-g386c763-akshatha: unexpected operator
Distro Version Number: 2.08.01.0000-7-g386c763-akshatha
/home/akshatha/chimera-src/bitbake/bin/bitbake uvhconn -c populate_sdk BBPATH=/home/akshatha/chimera-src/build
Loading cache: 100% |############################################| Time: 0:00:00
Loaded 3068 entries from dependency cache.
Parsing recipes: 100% |##########################################################################################################
Parsing of 2250 .bb files complete (2226 cached, 24 parsed). 3092 targets, 396 skipped, 0 masked, 0 errors.
NOTE: Resolving any missing task queue dependencies

Build Configuration:
BB_VERSION           = "1.36.0"
BUILD_SYS            = "x86_64-linux"
NATIVELSBSTRING      = "ubuntu-16.04"
TARGET_SYS           = "arm-tait-linux-gnueabi"
MACHINE              = "trex"
DISTRO               = "chimera"
DISTRO_VERSION       = "Not-known-yet"
TUNE_FEATURES        = "arm armv7a vfp thumb neon callconvention-hard"
TARGET_FPU           = "hard"
meta-chimera         = "master:386c763c680fb8a055781c4615c2dbe279c26bbb"
meta-ti              = "HEAD:f16e3f342f562b71901079764e81dd120751945b"
meta                 = "HEAD:1b18cdf6b8bdb00ff5df165b9ac7bc2b10c87d57"
meta-python
meta-networking
meta-oe
meta-webserver       = "HEAD:dacfa2b1920e285531bec55cd2f08743390aaf57"

Initialising tasks: 100% |#######################################################################################################
Checking sstate mirror object availability: 100% |###############################################################################
NOTE: Executing SetScene Tasks
NOTE: Executing RunQueue Tasks
NOTE: Tasks Summary: Attempted 5767 tasks of which 5767 didn't need to be rerun and all succeeded.
Build successful
```

Fig 4. Software Application built.

Fig.4 shows the software application built on the Linux platform which is then ported on to the Hardware board confirmed. Henceforth we are creating a board support package layers by building the application source using various commands and syntaxes as shown in Fig.4

The Beaglebone Black is been booted up which has then been ported on the Hardware Board namely the Beagle Bone Black which then gets booted up when the Data Terminal application has been built. Using this has the main device for communication that has to be established between the SCADA Master and the RTU [7] further implementation is been done.

V. CONCLUSION

This paper has discussed the Communication that is been established between the SCADA Master and the RTU over the air interface using standard SCADA Protocols. It further discusses how both voice and data can be supported over the same channel .When Communication occurs , both voice and data has to be transmitted and received simultaneously along with other supporting features like the cellular Modem, WIFI, Ethernet etc. Furthermore, this paper discusses how such applications are found useful in case of utilities such as the Mining Oil, Gas, Fire Fighters, Disaster, Emergency cases by using the technique of Land Mobile Radio Technology having the features of push-to-talk ability.

Hence by using a reference source called the Yocto Project which is an Open Source Embedded Project out of which any of the application sources such as Software Development Kit can be derived.

REFERENCES

[1] Rajepova Ejesh,Zhang Zhonglin,"*Safety of the SCADA Systems by using Industry Protocols Data Communication*",4th International Conference on Information Science and Control Engineering,2017.

[2]Nannan He,Ying Qian,Han-way Huang,"*Experience of teaching embedded systems design with BeagleBone Black board*",IEEE Conference on Electro Information Technology(EIT),2016.

[3]Lehab Abduljabbar,Kamil Hemant Mahajan,"*Increasing SCADA System availability by Fault Tolerance Techniques*",International Conference on Computing,Communication,Control and Automation,2017.

[4]Filippo Battaaglia,Giancarlo Iannizzotto,"*An open and portable Software Development Kit for Handheld devices with Proprietary Operating Systems*",IEEE Transactions on Consumer Electronics,Vol 55,No.4,November 2009.

[5]Anass Lekbich,Abdelaziz belfqih,"*A secure wireless control of Remote Terminal Unit using the Internet of Things in smart grids*",6th International Conference on Wireless Networks and Mobile Communications,Nov.2018.

[6]Ahmad Safwan Haron,Mohamad Sofian Abu Talip,"*Internet of Things Platform on ARM FPGA Using Embedded Linux*".International Conference on Advanced Computing and Application,2017.

[7]B.Madonsela,I.E.Davidson,"*Advances on Telecontrol and Remote Terminal Unit(RTU)for Power Substations*",IEEE PES/IAS PowerAfrica,2018.

[8]https://www.sciencedirect.com/science/article/pii/S2215098616303482.

[9]Ashwin Holkar,Legineni Mahendra,"*Secure Interoperable Gateway for Wireless Scada System*",International Conference on Computational Systems and Information Systems for Sustainable Solutions,March 2016.

[10]Harita khandewal,Parthesh Mankodi,Ritheshprajapati,"*Enhancement of Automation Testing System using Yocto Project",*International Conference on Electronics,Communication,andAerospace Technology,2017.