November-December 2019
ISSN: 0193-4120 Page No. 1784 – 1798

Next Generation Power Plant Control through IoT, using encryption in layer 2 of Communication protocol

Iqra Hussain[1], Dr. Nitin Pandey[2] Dr. Mukesh Chandra Negi[3]
[1]Amity Institute of Information Technology,
Amity University Uttar Pradesh, Noida
iqrahussain4@gmail.com

[2]Assistant Professor
Amity Institute of Information Technology,
Amity University Uttar Pradesh, Noida
npandey@amity.edu

[3]Delivery Manager,
TechMahindra Ltd
A7, Sector 64, Noida
MN00330419@techmahindra.com

Article Info
Volume 81
Page Number: 1784 - 1798
Publication Issue:
November-December 2019

Article History
Article Received: *5 March 2019*
Revised: *18 May 2019*
Accepted: *24 September 2019*
Publication: *09 December 2019*

Abstract
In current epoch every field is shifting to the internet control and making its way in the field where everything is connected to Internet. Hence a need arises in the field of Industries as well. This paper aims to take the Power Station control operation to a next generation and making it shift to the IoT. Through this technological intervention this sector is going to witness a step ahead in remote control operation and monitoring of Power Stations. And to achieve confidentiality, integrity, availability, privacy, authenticity and trustworthiness, the data security or communication security becomes a big concern here. Our proposition will be to address the above concerns regarding security and confidentiality of the data. This shall be achieved by introducing encryption techniques at the layer 2 of communication protocols, which will enable secure data communication between remote operation stations of the Power Plant through the internet. The encryption scheme employed to cover the security parameter will be AES which will get implemented at the sub loop level or sub control system of the power plant. The statistics utilized were made available by NTPC, India and the simulations were executed via MATLAB.

Keywords: DDCMIS, PLC, DCS, SCADA, AES, Control logic, Field, Remote station, I/O, ATR, FSSS, TSI, BMS, PPCS, CPU, Controller, RTU, MMIPS, Local Host Station, Remote Station, NTPC.

November-December 2019
ISSN: 0193-4120 Page No. 1784 – 1798

1. INTRODUCTION

A Power Plant control system (PPCS) is the name that covers different classes of systems as well as the related instrumentationused in power plantsfor productionpurposes, including the subsequent sub systems; the programmable logic controller (PLC), the Distributed Control System (DCS), the Distributed Digital Control Monitoring and Information System (DDCMIS), and other control system configurations like the Supervisory Control and Data Acquisition Systems (SCADA).

Power Plant Control systems, that are planted on information obtained from remote systems that can be automatic or operative, the decision-making instructions are driven to control devices that are located remotely, and these are usually called as field devices. The operations that are indigenous like when a valve is opened and closed or information collection against systematic sensors or supervising local environments in case of any alarmed situations are handled by these field devices. [5]

1.1. Programmable Logic Controllers

The PLCs can either be tiny building blocks or tools with many I/O devices housed with processors, to large framemounted automatic tools to a number of tens of I/O devices that are generally connected to further PLCs. The main components included in the basic architectural definition of a PLC are -the processor modules, the power supplies, and the I/O module. The central processing unit (CPU) and the memory are included in the processing modules and along a microprocessor; CPU even constitutes an interface connected to a programmed device and interfaces to additional remote I/O devices or extra communication networks. [1]

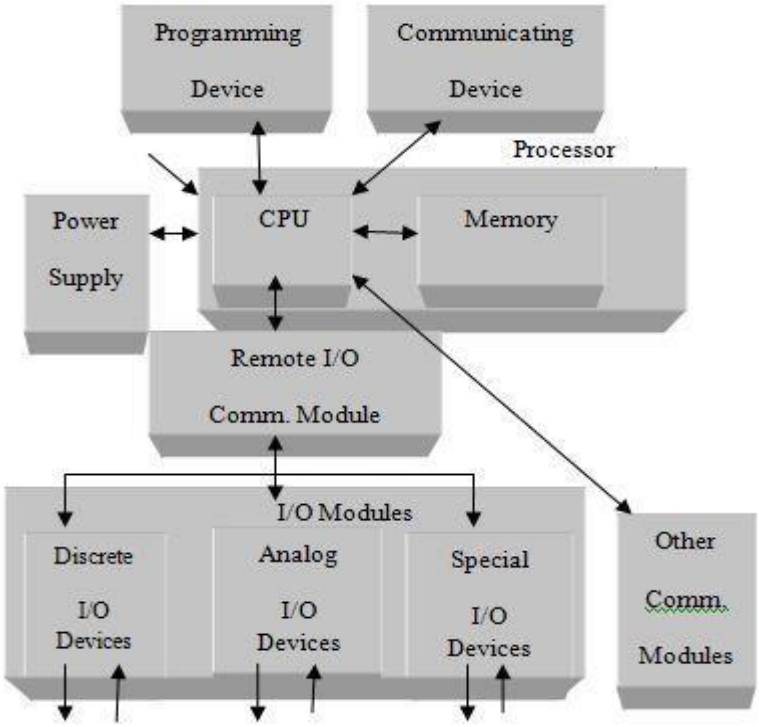


Fig. 1: PLC architecture

November-December 2019
ISSN: 0193-4120 Page No. 1784 – 1798

1.2. Distributed Control Systems

Distributed Control Systems (DCSs) are automatedcontrol systems for processes, in which a controller is distributed all through the system. It stands against to a non-distributed system that makes use of a discrete controller. In a DCS, controllers in a hierarchy are linked by the communication network that allows centralized control rooms and local on-plant monitoring as well. A DCS generally makes use of a self-engineered processor as a controller, and makes use of either a proprietary interconnection or a standard protocol for communication. The input modules forward data to the processors and data is accordingly processed and the desired control actions are performed by the output modules. Then these output modules transfer commands to the last control devices, like a control valve. [2]

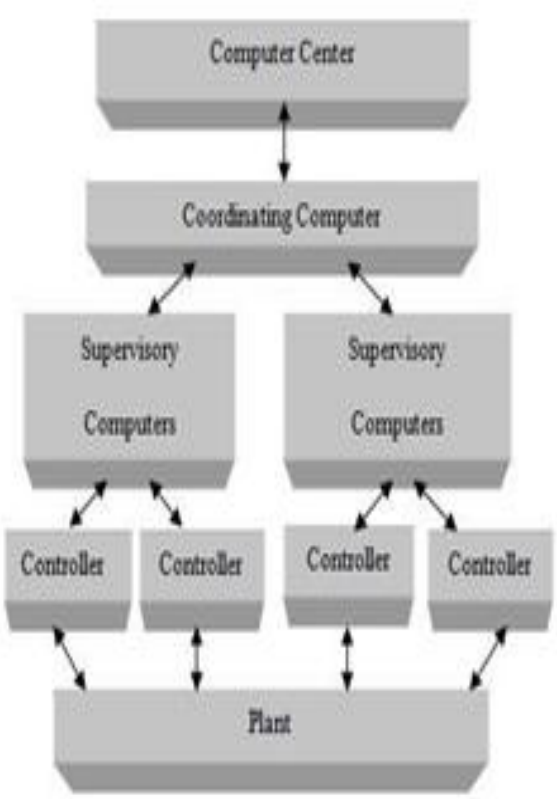


Fig. 2: DCS architecture

1.3. Distributed Digital Control Monitoring and Information System

In DDCMIS control systems, Distributed stands for no central control plus this control is extended to several divisions, digital means the data is processed in digital form making using microprocessors sourced category of hardware's and Monitoring and information system interface humans with processes using computer systems. In DDCMIS control systems the technology that is used in controllers constitutes Local Pneumatic Controller, the Miniaturized and Centralized Pneumatic Controller, the Solid State Controller, the Computerized Controls, and the Distributed Microprocessor based Controls. DDCMIS control systems have these components, the Man Machine Interface and Process Information System (MMIPS), the Data Communication System and the Control System.

A DDCMIS control system is highly flexible for modification in control strategy, self diagnostic, highly reliable. The main objectives that are incorporated in a DDCMIS control system include higher reliabilities, better response time, extended lifetime of plant equipments, improved operator interfaces to plant, improved accessibility of retrieval systems and plant data.

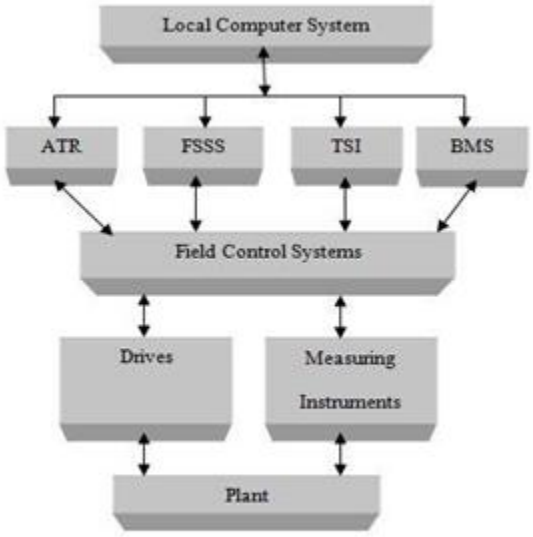


Fig. 3: DDCMIS architecture

.

November-December 2019
ISSN: 0193-4120 Page No. 1784 – 1798

1.4. Supervisory control and data acquisition Systems

Supervisory control and data acquisition (**SCADA**) are control systemarchitectures making use of networking data communications andGUIfor a high-level supervision, however makes use of additional separate PIDcontroller that interfaces to plant processes or machines in the plant. While operator interface that enables monitoring and process command issuing, like changes in controller set points are controlled via SCADA supervisory computer systems. And real-time control logic or calculations of controller is carried out by networking modules that are connected to sensors and actuators in the fields.

SCADA systems have are manufactured in a synonymous way to control systemsthat are distributed in functioning, however use several means of interfaces to plants. They large-scale processes including number of sites and working over vast distance are controlled by these systems. It forms one of the majorly used types of **power plant control system**.

SCADA software's exist only at the supervisory levels since control action is performed itself by RTUs or PLCs. SCADA control function is generally concerned to principal or supervisory levels of interventions. [3]

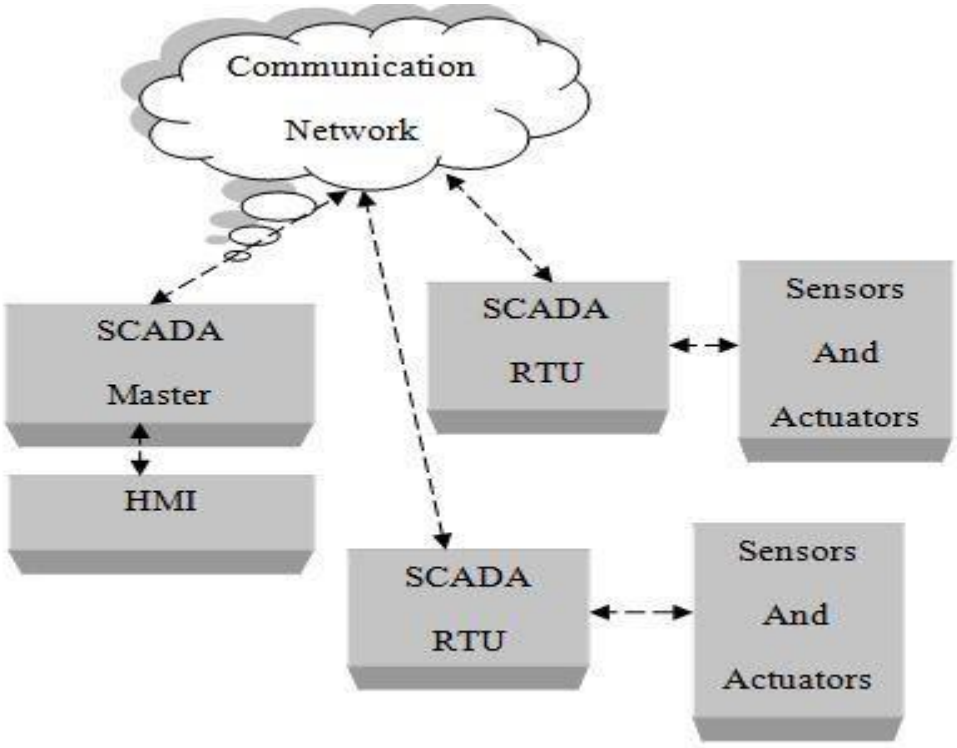


Fig. 4: SCADA architecture

2. PROPOSITION

When wetalk about any power plant, its operation is connected to the control room and these control rooms constitute different control systems as per the requirements of the power plant & are always physically located inside the Power Plant. The access & control to the Power Plant is from these control rooms i.e. at the field level data is sent to the input/output (I/O) module of different control systems which further accordingly process the data at the control stations placed in the control room as per

November-December 2019
ISSN: 0193-4120 Page No. 1784 – 1798

the desired requirements,. Since there can be different types of control systems involved in a particular power plant operation, a certain group of people with the desired set of specialties need to be present there to take care of the smooth operation of power plant.

The proposal is to remotely Control and monitor of a power plant. This is to put the power plant operation into the field of IoT and accordingly control& operate any particular power plant without physically being present there. But when we talk about remote access to the operation of power plants, the issues of confidentiality, integrity, availability, privacy, & authenticity of data becomes a big concern and need to be taken care of so that the remote control to power plants through internet is a possibility.

The proposition states that the data that will be received from the Field Control, going to the different modules of the control systems will be encrypted at that point and then this encrypted data will further be forwarded to the localized servers and via this server, data will be accessible to the remotely located station through internet. Only authenticated recipients will be able to decrypt the data accordingly and as a reply to the obtained information, remotely located station will send the encrypted response in return to local station.

Now the data will once more be decrypted and will be further passed to control modules, further the required data will be forwarded to the field control and accordingly the required actions will be taken. All the communication of the power plant from the Remote stations is through the internet. Control systems are linked to field devices e.g. actuators or sensors via input/output control modules. The real world parameters like pressure flows, temperatures and various operating conditions are communicated to the controllers via field devices. The Encryption Decryption scheme employed here is AES which is a block cipher i.e. the total number encrypted bytes is fixed. It currents encrypts a block of 16 bytes at a single time. [4]

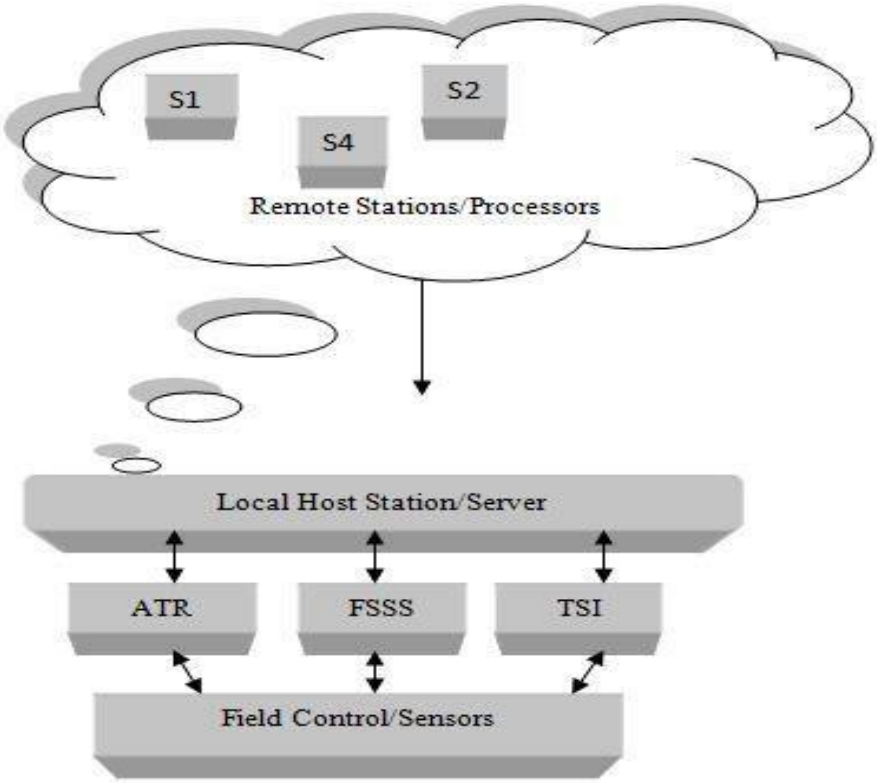


Fig. 5: General Proposition architecture

November-December 2019
ISSN: 0193-4120 Page No. 1784 – 1798

2.1. Representation of Input/output Architectures

The inputs that are received from the fields can be both analog and digital in nature. The digital inputs will directly be encrypted accordingly but the analoginputs will first be converted to digital form and then encrypted. Similarly when we get the logic outputs, it is further relocated to plant in encrypted form. The basic schemes of data communication are explained as:

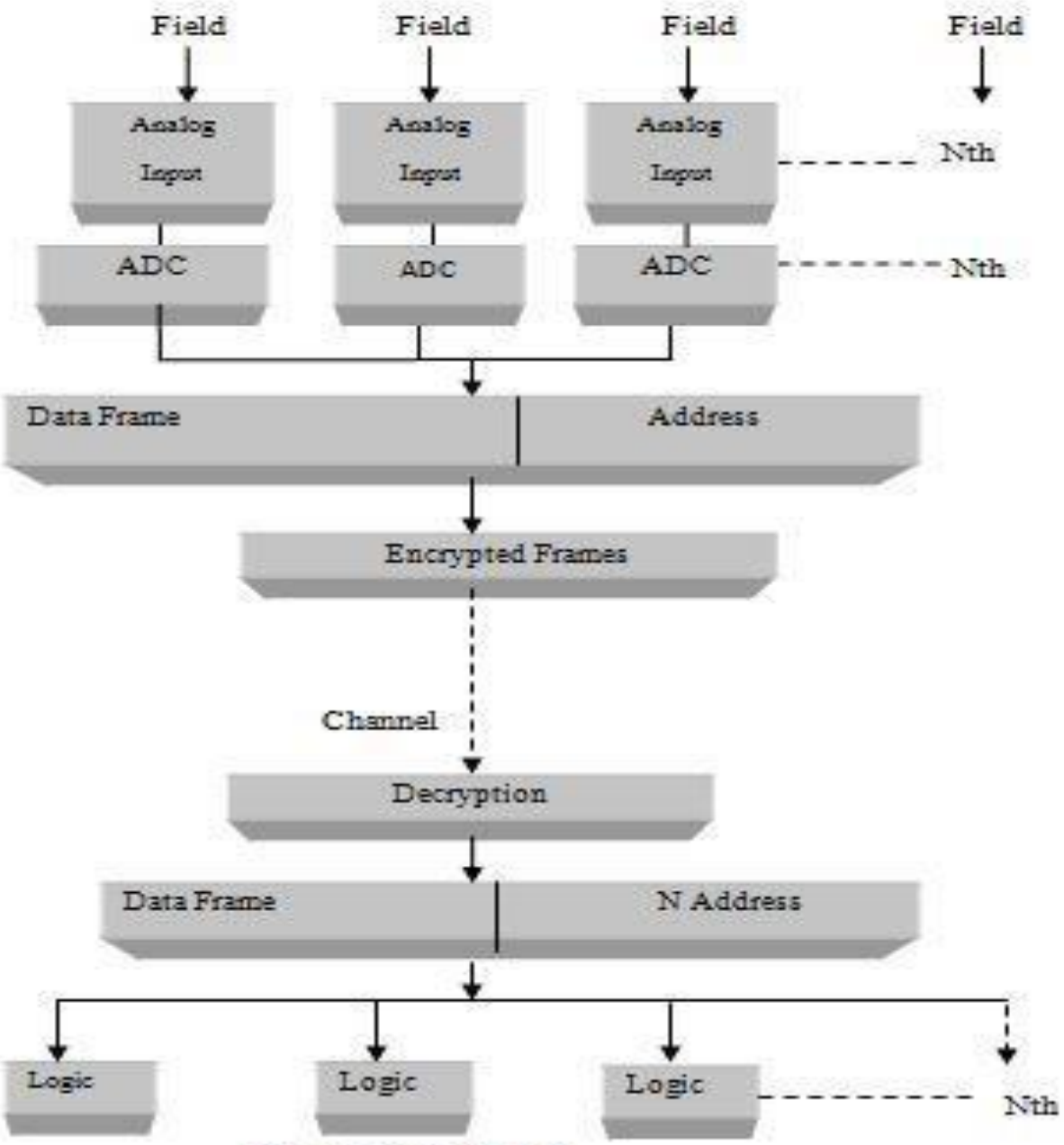


Fig. 6: Analog Input

November-December 2019
ISSN: 0193-4120 Page No. 1784 – 1798

In Fig. 6, N number of analog inputs from the field are accepted and further converted to the digital form using an analog digital converter (ADC). After the inputs are received in shape of bits which includes the addresses also, this data is encrypted prior its passed to channels. On next side the data accepted gets decrypted plus we have the data again that is further passed to the logic control.

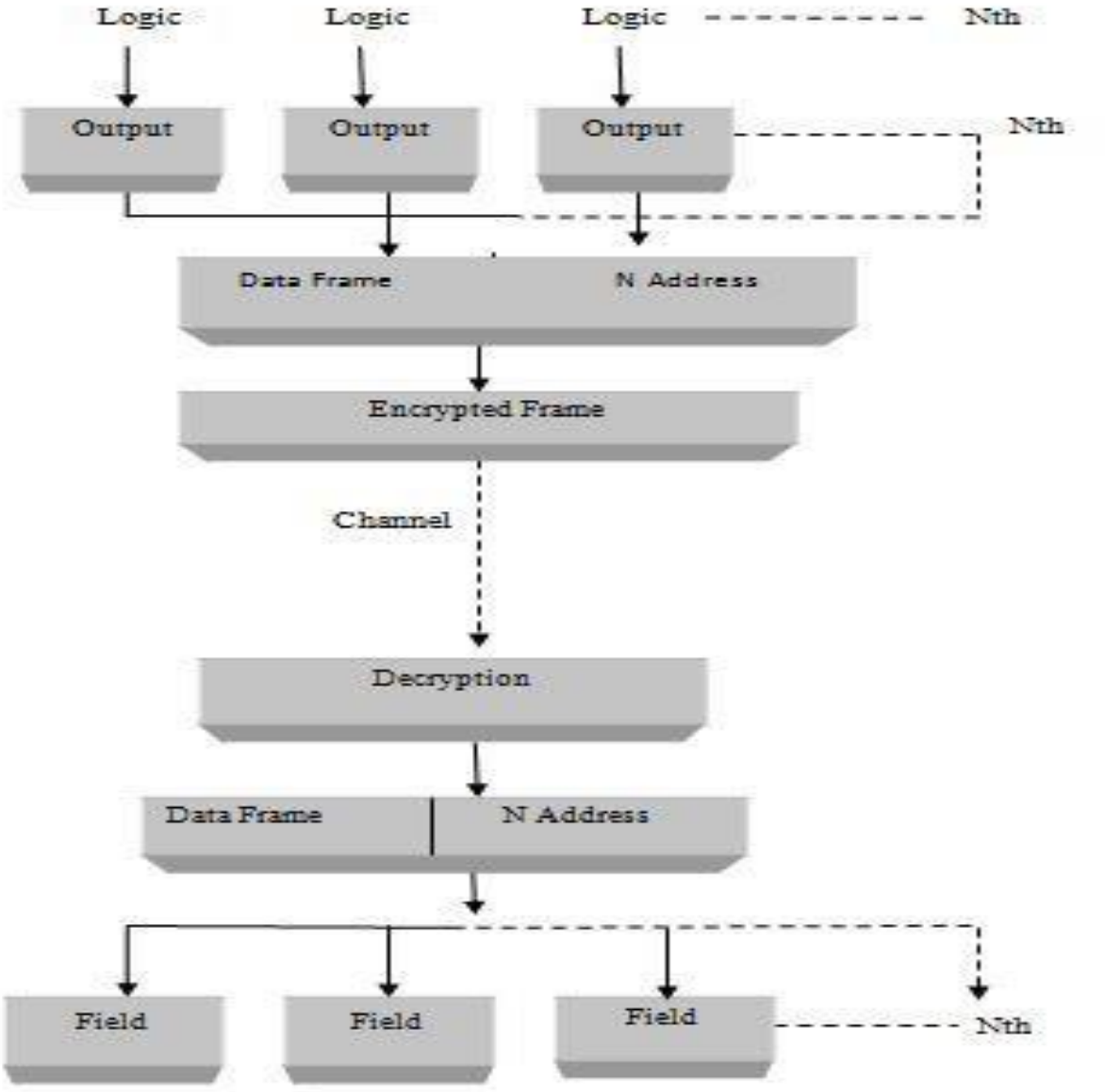


Fig. 7: Analog Output

In Fig. 7, the output is received after the logic is applied to it and then this logical output is again encrypted prior being passed across the channels. And on next side this encrypted logic output is further decrypted. Since the logic output is in the digital form, therefore before this logic output is passed to the field it is again converted to the analog form using a digital analog converter (DAC).

November-December 2019
ISSN: 0193-4120 Page No. 1784 – 1798

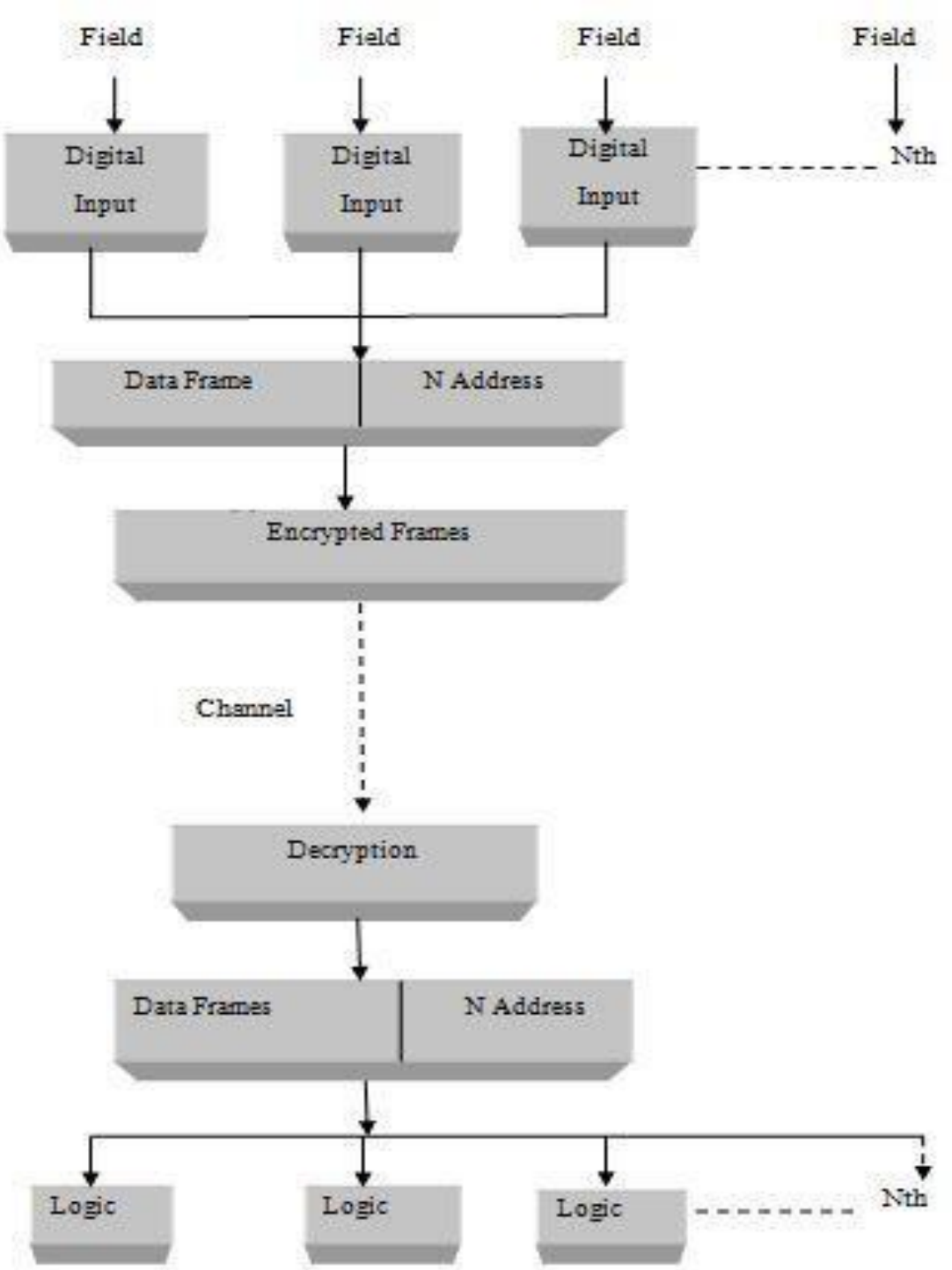


Fig. 8: Digital Input

In Fig. 8, N numbers of digital inputs are accepted from the field directly. This input data along with the address is encrypted before it is passed through the channel to the other part. And on the next side the data gets decrypted and the logic is applied to this input data accordingly and passed on further to the logic control.

November-December 2019
ISSN: 0193-4120 Page No. 1784 – 1798

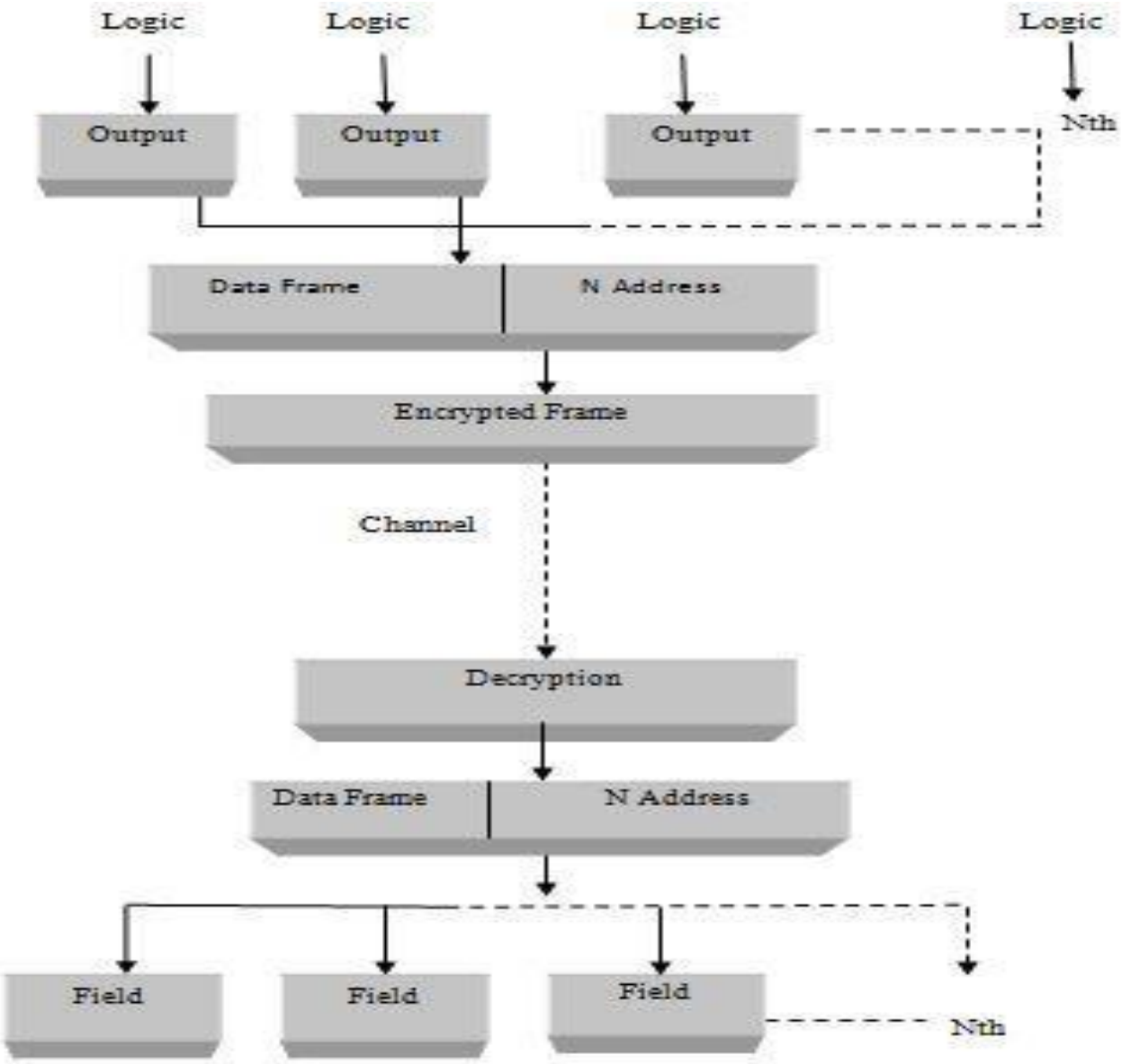


Fig. 9: Digital Output

In Fig. 9, once the logic is applied to the digital input and the desired actions are taken accordingly. This logic output with the address is again encrypted prior being passed across the channels. On the next side of the channel the encrypted logic output is received and further decrypted and ultimately passed to the field.

3. IMPLEMENTATION

We started with the turbine start up and shut down scheme of NTPC Power station. Here system S1 is linked to Tx/Rx (Transmitter/Receiver) of the turbine controlling cabinet. While further to the next side a server is connected to this system via an Ethernet router. (Fig. 10).

November-December 2019
ISSN: 0193-4120 Page No. 1784 – 1798

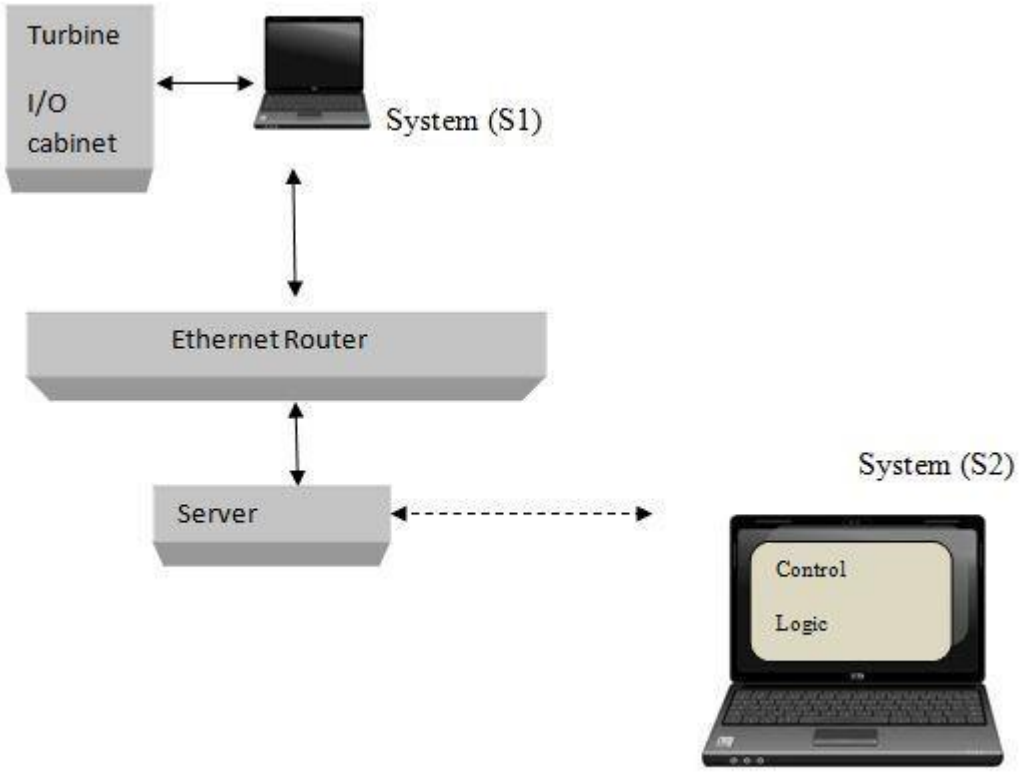


Fig. 10: Implementation

The conventional nomenclature of turbine start up and along with inputs/outputs utilized is;

Input 1: 10MAA10CG001B, XG01; STM TURB HP ESV1, OPEN
Input 2: 10MAA20CG001B, XG01; STM TURB HP ESV2, OPEN
Input 3: 10MAC11CG021B, XG01; STM TURB LP ESV1, OPEN
Input 4: 10MAC12CG021B, XG01; STM TURB HP ESV2, OPEN
Input 5: 10MYA010U001, XT18; SPEED TRANS ENT, LOW
Input 6: 10MYA010U001, XT25; TURBINE GOVERNOR, FAULTED

The system that lays in-between control cabinet and the server is made use for encryption/decryption of data sequences as following:

Cipher text of Input 1: cfee c2 38 3f 47 a2 15 e0 59 b4 20 60 5b 70 1d
Cipher text of Input 2: f5 5c 99 a7 a9 97 2a 39 62 28 e9 9f 01 e0 63 de
Cipher text of Input 3: f9 3c ef 4c 31 4b 6f f2 62 b4 a2 0b 8e ce e6 9e
Cipher text of Input 4: 2a 7a ff 47 fb fc f3 3c c7 b5 29 66 95 36 ee 64
Cipher text of Input 5: 48 c4 11 88 07 66 8f f4 f8 e5 fc 1f 2a 34 5f 2c
Cipher text of Input 6: 3c 88 4e 3e b8 e6 9e ed 61 41 8c aa 79 c0 e8 a3

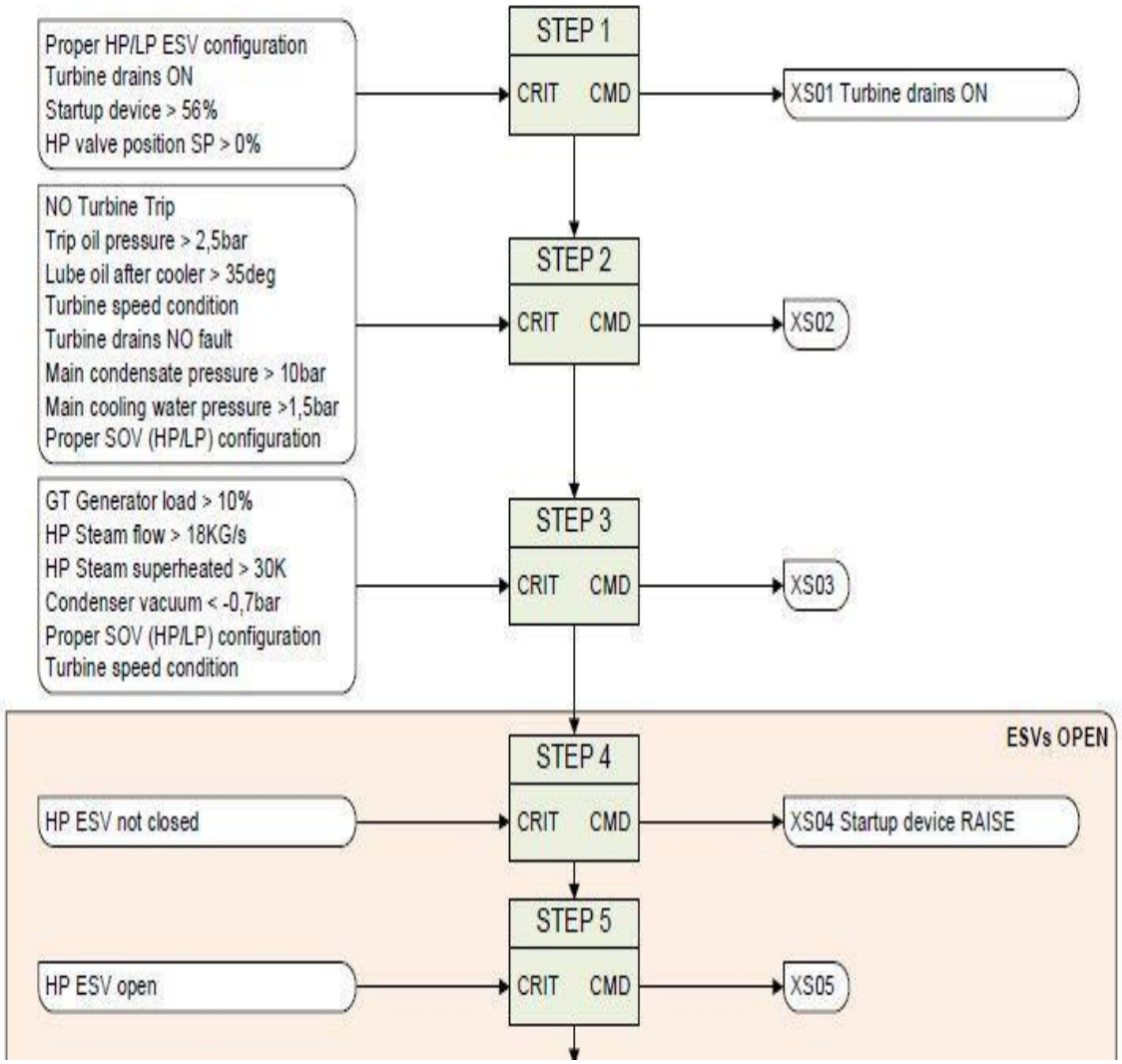
November-December 2019
ISSN: 0193-4120 Page No. 1784 – 1798

The remote system is used for accessing the server and further decryption of cipher text is done in sequence and the results attained are as following:

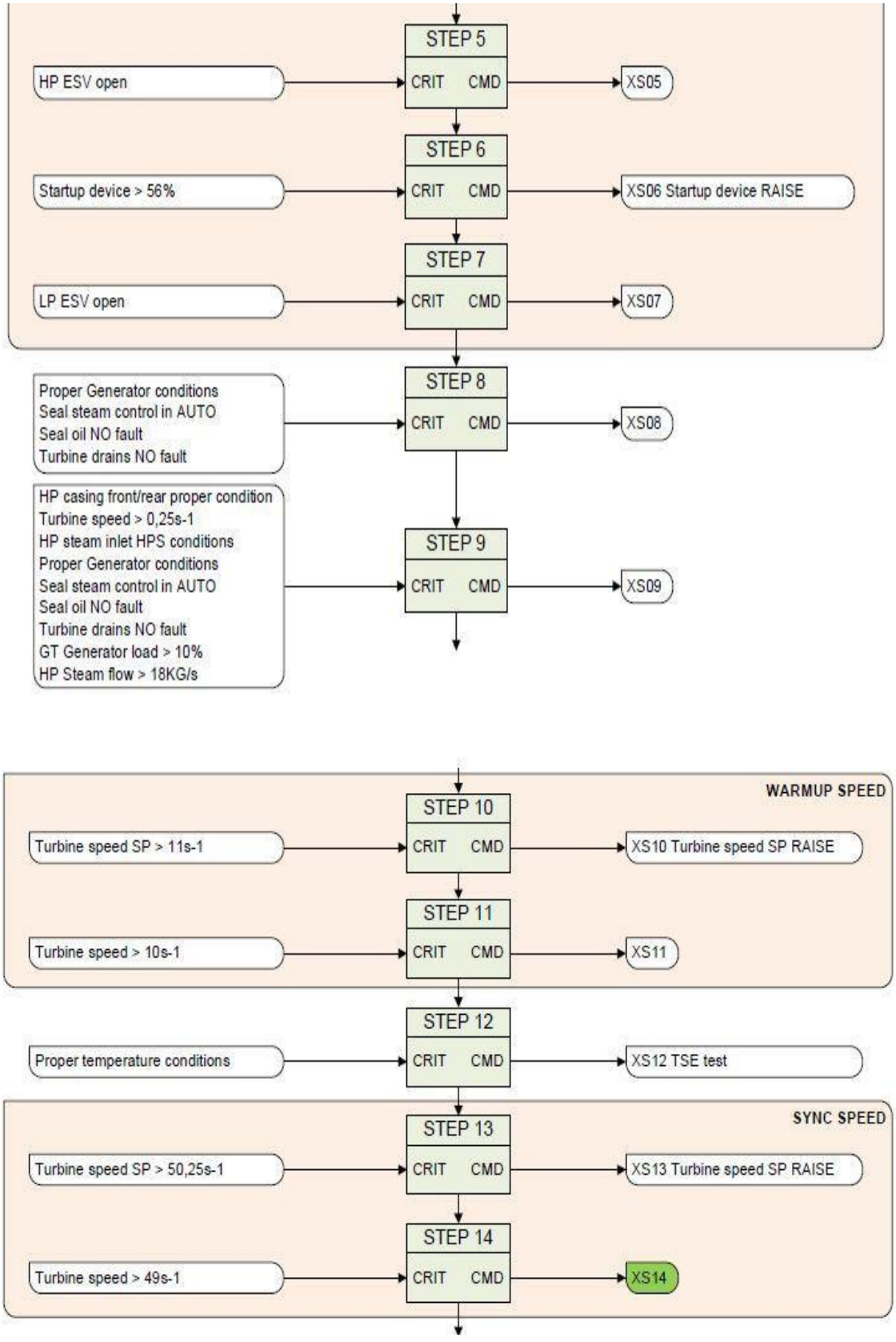
Output 1: 31 30 4d 41 41 31 30 43 47 30 30 31 58 47 30 31: 10MAA10CG001B, XG01
Output 2: 31 30 4d 44 41 31 30 43 47 30 30 31 58 47 30 31: 10MAA20CG001B, XG01
Output 3: 31 30 4d 41 43 31 31 43 47 30 32 31 58 47 30 31: 10MAC11CG021B, XG01
Output 4: 31 30 4d 41 43 31 32 43 47 30 32 31 58 47 30 31: 10MAC12CG021B, XG01
Output 5: 31 30 4d 59 41 30 31 30 55 30 30 31 58 54 31 38: 10MYA010U001, XT18
Output 6: 31 30 4d 59 41 30 31 30 55 30 30 31 58 54 32 35: 10MYA010U001, XT25

The control logics are operated on decrypted data. Next the outputs are supplied back to servers once more in encrypted forms, and system S1 is used for accessing data from servers and results are supplied back in decrypted forms to the Tx/Rx of controlling cabinets. Controlling logics of turbine start up/shut down as provided by NTPC:

Start up sequence logic:



November-December 2019
ISSN: 0193-4120 Page No. 1784 – 1798



November-December 2019
ISSN: 0193-4120 Page No. 1784 – 1798

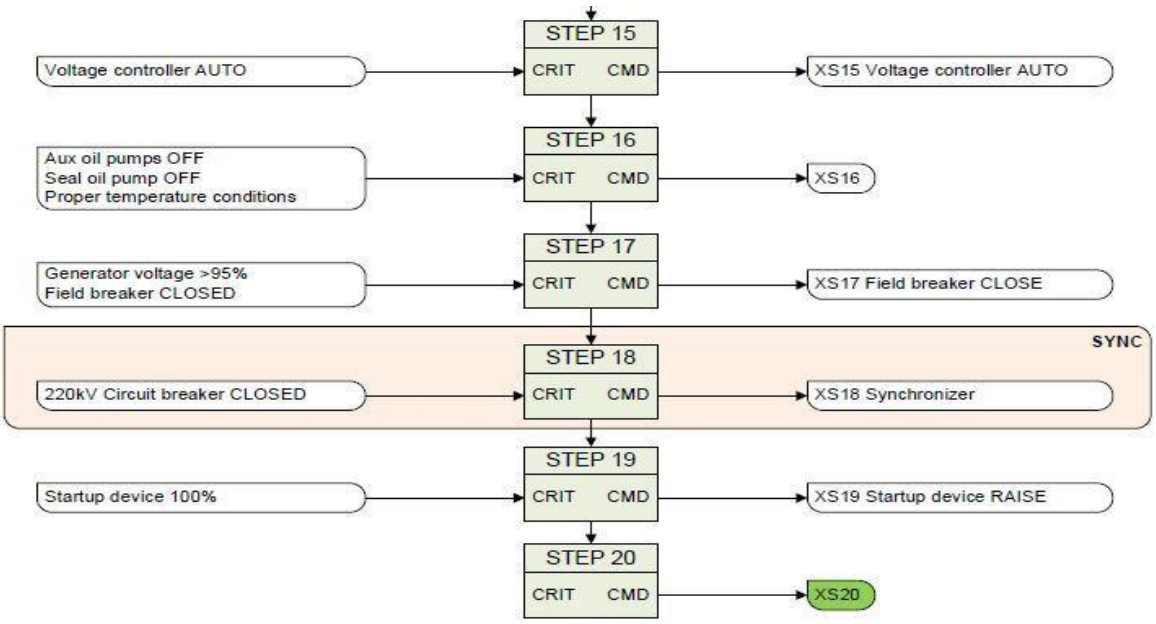


Fig 11: Start-up Sequence Logic

Shut Down sequence logic:

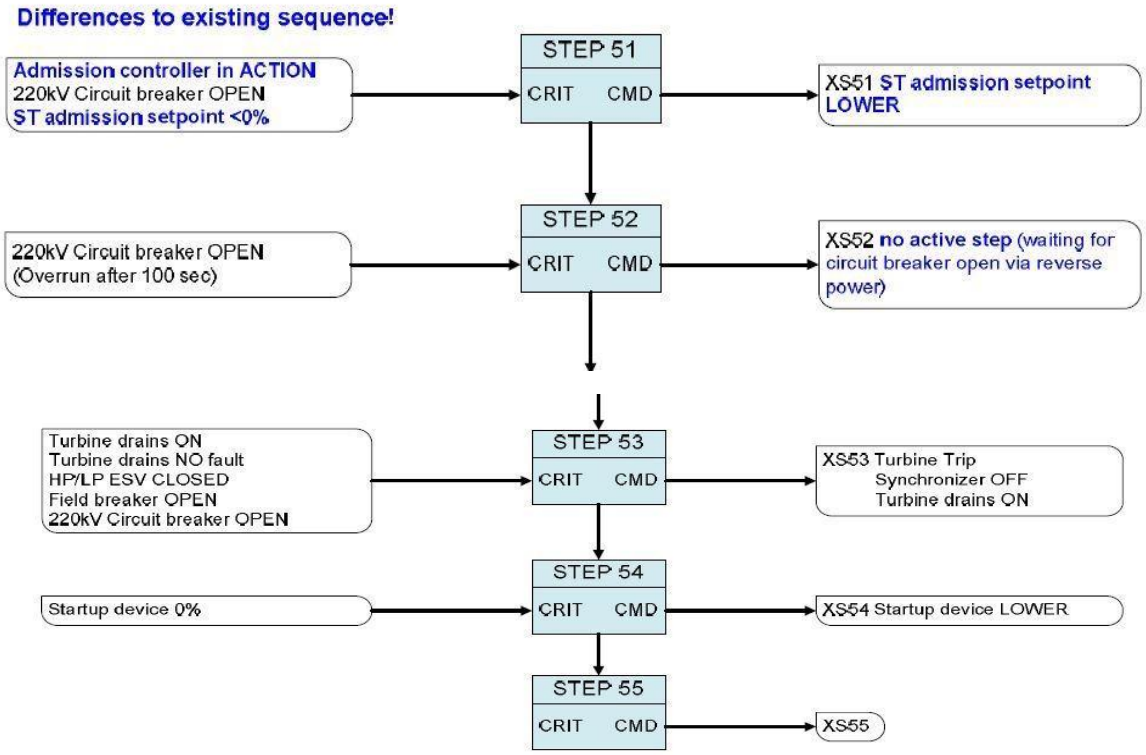


Fig 12: Shut Down Sequence Logic

November-December 2019
ISSN: 0193-4120 Page No. 1784 – 1798

The controlling logics in remote system S2 is used for performing logical operations on outputs and further give Logical outputs as following:
Output 1: 10MYAU1UU001, ZA06; SPEED POSN SETPOINT, STOP RAISE
Output 2: 11LBA10EE001, YP01; WARM UP LINES, PROT SHUTD
Output 3: 12LBA10EE001, YP01; WARM UP LINES, PROT SHUTD
Output 4: 10MAL10EE001, YA21; TURBINE DRAINS, ON
Output 5: 10MAX47BY001M, YB21; START UP DEVICE, RAISE
Output 6: 10MAY01EP001, Y740; TSE TESTING, BLOCK
Cipher text of Output 1: 2f 5c 24 bc f9 8d 8c b7 a2 aa 90 52 77 f7 df 12
Cipher text of Output 2: c2 0e 77 06 88 5a c5 04 7d 9d 01 48 44 0c b7 95
Cipher text of Output 3: 16 93 e0 de 92 57 6d 70 ce f0 16 a5 3c bd 87 45
Cipher text of Output 4: 36 58 79 82 a3 74 5e c6 74 b6 0d 9b 01 7e 66 74
Cipher text of Output 5: b3 8a c7 97 21 8b b6 32 39 b2 c4 d3 64 d0 aa 8c
Cipher text for Output 6: 87 d7 d7ff 35 b6 d4 eaec 43 85 cf 10 39 01 fe

The Outputs in encrypted forms is supplied back across the servers to the system S1 where it is decrypted and further passed to the controlling cabinets.
Output 1: 31 30 4d 5a 41 55 31 55 55 30 30 31 5a 41 36 30: 10MYAU1001, ZA06
Output 2: 31 31 4c 42 41 31 30 45 45 30 30 31 59 50 3031: 11LBA10EE001, YP01
Output 3: 31 32 4c 42 41 31 30 45 45 30 30 31 59 50 3031: 12LBA10EE001, YP01
Output 4: 31 31 4d 41 4c 31 30 45 45 30 30 31 59 41 32 31: 10MAL10EE001, YA21
Output 5: 31 30 4d 41 58 34 37 42 59 30 30 31 59 42 32 31: 10MAX47BY001M, YB21
Output 6: 31 30 4d 41 59 30 31 45 50 30 30 31 59 37 34 30: 10MAY01EP001, Y740

4. CONCLUSION AND SCOPE

The implementations was carried out at C&I department of NTPC and the data security is achieved using AES as the encryption scheme at layer 2 of the communication protocol. The problem that we encountered was regarding the time delay; the time taken for the whole encryption decryption was more than expected.

The further scope of this paper will be using further an encrypting scheme that will accordingly minimize the time delays and provide data security as well.

5. ACKNOWLEDGEMENT

Writers of this research are thankful to the Founder President of Amity University, Dr. Ashok K. Chauhan, who has overpoweringly shown his eager attention in development study in Amity University and is an inspiration for accomplishing advanced triumph.

REFERENCES

1. https://en.wikipedia.org/wiki/Programmable_logic_controller
2. https://en.wikipedia.org/wiki/Distributed_control_system
3. https://en.wikipedia.org/wiki/SCADA
4. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
5. http://www.power-eng.com/o-m/instrumentation-controls.html
6. http://www.ntpc.co.in/
7. Bijoy Babu,ThafasalIjyas,Muneer P.,Justin Varghese, Anti-Cyber Crimes (ICACC), 2017 2nd International Conference, Abha, Saudi Arabia, “Security issues in SCADA based industrial control systems”
8. Vivek Umasuthan,Transmission and Distribution Conference and Exposition (T&D), 2016 IEEE/PES“Protecting the Communications Network at Layer 2”.

November-December 2019
ISSN: 0193-4120 Page No. 1784 – 1798

9. Hyun-Jin Kim;Hyun-Soo Chang;Jeong-Jun Suh;Tae-shik Shon,2016 International Conference on Industrial Engineering, Management Science and Application (ICIMSA), "A Study on DeviceSecurityinIoTConvergence"
10. MinelaGrabovica;SrđanPopić;DraženPezer; Vladimir Knežević2016 Zooming Innovation in Consumer Electronics International Conference (ZINC), "Providedsecuritymeasures of enabling technologies in Internet of Things (IoT): A survey"
11. ArunanSivanathan;Daniel Sherratt;Hassan Habibi Gharakheili;Vijay Sivaraman;Arun Vishwanath, 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), "Lowcost flow-basedsecuritysolutions for smart-homeIoTdevices"
12. Sandip Ray;Swarup Bhunia;YierJin;Mark Tehranipoor,2016 IEEE 34th VLSI Test Symposium (VTS), Year: 2016, "Securityvalidation inIoTspace"

Mrs. Iqra Hussain has received her M.Sc. Information Technology from Islamic University of Science and Technology Jammu and Kashmir and B.sc Information Technology from Kashmir University, India. Her major areas of interests include Network security in Internet of Things. She has research publications in areas of Network security, cryptography, IOT and layer two protocols published in International Conferences. She has consistently maintained percentage above distinction throughout her academic career. She is currently pursuing her PhD as a full time Research Scholar from Amity University Noida, India.

Dr. Nitin Pandey was born in India. He is an Assistant Professor at Amity Institute of Information Technology, Amity University Uttar Pradesh. His area of research is Coding theory, Cryptography and Network Security. He is completed his Ph.D. from Mewar University Chittorgarh. He has done B.Sc. and M.Sc. in Mathematics from DeenDayalUpadhaya University Gorakhpur Uttar Pradesh. He has completed Master of Computer Application from Maharishi Dayanand University Rohtak Haryana. He is CISCO Certified Instructor. He is the author and co-author of more than 20 publications in technical journals and conferences.

Dr. Mukesh Negi is a Ph. D. (Comp. Sc.) from JJT University, Rajasthan, Masters of Computer Applications (MCA) from M.D University, Rohtak, Haryana, M.Sc. (Computer Science) from M.D University, Rohtak, Haryana, B.Sc. (PCM) from Kumaon University, Nainital, Uttarakhand. He is working as Sr. Technical Project Manager, India Business Group with IT MNC TechMahindra Ltd, Noida, India and has a total IT Industry Experience of 16+ Years.