BEFORE THE HON'BLE CENTRAL ELECTRICITY REGULATORY COMMISSION
NEW DELHI

PETITION NO……

IN THE MATTER OF : Petition Under Section 62 and 79 (1) (a) of the Electricity Act, 2003 read with Chapter-III of the Central Electricity Regulatory Commission (Conduct of Business) Regulations, 2023 and Chapter-3, Regulation-9 of Central Electricity Regulatory Commission (Terms and Conditions of Tariff) Regulations, 2024 for approval of tariff of **Tanda Super Thermal Power Station Stage-I (4x110 MW) for the period from 01.04.2024 to 31.03.2029**.

INDEX

BEFORE THE HON'BLE CENTRAL ELECTRICITY REGULATORY COMMISSION
NEW DELHI

PETITION NO……

IN THE MATTER OF : Petition Under Section 62 and 79 (1) (a) of the Electricity Act, 2003 read with Chapter-III of the Central Electricity Regulatory Commission (Conduct of Business) Regulations, 2023 and Chapter-3, Regulation-9 of Central Electricity Regulatory Commission (Terms and Conditions of Tariff) Regulations, 2024 for approval of tariff of **Tanda Super Thermal Power Station Stage-I (4x110 MW) for the period from 01.04.2024 to 31.03.2029**.

AND
IN THE MATTER OF

Petitioner: : NTPC Ltd.
NTPC Bhawan
Core-7, Scope Complex
7, Institutional Area, Lodhi Road
New Delhi-110 003.

Respondents **1.** Uttar Pradesh Power Corp. Ltd. (UPPCL)
Shakti Bhawan
14, Ashok Marg,
Lucknow – 226 001.

The Petitioner humbly states that:

1) The Petitioner herein NTPC Ltd. (hereinafter referred to as '**Petitioner**' or **'NTPC')**, is a company incorporated under provisions of the Company Act, 1956 and a Government Company as defined under Section 2(45) of the Companies Act, 2013. Further, NTPC is a 'Generating Company' as defined under Section 2(28) of the Electricity Act, 2003.

2) In terms of Section 79(1)(a) of Electricity Act, 2003, the Hon'ble Commission has been vested with the functions to regulate the tariff of NTPC, being a Generating Company owned and controlled by the Central Government. The regulation of the tariff of NTPC is as provided under Section 79(1)(a) read

Section 61, 62 and 64 of the Electricity Act, 2003 and the Regulations notified by the Hon'ble Commission in exercise of powers under Section 178 read with Section 61 of the Electricity Act, 2003.

3) The Petitioner is having power stations/ projects at different regions and places in the country. **Tanda Super Thermal Power Station Stage-I (4x110 MW) (**hereinafter referred to as Tanda St-I) is one such station located in the State of Uttar Pradesh. The power generated from Tanda St-I is being supplied to the respondents herein above.

4) The Hon'ble Commission has notified the Central Electricity Regulatory Commission (Terms & Conditions of Tariff) Regulations, 2024 (hereinafter 'Tariff Regulations 2024') which came into force from 01.04.2024, specifying the terms & conditions and methodology of tariff determination for the period 01.04.2024 to 31.03.2029.

5) Regulation 9(2) of Tariff Regulations 2024 provides as follows:

"(2) In case of an existing generating station or unit thereof, or transmission system or element thereof, the application shall be made by the generating company or the transmission licensee, as the case may be, by 30.11.2024 , based on admitted capital cost including additional capital expenditure already admitted and incurred up to 31.3.2024 (either based on actual or projected additional capital expenditure) and estimated additional capital expenditure for the respective years of the tariff period 2024-29 along with the true up petition for the period 2019-24 in accordance with the CERC (Terms and Conditions of Tariff) Regulations, 2019."

In terms of above, the Petitioner is filing the present petition for determination of tariff for Tanda St-I for the period from 01.04.2024 to 31.03.2029 as per the Tariff Regulations 2024.

6) The tariff of the Tanda St-I for the tariff period 1.4.2019 to 31.3.2024 was determined by the Hon'ble Commission vide its order dated 17.042024 in Petition No.445/GT/2020 in accordance with the CERC (Terms & Conditions of Tariff) Regulations 2019. The petitioner vide affidavit dated 21.11.2024 had filed

a separate true up petition for the period 01.04.2019 to 31.03.2024 for revision of tariff in line with the applicable provisions of Tariff Regulations 2019.

7) It is submitted that Hon'ble Commission vide order dated 17.04.2024 in Petition no 445/GT/2020 has allowed a capital cost of Rs 124374.52 Lakh as on 31.03.2024 based on the admitted projected capital expenditure for the 2019-24 period. However, the actual closing capital cost as on 31.03.2024 has been worked out in the foresaid true-up petition as Rs. 124753.82 Lakh based on the actual expenditure after truing up exercise for the period 2019-24. Accordingly, the Petitioner has adjusted an amount of Rs. 379.30 Lakh from the admitted capital cost as on 31.03.2024 and accordingly the opening capital cost as on 01.04.2024 has been considered as Rs. 124753.82 Lakh in the instant petition. The Hon'ble Commission may be pleased to accordingly adopt this adjustment in the admitted capital cost as on 31.3.2024 and determine the tariff in the present petition for the period 2024-29.

8) The capital cost claimed in the instant petition is based on the opening capital cost as on 01.04.2024 considered as above and projected estimated capital expenditures claimed for the period 2024-29 under Regulation 19 and Regulation 24, 25 and 26 of the Tariff Regulations, 2024.

9) The Petitioner further respectfully submits that as per Regulation 36(1)(6) of the Tariff Regulations 2024, the water charges, security expenses, ash transportation expenses and capital spares consumed for thermal generating stations are to be allowed separately. The details in respect of water charges such as type of cooling water system, water consumption, rate of water charges as applicable for 2023-24 have been furnished below. In accordance with provision of the Regulations, the petitioner shall be furnishing the details of actual for the relevant year at the time of truing up and the same shall be subject to retrospective adjustment.

Description	**Remarks**
Type of Plant	Coal based station
Type of cooling water system	Closed Cycle

Rate of Water charges	Water Charges: Rs 12.48 (Rs/1000 Cubic Feet) Royalty: Rs 6 Lakh/Cusec Per Year
Total Water Charges	Rs. 98.55 lacs

10) Similarly, the Petitioner is claiming the security & ash transportation expenses based on the estimated expenses for the period 2024-29, the same shall be subject to retrospective adjustment based on actuals at the time of truing up. In respect of capital spares consumption, it is submitted that the same shall be claimed at the time of true-up in terms of the proviso to the Regulation 36(1)(6) based on actual consumption of spares during the period 2024-29.

11) However, it is submitted that the expenditure towards the ash transportation charges is recurring in nature and the Petitioner has been incurring ash transportation expenditure in its stations in the current tariff period also. In case the same is permitted to be recovered after the issuance of the tariff order for the period 2024-29, there will be additional liability on the beneficiary on account of the interest payment for the period till the time the tariff petitions for the period 2024-29 is decided. To avoid the interest payment liability of the beneficiaries, it is prayed that the petitioner may be allowed to recover/ pass on the ash transportation charges on a monthly basis subject to true-up at the end of the 2024-29 period.

12) The petitioner humbly submits that petition no. 227/MP/2024 has been filed by the petitioner concerning Ash Transport Expenditure for its stations which is under active consideration of this Hon'ble Commission and the outcome of the said petition will be applicable to the instant petition also.

13) The petitioner has accordingly calculated the tariff for 2024-29 period based on the above and the same is enclosed as **Appendix-I** to this petition.

14) The Petitioner humbly submits that the pay/wage revision for the employees of the Petitioner will be due wef 01.01.2027. Further, the wage/pay revision of CISF and Kendriya Vidyalaya employees will also be due for revision during

tariff period 2024-29. Regulation-36(1)(8) of CERC (Terms & Conditions of Tariff) Regulations-2024 provides as below:

"In the case of a generating company owned by the Central or State Government, the impact on account of implementation of wage or pay revision shall be allowed at the time of truing up of tariff."

In accordance with the above said regulation, the Petitioner shall approach the Hon'ble Commission for allowing the impact of Pay/wage revision of employees of the Petitioner i.e. NTPC Limited, CISF and Kendriya Vidyalaya (wherever applicable) as additional O&M at the time of truing-up of tariff for the control period 2024-29. Hon'ble Commission may be pleased to grant liberty to consider the impact of wage/pay revision as an additional impact on O&M from the date same is implemented and allow the same as additional O&M over and above the normative O&M.

15) It is submitted that in terms of Regulation 60 (5) of the Tariff Regulations 2024, the Petitioner is required to furnish details qua providing the details of Landed Price & Gross Calorific Value ("GCV") of coal in Form 15. It is further submitted that the Petitioner in terms of Regulation 40 of the Tariff Regulations 2019 was required to furnish the details for Landed Price & GCV of coal also as per Form 15 of the Tariff Regulations, 2019.

16) However, in so far as the present Petition is concerned, the Petitioner has prepared & submitted the data of coal as per Form 15 of the Tariff Regulations, 2019. The same is because of the following reasons:-

(a) This Hon'ble Commission had notified the Tariff Regulations, 2019 on 07.03.2019 and the same was in effect till 31.03.2024.

(b) The Petitioner being a diligent utility has been seamlessly providing the said data of coal in terms of the prescribed format (i.e. Form 15 of Annexure-I (Part I)) of the Tariff Regulations, 2019 to this Hon'ble Commission for computation of Interest on Working Capital.

(c) Thereafter, this Hon'ble Commission on 15.03.2024 notified the Tariff Regulations, 2024, wherein the format of Form 15 was changed.

amended by this Hon'ble Commission and a new format was placed in the Tariff Regulations 2024 in the month of June'2024.

(d) By virtue of the said change, the Petitioner has been obligated to furnish the data of coal for its existing plants month wise for the preceding 12 months i.e. for FY 2023-24 for computation of Interest on Working Capital.

17) It is humbly submitted that by virtue of the Tariff Regulations, 2024, this Hon'ble Commission has added a new format/ revised the format of Form-15 which has not prescribed in the past Tariff Regulations i.e. of 2019. Hence, it is only now (in the Tariff Regulations 2024) that the Petitioner has been obligated to furnish the data of coal as per the new format of Form-15.

A True copy of the Form 15 of Tariff Regulations 2019 and Form 15 of Tariff Regulations 2024, is marked and annexed herewith as Annexure P/ [•]

18) It is respectfully submitted that since the format for Form 15 has been changed in Tariff Regulations, 2024 and was notified in the month of June'2024, the Petitioner could not have been aware about the said changes earlier, hence the Petitioner did not maintain the data required in new format of Form 15 of Tariff Regulations, 2024.

19) Therefore, this Hon'ble Commission may kindly exempt the Petitioner from furnishing the data of coal in terms of new format of Form 15 of the Tariff Regulations, 2024 & may be allowed to furnish the details of coal for FY 2023-24 in terms of the prescribed format of Form-15 of the Tariff Regulations, 2019.

20) In light of the above submissions, it may kindly be noted that no prejudice shall be caused to any party if the Petitioner is allowed for providing the details of Landed Price & GCV of coal to this Hon'ble Commission in terms of Form 15 of the Tariff Regulations, 2019 as the value of Landed Price & GCV of coal will remains unaffected.

21) It is submitted the Petitioner has served the copy of the Petition on to the Respondents mentioned herein above and has posted the Petition on the company website i.e. www.ntpc.co.in.

22) In accordance with the 'Conduct of Business Regulations 2023' of the Hon'ble Commission, the Petitioner shall, within 7 days after filing the tariff petition, publish a notice about such filing in at least two daily leading digital newspapers one in English language and another in any of the Indian languages, having wide circulation in each of the States and Union Territories where the beneficiaries are situated, as per Form 14 appended to these regulations. Subsequently, the Petitioner shall submit the proof of publications as soft copies of the publications under an affidavit through the e-filing portal of the Hon'ble Commission within one week from the date of publication. Further, the Petitioner shall also submit the detail of expenses incurred for publication of the notice along with the prayer for recovery of Publication Expenses as per Regulation-94 of CERC Tariff Regulations 2024.

23) It is submitted that the Petitioner has already paid the requisite filing fee vide **UTR No. 37c568eba62158b7b321** on 24.04.2024 for the year 2024-25 and the details of the same have been duly furnished to the Hon'ble Commission. For the subsequent years, it shall be paid as per the provisions of the CERC (Payment of Fees) Regulations, 2012 as amended. Further Regulation 94 (1) of Tariff Regulations 2024 provides that the application fee and publication expenses may be allowed to be recovered directly from the beneficiaries at the discretion of the Hon'ble Commission. Accordingly, it is prayed that Hon'ble Commission may be pleased to allow recovery of filing fee and publication fee directly from the beneficiaries.

24) It is submitted that the petitioner is filing this tariff petition subject to the outcome of its various appeals/ petitions pending before different courts. Besides, the petitions filed by NTPC for determination of capital base as on 31.3.2019 through true-up exercise are pending before the Hon'ble Commission and would take some time. The Petitioner, therefore, reserves its right to amend the tariff petition as per the outcome in such appeals/ petitions, if required.

Prayers

In the light of the above submissions, the Petitioner, therefore, prays that the Hon'ble Commission may be pleased to:

i) Approve tariff of **Tanda Super Thermal Power Station Stage-I (4x110 MW)** for the period from 01.04.2024 to 31.03.2029.

ii) Allow the recovery of filing fees as & when paid to the Hon'ble Commission and publication expenses from the beneficiaries.

iii) Allow reimbursement of Ash Transportation Charges directly from the beneficiaries on monthly basis, subject to true up.

iv) Grant liberty to approach the Hon'ble Commission to allow for the recovery of pay/wage revision due in 2024-29 period as additional O&M over and above the normative O&M.

v) Pass any other order as it may deem fit in the circumstances mentioned above.

Petitioner

Noida

BEFORE THE HON'BLE CENTRAL ELECTRICITY REGULATORY COMMISSION
NEW DELHI

PETITION NO.....

IN THE MATTER OF : Petition Under Section 62 and 79 (1) (a) of the Electricity Act, 2003 read with Chapter-III of the Central Electricity Regulatory Commission (Conduct of Business) Regulations, 2023 and Chapter-3, Regulation-9 of Central Electricity Regulatory Commission (Terms and Conditions of Tariff) Regulations, 2024 for determination of tariff of **Tanda Super Thermal Power Station Stage-I (4x110 MW) for the period from 01.04.2024 to 31.03.2029**.

AND
IN THE MATTER OF

Petitioner: NTPC Ltd.
NTPC Bhawan
Core-7, Scope Complex
7, Institutional Area, Lodhi Road
New Delhi-110 003

Respondents: 1. Uttar Pradesh Power Corp. Ltd. (UPPCL)
Shakti Bhawan
14, Ashok Marg
Lucknow – 226 001

NOTARY YOGENDRA SINGH AREA NOIDA G.B. NAGAR REGN. NO. 5677/08 NOTARIAL NOTARIAL GOVT. OF INDIA

AFFIDAVIT

I, Parimal Piyush, Son of Late Bharat Mishra, aged about 49 years, resident of IN1-2004, Inspire, Eldeco Aamantran, Sector-119, Noida (UP), do hereby solemnly affirm and state as follows:

1. That the deponent is the Additional General Manager (Commercial) of the Petitioner NTPC Ltd. and is well conversant with the facts and the circumstances of the case and therefore competent to swear this affidavit.

2. That the accompanying Petition under Section 62 and 79 (1) (a) of the Electricity Act, 2003, has been filed by my authorized representative under my instruction

NOTARY YOGENDRA SINGH AREA NOIDA G.B. NAGAR REGN. NO. 5677/08 GOVT. OF INDIA

परिमल पीयूष/PARIMAL PIYUSH
अपर महाप्रबन्धक (वाणिज्यिक)
Addl. General Manager (Commercial)
एन टी पी सी लिमिटेड/NTPC LIMITED
EOC, A-8A, Sector-24, Noida-201301 (U.P.)

Signature Not Verified
Digitally signed by PARIMAL PIYUSH
Date: 2024.11.25 22:55:12 IST
Reason: AGM(Commercial)
Location: NTPC Limited

and the contents of the same are true and correct to the best of my knowledge and belief.

3. That the contents of Para No .....1..... to .....24.... as mentioned in the Petition are true and correct based on the my personal knowledge, belief and records maintained in the office.

4. That the annexures annexed to the Petition are correct and true copies of the respective originals.

5. That the Deponent has not filed any other Petition or Appeal before any other forum or court of law with respect to the subject matter of the dispute.

परिमल पीयूष/PARIMAL PIYUSH
अपर महाप्रबन्धक (वाणिज्यिक)
Addl. General Manager (Commercial)
एन टी पी सी लिमिटेड/NTPC LIMITED
EOC, A-8A, Sector-24, Noida-201301 (U.P.)

(Deponent)

Verification:

Verified at Noida on this ..... day of November 2024, that the contents of my above noted affidavit are true and correct to my knowledge and no part of it is false and nothing material has been concealed therefrom.

(Deponent)

परिमल पीयूष/PARIMAL PIYUSH
अपर महाप्रबन्धक (वाणिज्यिक)
Addl. General Manager (Commercial)
एन टी पी सी लिमिटेड/NTPC LIMITED
EOC, A-8A, Sector-24, Noida-201301 (U.P.)

NOTARY
YOGENDRA SINGH
AREA NOIDA
G.B.NAGAR
REGN. NO. 5677/08
GOVT. OF INDIA

ATTESTED
YOGENDRA SINGH
NOTARY NOIDA
G B NAGAR (U.P.) INDIA

25 NOV 2024

Signature Not Verified
Digitally signed by PARIMAL PIYUSH
Date: 2024.11.25 22:55:12 IST
Reason: AGM(Commercial)
Location: NTPC Limited

PART-I
APPENDIX-I

TARIFF FILING FORMS (THERMAL)

FOR DETERMINATION OF TARIFF

FOR

Tanda Super Thermal Power Station Stage-I

(From 01.04.2024 to 31.03.2029)

Checklist of Main Tariff Forms and other information for tariff filing for Thermal Stations

Form No.	Title of Tariff Filing Forms (Thermal)	Tick
FORM- 1	Summary of Tariff	✓
FORM -1 (I)	Statement showing claimed capital cost	✓
FORM -1 (II)	Statement showing Return on Equity	✓
FORM-2	Plant Characteristics	✓
FORM-3	Normative parameters considered for tariff computations	✓
FORM-3A**	Statement showing O&M Expenses	✓
FORM- 4	Details of Foreign loans	**NA**
FORM- 4A	Details of Foreign Equity	**NA**
FORM-5	Abstract of Admitted Capital Cost for the existing Projects	**NA**
FORM- 6	Financial Package upto COD	**NA**
FORM- 7	Details of Project Specific Loans	**NA**
FORM- 8	Details of Allocation of corporate loans to various projects	✓
FORM-9A	Summary of Statement of Additional Capitalisation claimed during the period	✓
FORM-9##	Statement of Additional Capitalisation after COD	✓
FORM- 10	Financing of Additional Capitalisation	***
FORM- 11	Calculation of Depreciation on original project cost	✓
FORM- 12	Statement of Depreciation	✓
FORM- 13	Calculation of Weighted Average Rate of Interest on Actual Loans	✓
FORM- 14	Draw Down Schedule for Calculation of IDC & Financing Charges	**NA**
FORM- 15	Details of Fuel for Computation of Energy Charges	✓
FORM- 15A**	Details of Seconday Fuel for Computation of Energy Charges	✓
FORM- 15B**	Computation of Energy Charges	✓
FORM- 16	Details of Limestone for Computation of Energy Charge Rate	**NA**
FORM-17***	Details of Capital Spares	***
FORM- 18***	Non-Tariff Income	***
FORM-19***	Details of Water Charges	***
FORM-20***	Details of Statutory Charges	***

PART-I

List of Supporting Forms / documents for tariff filing for Thermal Stations

Form No.	Title of Tariff Filing Forms (Thermal)	Tick
FORM-A	Abstract of Capital Cost Estimates	**NA**
FORM-B	Break-up of Capital Cost for Coal/Lignite based projects	**NA**
FORM-C	Break-up of Capital Cost for Gas/Liquid fuel based Projects	**NA**
FORM-D	Break-up of Construction/Supply/Service packages	**NA**
FORM-E	Details of variables , parameters , optional package etc. for New Project	**NA**
FORM-F	Details of cost over run	**NA**
FORM-G	Details of time over run	**NA**
FORM –H	Statement of Additional Capitalisation during end of the useful life	**NA**
FORM –I***	Details of Assets De-capitalised during the period	***
FORM –J***	Reconciliation of Capitalisation claimed vis-à-vis books of accounts	***
FORM –K***	Statement showing details of items/assets/works claimed under Exclusions	***
FORM-L	Statement of Capital cost	✓
FORM-M	Statement of Capital Woks in Progress	✓
FORM-N	Calculation of Interest on Normative Loan	✓
FORM-O	Calculation of Interest on Working Capital	✓
FORM-P	Incidental Expenditure up to SCOD and up to Actual COD	**NA**
FORM-Q	Expenditure under different packages up to SCOD and up to Actual COD	**NA**
FORM-R	Actual cash expenditure	**NA**
FORM-S	Statement of Liability flow	***
FORM-T	Summary of issues involved in the petition	✓

**** Additional Forms**
Provided yearwise for the period 2024-29
***** Shall be provided at the time of true up**

List of supporting documents for tariff filing for Thermal Stations

S. No.	Information / Document	Tick
1	Certificate of incorporation, Certificate for Commencement of Business, Memorandum of Association, & Articles of Association (For New Station setup by a company making tariff application for the first time to CERC)	NA
2	A. Station wise and Corporate audited Balance Sheet and Profit & Loss Accounts with all the Schedules & annexures on COD of the Station for the new station & for the relevant years.	***
	B. Station wise and Corporate audited Balance Sheet and Profit & Loss Accounts with all the Schedules & annexures for the existing station for relevant years.	
3	Copies of relevant loan Agreements	NA
4	Copies of the approval of Competent Authority for the Capital Cost and Financial package.	NA
5	Copies of the Equity participation agreements and necessary approval for the foreign equity.	NA
6	Copies of the BPSA/PPA with the beneficiaries, if any	NA
7	Detailed note giving reasons of cost and time over run, if applicable.	NA
	List of supporting documents to be submitted:	
	a. Detailed Project Report	
	b. CPM Analysis	
	c. PERT Chart and Bar Chart	
	d. Justification for cost and time Overrun	
8	Generating Company shall submit copy of Cost Audit Report along with cost accounting records, cost details, statements, schedules etc. for the Generating Unit wise /stage wise/Station wise/ and subsequently consolidated at Company level as submitted to the Govt. of India for first two years i.e. 2019-20 and 2020-21 at the time of mid-term true-up in 2021-22 and for balance period of tariff period 2019-24 at the time of final true-up in 2024-25. In case of initial tariff filing the latest available Cost Audit Report should be furnished.	***
9	Any other relevant information, (Please specify)	NA
10	Reconciliation with Balance sheet of any actual additional capitalization and amongst stages of a generating station	***
11	BBMB is maintaining the records as per the relevant applicable Acts. Formats specified herein may not be suitable to the available information with BBMB. BBMB may modify the formats suitably as per available information to them for submission of required information for tariff purpose.	NA

***** Shall be provided at the time of true up**

Summary of Tariff

PART-I
FORM- 1

Name of the Petitioner:	**NTPC Limited**
Name of the Generating Station:	**Tanda Super Thermal Power Station Stage-I**
Place (Region/District/State):	**Northern Region/ Ambedkar Nagar/ Uttar Pradesh**

Amount in Rs. Lakhs

S. No.	Particulars	Unit	Existing 2023-24	2024-25	2025-26	2026-27	2027-28	2028-29
1	2	3	4	5	6	7	8	9
1.1	Depreciation	Rs Lakh	4,475.50	4,067.96	292.61	640.92	806.87	815.48
1.2	Interest on Loan	Rs Lakh	0.00	-	100.36	255.93	278.12	216.08
1.3	Return on Equity	Rs Lakh	7,005.89	7,059.76	7,206.70	7,396.85	7,477.79	7,481.45
1.4	Interest on Working Capital	Rs Lakh	5,658.56	5,888.74	5,845.97	5,866.77	5,880.57	5,893.31
1.5	O&M Expenses	Rs Lakh	22,862.28	21,896.99	22,095.75	22,308.83	22,537.38	22,782.67
1.6	Special Allowance (If applicable)	Rs Lakh	0.00	-	-	-	-	-
1.7	Unrecovered Depreciation	Rs. Lakh	0.00	16.27	0.00	0.00	0.00	0.00
	Total	Rs Lakh	**40,002.23**	**38,929.73**	**35,541.40**	**36,469.31**	**36,980.73**	**37,188.98**
2.1	Landed Fuel Cost of coal as per FSA approved by beneficiaries	Rs/Ton	4,757.05	4595.86				
	(%) of Fuel Quantity	(%)	66.75	67.80				
2.2	Landed Fuel Cost of Imported Coal as per FSA approved by beneficiaries	Rs/Ton	NA					
	(%) of Fuel Quantity	(%)	NA					
2.3	Landed Fuel Cost of coal other than FSA	Rs/Ton	3825.09	3956.19				
	(%) of Fuel Quantity	(%)	21.26	20.90				
2.4	Landed Fuel Cost Imported Coal other than FSA.	Rs/Ton	19,478.31	14220.24				
	(%) of Fuel Quantity	(%)	11.99	11.29				
2.5	Secondary fuel oil cost	Rs/Unit	0.05	0.05	0.05	0.05	0.05	0.05
	Energy Charge Rate ex-bus	Rs/Unit	4.78	5.12	5.12	5.12	5.12	5.12

(Petitioner)

Signature Not Verified

Digitally signed by PARIMAL PIYUSH
Date: 2024.11.25 22:55:12 IST
Reason: AGM(Commercial)
Location: NTPC Limited

PART-I
FORM- 1(I)

Name of the Petitioner:	**NTPC Limited**
Name of the Generating Station:	**Tanda Super Thermal Power Station Stage-I**

Amount in Rs. Lakhs

Statement showing claimed capital cost – (A+B)

S. No.	Particulars	2024-25	2025-26	2026-27	2027-28	2028-29
1	2	3	4	5	6	7
1	Opening Capital Cost	1,24,753.82	1,25,962.32	1,30,023.32	1,32,765.96	1,32,895.96
2	Add: Addition during the year	1,208.50	4,061.00	2,742.64	130.00	-
3	Less: De-capitalisation during the year	-	-	-	-	-
4	Less: Reversal during the year	-	-	-	-	-
5	Add: Discharges during the year	-	-	-	-	-
6	Closing Capital Cost	1,25,962.32	1,30,023.32	1,32,765.96	1,32,895.96	1,32,895.96
7	**Average Capital Cost**	**1,25,358.07**	**1,27,992.82**	**1,31,394.64**	**1,32,830.96**	**1,32,895.96**

Statement showing claimed capital cost eligible for RoE @ normal rate (A)

S. No.	Particulars	2024-25	2025-26	2026-27	2027-28	2028-29
1	2	3	4	5		7
1	Opening Capital Cost	1,24,453.01	1,25,661.51	1,29,472.51	1,32,215.15	1,32,345.15
2	Add: Addition during the year	1,208.50	3,811.00	2,742.64	130.00	-
3	Less: De-capitalisation during the year	-	-	-	-	-
4	Less: Reversal during the year	-	-	-	-	-
5	Add: Discharges during the year	-	-	-	-	-
6	Closing Capital Cost	1,25,661.51	1,29,472.51	1,32,215.15	1,32,345.15	1,32,345.15
7	**Average Capital Cost**	**1,25,057.26**	**1,27,567.01**	**1,30,843.83**	**1,32,280.15**	**1,32,345.15**

PART-I
FORM- 1(I)

Name of the Petitioner:	**NTPC Limited**
Name of the Generating Station:	**Tanda Super Thermal Power Station Stage-I**

Statement showing claimed capital cost eligible for RoE@SBI MCLR+350 bp (B)

S. No.	Particulars	2024-25	2025-26	2026-27	2027-28	2028-29
1	2	3	4	5		7
1	Opening Capital Cost	300.82	300.82	550.82	550.82	550.82
2	Add: Addition during the year	-	250.00	-	-	-
3	Less: De-capitalisation during the year	-	-	-	-	-
4	Less: Reversal during the year	-	-	-	-	-
5	Add: Discharges during the year	-	-	-	-	-
6	Closing Capital Cost	300.82	550.82	550.82	550.82	550.82
7	**Average Capital Cost**	**300.82**	**425.82**	**550.82**	**550.82**	**550.82**

(Petitioner)

Statement showing Return on Equity at Normal Rate

PART-I
FORM- 1(IIA)

Name of the Petitioner	**NTPC Limited**
Name of the Generating Station	**Tanda Super Thermal Power Station Stage-I**

Amount in Rs. Lakhs

S. No.	Particulars	2024-25	2025-26	2026-27	2027-28	2028-29
1	2	3	4	5	6	7
	Return on Equity eligible for RoE @ Normal Rate					
1	Gross Opening Equity (Normal)	37,335.90	37,698.45	38,841.75	39,664.54	39,703.54
2	Less: Adjustment in Opening Equity	-	-	-	-	-
3	Adjustment during the year	-				
4	Net Opening Equity (Normal)	37,335.90	37,698.45	38,841.75	39,664.54	39,703.54
5	Add: Increase in equity due to addition during the year	362.55	1143.30	822.79	39.00	0.00
7	Less: Decrease due to De-capitalisation during the year	0.00	0.00	0.00	0.00	0.00
8	Less: Decrease due to reversal during the year	0.00	0.00	0.00	0.00	0.00
9	Add: Increase due to discharges during the year	0.00	0.00	0.00	0.00	0.00
10	Net closing Equity (Normal)	37,698.45	38,841.75	39,664.54	39,703.54	39,703.54
11	Average Equity (Normal)	37,517.18	38,270.10	39,253.15	39,684.04	39,703.54
	Rate of ROE (%)-Pre Tax	15.50%	15.50%	15.50%	15.50%	15.50%
12	Rate of ROE (%)-Post Tax	18.782%	18.782%	18.782%	18.782%	18.782%
13	**Total ROE**	**7,046.48**	**7,187.89**	**7,372.53**	**7,453.46**	**7,457.12**

(Petitioner)

Statement showing Return on Equity linked to SBI MCLR:

PART-I
FORM- 1(IIB)

Name of the Petitioner:	**NTPC Limited**
Name of the Generating Station:	**Tanda Super Thermal Power Station Stage-I**

Amount in Rs. Lakhs

S. No.	Particulars	2024-25	2025-26	2026-27	2027-28	2028-29
1	2	3	4	5	6	7
Statement showing Return on Equity Eligible@SBI MCLR + 350 basis points						
1	Gross Opening Equity (Normal)	90.25	90.25	165.25	165.25	165.25
2	Less: Adjustment in Opening Equity	0.00	0.00	0.00	0.00	0.00
3	Adjustment during the year	0.00	0.00	0.00	0.00	0.00
4	Net Opening Equity (Normal)	90.25	90.25	165.25	165.25	165.25
5	Add: Increase in equity due to addition during the year	0.00	75.00	0.00	0.00	0.00
7	Less: Decrease due to De-capitalisation during the year	0.00	0.00	0.00	0.00	0.00
8	Less: Decrease due to reversal during the year	0.00	0.00	0.00	0.00	0.00
9	Add: Increase due to discharges during the year	0.00	0.00	0.00	0.00	0.00
10	Net closing Equity (Normal)	90.25	165.25	165.25	165.25	165.25
11	Average Equity (Normal)	90.25	127.75	165.25	165.25	165.25
12	Rate of ROE (%)-Pre Tax	12.15%	12.15%	12.15%	12.15%	12.15%
12A	Rate of ROE (%)-Post Tax	14.72%	14.72%	14.72%	14.72%	14.72%
13	**Total ROE**	**13.29**	**18.81**	**24.33**	**24.33**	**24.33**

(Petitioner)

Signature Not Verified

Digitally signed by PARIMAL PIYUSH
Date: 2024.11.25 22:55:12 IST
Reason: AGM(Commercial)
Location: NTPC Limited

PART-I
FORM-2

Plant Characteristics

Name of the Petitioner	**NTPC Ltd**			
Name of the Generating Station	**Tanda TPS**			
Unit(s)/Block(s)/Parameters	**Unit-I**	**Unit-II**	**Unit-III**	**Unit-IV**
Installed Capacity (MW)	110	110	110	110
Schedule COD as per Investment Approval	21.03.88	11.03.89	28.03.90	20.02.98
Actual COD /Date of Taken Over (as applicable)	14.01.2000			
Pit Head or Non Pit Head	Non Pit Head			
Name of the Boiler Manufacture	BHEL			
Name of Turbine Generator Manufacture	CZECH SKODA			
Main Steams Pressure at Turbine inlet (kg/Cm^2) abs				
Main Steam Temperature at Turbine inlet (^oC)				
Reheat Steam Pressure at Turbine inlet ($kg/Cm^{2)}$				
Reheat Steam Temperature at Turbine inlet (^oC)				
Main Steam flow at Turbine inlet under MCR condition (tons/hr)				
Main Steam flow at Turbine inlet under VWO condition(tons/hr)				
Unit Gross electrical output under MCR /Rated condition (MW)				
Unit Gross electrical output under VWO condition (MW)				
Guaranteed Design Gross Turbine Cycle Heat Rate(kCal/kWh)				
Conditions on which design turbine cycle heat rate guaranteed				
% MCR				
% Makeup Water Consumption				
Design Capacity of Make up Water System				
Design Capacity of Inlet Cooling System				
Design Cooling Water Temperature (^0C)				
Back Pressure				
Steam flow at super heater outlet under BMCR condition(tons/hr)				
Steam Pressure at super heater outlet under				
BMCR condition) ($kg/Cm^{2)}$				
Steam Temperature at super heater outlet under				
BMCR condition (^0C)				
Steam Temperature at Reheater outlet at BMCR condition (^0C)				
Design / Guaranteed Boiler Efficiency (%)				
Design Fuel with and without Blending of domestic/imported coal				
Type of Cooling Tower	Induced Draft Cooling Tower (IDCT)			
Type of cooling system	Closed Cycle			
Type of Boiler Feed Pump	Motor Driven			
Fuel Details				
-Primary Fuel	Coal			
-Secondary Fuel	LDO			
-Alternate Fuels	N/A			
Special Features/Site Specific Features				
Special Technological Features				
Environmental Regulation related features	ESP, DSI (under implementation)			
Any other special features				

					PART-I
					FORM-2
Plant Characteristics					
Name of the Petitioner	**NTPC Ltd**				
Name of the Generating Station	**Tanda TPS**				
Unit(s)/Block(s)/Parameters	**Unit-I**	**Unit-II**	**Unit-III**	**Unit-IV**	
					(Petioner)

Signature Not Verified

Digitally signed by PARIMAL PIYUSH
Date: 2024.11.25 22:55:12 IST
Reason: AGM(Commercial)
Location: NTPC Limited

Normative parameters considered for tariff computations							PART-I FORM-3
Name of the Petitioner:	**NTPC Limited**						
Name of the Generating Station:	**Tanda Super Thermal Power Station Stage-I**						
							(Year Ending March)
Particulars	**Unit**	**Existing 2023-24**	**2024-25**	**2025-26**	**2026-27**	**2027-28**	**2028-29**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Base Rate of Return on Equity at normal rate	%	15.50%	15.50%	15.50%	15.50%	15.50%	15.50%
Rate of Return on Add - cap beyond the original scope of work including additional capitalization due to Change in Law, Force Majeure	%	7.80%	12.15%	12.15%	12.15%	12.15%	12.15%
Effective Tax Rate	%	17.472%	17.472%	17.472%	17.472%	17.472%	17.472%
Target Availability	%	85.00%	85.00%	85.00%	85.00%	85.00%	85.00%
Peak Hours	%	85.00%	85.00%	85.00%	85.00%	85.00%	85.00%
Off-Peak Hours	%	85.00%	85.00%	85.00%	85.00%	85.00%	85.00%
ß- Average Monthly Frequency Response Performance	0-1	It will be provided at the time of truing up					
Auxiliary Energy Consumption	%	11.50%	12.00%	12.00%	12.00%	12.00%	12.00%
Gross Station Heat Rate	kCal/kWh	2750.00	2750.00	2750.00	2750.00	2750.00	2750.00
Specific Fuel Oil Consumption	ml/kWh	0.50	0.50	0.50	0.50	0.50	0.50
Cost of Coal/Lignite for WC	in Days	50	50	50	50	50	50
Cost of Main Secondary Fuel Oil for WC	in Months	2	2	2	2	2	2
Fuel Cost for WC	in Months						
Liquid Fuel Stock for WC	in Months						
O&M Expenses	Rs lakh/MW	46.16	42.52	42.52	42.52	42.52	42.52
Maintenance Spares for WC	% of O&M	20.00%	20.00%	20.00%	20.00%	20.00%	20.00%
Receivables for WC	in Days	45.00	45.00	45.00	45.00	45.00	45.00
Storage capacity of Primary fuel	MT	5 Lakh MT					
SBI 1 Year MCLR plus 350 basis point	%	12.00%	11.90%	11.90%	11.90%	11.90%	11.90%
Blending ratio of domestic coal/imported coal	%	1129.46%	0.00%	0.00%	0.00%	0.00%	0.00%
Norms for consumption of reagent		NA					
Specific Limestone consumption for Wet Limestone FGD							
Specific Limestone consumption for Lime Spray Dryer or Semi-dry FGD							
Specific consumption of sodium bicarbonate							
Specific Limestone consumption for CFBC based generating station							
specific urea consumption of the SNCR							
Specific ammonia consumption of the SCR							
Transit and Handling Losses of coal or lignite, as applicable	%	0.80%	0.80%	0.80%	0.80%	0.80%	0.80%

Petitioner

Signature Not Verified

Digitally signed by PARIMAL PIYUSH
Date: 2024.11.25 22:55:12 IST
Reason: AGM(Commercial)
Location: NTPC Limited

Part-I
FORM-3A
ADDITIONAL FORM

Calculation of O&M Expenses

Name of the Company :	**NTPC Limited**
Name of the Power Station :	**Tanda Super Thermal Power Station Stage-I**

Amount in Rs. Lakhs

S.No.	Particulars	2024-25	2025-26	2026-27	2027-28	2028-29
1	**2**	**3**	**4**	**5**	**6**	**8**
1	**O&M expenses under Reg.35(1)**					
1a	Normative	18,708.80	18,708.80	18,708.80	18,708.80	18,708.80
2	**O&M expenses under Reg.35(6)**					
2a	Water Charges	90.00	90.00	90.00	90.00	90.00
2b	Security expenses	876.93	964.63	1061.09	1167.20	1283.92
2c	Capital Spares*	To be provided at the time of Truing up				
3	O&M expenses-Ash Transportation	2221.26	2332.32	2448.94	2571.39	2699.96
	Total O&M Expenses	**21896.99**	**22095.75**	**22308.83**	**22537.38**	**22782.67**

* Shall be provided at the time of true-up.

Petitioner

FORM-8

Details of Allocation of Corporate Bonds to various projects	
Name of the Company	**NTPC LIMITED**
Name of the Power Station	Tanda Super Thermal Power Station Stage-I
Commercial Operation Date (COD)	**14-01-2000**
Bond-61	
Particulars	
Source of Loan - Bonds Series	**61**
Currency	INR
Amount of Loan sanctioned (In Lakh)	1,07,250.00
Amount of Gross Loan drawn upto COD (In Lakh)	1,07,250.00
Interest Type	Fixed
Fixed Interest Rate, if applicable**	8.10%
Base Rate, if Floating Interest	N/A
Margin, if Floating Interest	N/A
Are there any Caps/Floor	No
If above is yes,specify caps/floor	N/A
Moratorium Period (In Years)	5
Moratorium effective from*	27-05-2016
Repayment Period	Installments Due on 27/05/2021, 27/05/2026 & 27/05/2031
Repayment effective from	27-05-2021
Repayment Frequency	Installments Due on 27/05/2021, 27/05/2026 & 27/05/2031
Repayment Instalment (In Lakh)	Installments 1st - 35,750.00 2nd - 35,750.00 3rd - 35,750.00
Base Exchange Rate	N/A
Door to Door Maturity (In Years)	15
Name of the Projects	**61**
Tanda R& M	400.00

-

*Moratorium period has been taken as the period from Deemed Date of Allotment till the date of first Redemption.
** Excluding Survillience fees of 0.03%

FORM-8

Details of Allocation of Corporate Bonds to various projects		
Name of the Company	**NTPC LIMITED**	
Name of the Power Station	Tanda Super Thermal Power Station Stage-I	
Commercial Operation Date (COD)	**14-01-2000**	
		(Amount in Rs. Lakh)
Bond-72		
Particulars		
Source of Loan - Bonds Series	**72**	
Currency	INR	
Amount of Loan sanctioned (In Lakh)		4,00,000
Amount of Gross Loan drawn upto COD (In L		4,00,000
Interest Type	Fixed	
Fixed Interest Rate, if applicable	5.45%	
Base Rate, if Floating Interest	N/A	
Margin, if Floating Interest	N/A	
Are there any Caps/Floor	No	
If above is yes,specify caps/floor	N/A	
Moratorium Period (In Years)	5	
Moratorium effective from*	15-10-2020	
Repayment Period	Bullet Repayment	
Repayment effective from	15-10-2025	
Repayment Frequency	Bullet Repayment	
Repayment Instalment (In Lakh)		4,00,000
Base Exchange Rate	N/A	
Door to Door Maturity (In Years)	5	
Name of the Projects	**72**	
TANDA R&M		1,500.00

-

Statement Giving Details of Project Financed through a Combination of loan Form 8 TRANCHE NO		
BP NO 5050000382	**T00001**	**D0005**
Unsecured Loan From SBBJ-II		
Source of Loan :	**SBBJ-II**	
Currency :	INR	
Amount of Loan :	5,00,00,00,000	
Total Drawn amount :	2,00,00,00,000	
Date of Drawal:	29.06.2018	
Interest Type :	Floating	
Fixed Interest Rate :	----------	
Base Rate, If Floating Interest	8.25%	
Margin, If Floating Interest :	0.00%	
Are there any Caps/ Floor :	Y/N	
Frequency of Intt. Payment	Monthly	
If Above is yes, specify Caps/ Floor :		
Moratorium Period :	5 Years	
Moratorium effective from :	29.06.2018	
Repayment Period (Inc Moratorium) :	15 Years	
Repayment Frequency :	10 Yearly Installments	
Repayment Type :	AVG	
First Repayment Date :	14.03.2020	
Base Exchange Rate :	RUPEE	
Date of Base Exchange Rate :	N.A.	
Project Code	**Project Name**	**Amount**
	SINGRAULI R&M	1,00,00,00,000
	Tanda R&M	1,00,00,00,000
Total Allocated Amount		**2,00,00,00,000.00**

Signature Not Verified

Digitally signed by PARIMAL PIYUSH
Date: 2024.11.25 22:55:12 IST
Reason: AGM(Commercial)
Location: NTPC Limited

Statement Giving Details of Project Financed through a Combination of loan		
Form 8 TRANCHE NO		
BP NO 5050000571	**T00001**	**D00004**
Unsecured Loan From Punjab National Bank-III		
Source of Loan :	**Punjab National Bank-III**	
Currency :	INR	
Amount of Loan :	20,00,00,00,000	
Total Drawn amount :	5,00,00,00,000	
Date of Drawl	21.08.2018	
Interest Type :	Floating	
Fixed Interest Rate :		
Base Rate, If Floating Interest	8.05%	
Margin, If Floating Interest :	0.00%	
Are there any Caps/ Floor :	Y/N	
Frequency of Intt. Payment	MONTHLY	
If Above is yes, specify Caps/ Floor :		
Moratorium Period :	3 Years	
Moratorium effective from :	21.08.2018	
Repayment Period (Inc Moratorium) :	12 Years	
Repayment Frequency :	9 Yearly Instalment	
Repayment Type :	AVG	
First Repayment Date :	01.02.2022	
Base Exchange Rate :	RUPEE	
Date of Base Exchange Rate :	N.A.	
Project Code	Project Name	Amount
	SINGRAULI R&M	1,00,00,00,000.00
	KORBA R&M	1,00,00,00,000.00
	RAMAGUNDAM R&M	1,00,00,00,000.00
	VINDHYACHAL R&M	1,00,00,00,000.00
	TANDA R&M	1,00,00,00,000.00
Total Allocated Amount		**5,00,00,00,000.00**

PART-I
FORM- 9A
ADDITIONAL FORM

Year wise Statement of Additional Capitalisation after COD

Name of the Petitioner	NTPC Limited
Name of the Generating Station	Tanda Super Thermal Power Station Stage-I
COD	14-01-2000
For Financial Year	2024-29 (Summary)

Amount in Rs Lakh

Sl. No.	Head of Work /Equipment	ACE Claimed (Projected)					Justification	Admitted Cost by the Commission, if any
		2024-25	2025-26	2026-27	2027-28	2028-29		
1	2	3	4	5	6	7	8	9
A.	**Works eligble for RoE at Normal Rate**							
1	Upgradation of SG-DCS OF U#3&4		223	246			Pl. refer Form-9 of respective FYs.	
2	Upgradation of TG-DCS OF U#3&4		300	325				
3	Upgradation of MAXDNA-DCS OF U#3&4		350	400				
4	Upgradation of Fire detection and protection system Main Plant		100	100				
5	Upgradation of DM Plant PLC Controllers		60					
6	Upgradation of Mechanical Type Positioners		56	57				
7	Replacement of Main Ejector with Vacuum pump		400	400				
8	Replacement of switchyard Isolators Stage-I			64				
9	Upgradation of HT/LT Switchgear			143.50	-			
10	Upgradation of Generator & Busbar Protection System			159.84	130.00			
11	Replacement of CRD -Retrofit of Energy chain for Trippers & Plough Feeder CHP Stage-I			196				
12	PLC Upgradation of CHP stage 1		68.20					
13	Stage 1 Ash Slurry line pipe replacement in culverts		75					
14	Stage-I Fire Hyd and Spray Pumps Replacement			33				

PART-I
FORM- 9A
ADDITIONAL FORM

Year wise Statement of Additional Capitalisation after COD

Name of the Petitioner	**NTPC Limited**
Name of the Generating Station	**Tanda Super Thermal Power Station Stage-I**
COD	**14-01-2000**
For Financial Year	**2024-29 (Summary)**

Amount in Rs Lakh

Sl. No.	Head of Work /Equipment	ACE Claimed (Projected)					Justification	Admitted Cost by the Commission, if any
		2024-25	2025-26	2026-27	2027-28	2028-29		
15	Stage-1 Clarifiers Replacement		99	99			**Pl. refer Form-9 of respective FYs.**	
16	Repair/strengthening work of all RCC structures of Stage I buildings as per RLA recommendations		2,080	520				
17	Upgradation against Obsolescence of HMI of M/s BHEL with cyber security features in NTPC Tanda	881.50						
18	Supply, erection and commissioning of fire detection and fire protection system for stacker re-claimer and coal conveyor	124.00						
19	Upgradation of SG (Ovation) DCS controllers & HMI, Unit-2 Stage-I	203.00						
Total additional capitalization claimed with RoE at Normal Rate (A)		**1,208.50**	**3,811.00**	**2,742.64**	**130.00**	**-**		
B.	**Works eligble for Return on Equity linked to SBI MCLR:**							
1	Augmentation of CCTV System		250.00				NA	
Total additional capitalization claimed with RoE at Wtd. Average Rate of Interest (B)		**-**	**250.000**	**-**	**-**	**-**		
Total Add. Cap. Claimed (A+B)		**1,208.500**	**4,061.000**	**2,742.640**	**130.000**	**-**		

(Petitioner)

Signature Not Verified

Digitally signed by PARIMAL PIYUSH
Date: 2024.11.25 22:55:12 IST
Reason: AGM(Commercial)
Location: NTPC Limited

PART-I
FORM- 9

Year wise Statement of Additional Capitalisation after COD

Name of the Petitioner	**NTPC Limited**
Name of the Generating Station	**Tanda Super Thermal Power Station Stage-I**
COD	**14-01-2000**
For Financial Year	**2024-25**

Amount in Rs Lakh

Sl. No.	Head of Work /Equipment	ACE Claimed (Projected)						Regulations under which claimed	Justification	Admitted Cost by the Commission, if any
		Accrual basis as per Ind AS	Ind AS adjustment	Accrual basis as per IGAAP	Un-discharged Liability included in col. 3	Cash basis	IDC included in col. 3			
1	2	3	3A	3B=3+3A	4	5= (3-4)	6	7	8	9
A.	**Works eligible for RoE at Normal Rate**									
1	Upgradation of HMI for cyber security features	881.50	-	881.50	-	881.50	-	25 (2) (c) & 26 (1) (b)	CEA under the provision of Regulation (10) of the Central Electricity Authority (Technical Standards for Connectivity to the Grid) (Amendment) Regulations, 2019 issued CEA (Cyber Security in Power Sector) Guidelines, 2021 (Attached as **Annexure-R/1 Colly**). The CEA guidelines, 2021 require for compliance of following salient points wrt Cyber Security in Power Sector: i) Phasing out of legacy systems ii) Ensuring security hardening with additional controls in consultation with the OEM iii) Maintaining system logs at least for 6 months duration. Further, Ministry of Electronics and Information Technology (MeitY), Govt of India vide its order No- No. 20(3)/2022-CERT-In GoI dated 28.04.2022 issued Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 (Attached as **Annexure-R/2 Colly**) which inter alia provides: *"All service providers, intermediaries, data centres, body corporate and Government organisations shall mandatorily enable logs of all their ICT systems and maintain them securely for a rolling period of 180 days and the same shall be maintained within the Indian jurisdiction. These should be provided to CERT-In along with reporting of any incident or when ordered / directed by CERT-In"* The HMI system installed at the instant stations were based on Windows XP for which no support from OEM, M/s Microsoft is available due to declaration of obsolescence and End of Life (EOL) of Windows XP (EOL April 2014) (Attached as **Annexure-R/3 Colly**). Accordingly, in compliance of CEA (Cyber Security in Power Sector) Guidelines, 2021 and direction from GoI order dated 28.04.2022 the HMI system needs to be upgraded for ensuring safe and reliable operation of the Station. Therefore, it is humbly submitted that Hon'ble Commission may be pleased to allow the replacement of HMI system under Regulations 25 (2) (c) read with 26 (1) (b)	NA

PART-I
FORM- 9

Year wise Statement of Additional Capitalisation after COD

Name of the Petitioner	**NTPC Limited**
Name of the Generating Station	**Tanda Super Thermal Power Station Stage-I**
COD	**14-01-2000**
For Financial Year	**2024-25**

Amount in Rs Lakh

Sl. No.	Head of Work /Equipment	ACE Claimed (Projected)						Regulations under which claimed	Justification	Admitted Cost by the Commission, if any
		Accrual basis as per Ind AS	Ind AS adjustment	Accrual basis as per IGAAP	Un-discharged Liability included in col. 3	Cash basis	IDC included in col. 3			
1	2	3	3A	3B=3+3A	4	5= (3-4)	6	7	8	9
2	Fire detection and protection system for CHP area	124.00	-	124.00	-	124.00	-	25 (2) (c) & 26 (1) (b)	Fire Fighting System for CHP area is required to prevent any damage in case of fire, as existence of coal in CHP area makes it vulnerable to fire hazard. As per CEA (Technical Standards for Construction of Electrical Plants and Electric Lines) Regulations. 2022 (relevant pages attached as **Annexure-R/4**), automatic medium velocity water spray system are to be provided for area related to Coal conveyors, transfer points, crusher houses etc. Further, Hon'ble Commission vide its order dated 17.04.2024 in Petition no-445/GT/2020 allowed the work of Fire Fighting System for CHP area at a cost of Rs 224.88 Lakh. However, the work could not be completed in totality by the end of Tariff Period 2019-24. As of now only a fraction of work is yet to be done which is expected to be completed by the end of FY 2024-25. In view of the above, it is humbly submitted that Hon'ble Commission may be pleased to allow the work of Fire Detection and Protection System for CHP area at the instant station	NA
3	Upgradation of SG (Ovation) DCS controllers	203.00	-	203.00	-	203.00	-	25 (2) (c) & 26 (1) (b)	SG (Ovation) Digital Control System (DCS) is installed at the instant station for control, monitoring and protection of the boiler as a separate DCS package by OEM M/s Emerson. M/s Emerson has refused to provide support for the existing system which has got obsolete. In recent third-party network security audit report submitted by M/s Grand Thornton, it was recommended that existing DCS needs to be upgraded immediately, to mitigate critical cyber security threats. The Audit Report by M/s Grand Thornton is attached as **Annexure-R/5**. Also, SG (Ovation) DCS is based on Windows XP operating system, for which support from M/s Microsoft has been withdrawn the End of Life declaration by M/s Microsoft is attached as **Annexure-R/3 Colly**. Further, requirement of upgradation of SG DCS control system is mandated as per the provisions of CEA (Cyber Security in Power Sector) Guidelines, 2021 (Attached as **Annexure-R/1 Colly**) and the provisions of directions from Govt of India in respect of cyber security of important installations including power plants issued vide Order No- 20(3)/2022-CERT-In GoI dated 28.04.2022 (attached as **Annexure-R2 Colly**.) In view of the above, it is humbly submitted that Hon'ble Commission may be pleased to allow the replacement of the work of Upgradation of SG (Ovation) DCS controllers	NA
Sub Total-A		1,208.50	-	1,208.50	-	1,208.50	-			

PART-I
FORM- 9

Year wise Statement of Additional Capitalisation after COD

Name of the Petitioner	NTPC Limited
Name of the Generating Station	Tanda Super Thermal Power Station Stage-I
COD	14-01-2000
For Financial Year	2024-25

Amount in Rs Lakh

Sl. No.	Head of Work /Equipment	ACE Claimed (Projected)						Regulations under which claimed	Justification	Admitted Cost by the Commission, if any
		Accrual basis as per Ind AS	Ind AS adjustment	Accrual basis as per IGAAP	Un-discharged Liability included in col. 3	Cash basis	IDC included in col. 3			
1	2	3	3A	3B=3+3A	4	5= (3-4)	6	7	8	9
B.	Works eligible for Return on Equity linked to SBI MCLR:									
1	NA	-		-		-		NA	NA	NA
Sub Total-B						-				
Total Add. Cap.		1,208.50	-	1,208.50	-	1,208.50				

(Petitioner)

PART-I
FORM- 9

Year wise Statement of Additional Capitalisation after COD

Name of the Petitioner	**NTPC Limited**
Name of the Generating Station	**Tanda Super Thermal Power Station Stage-I**
COD	**14-01-2000**
For Financial Year	**2025-26**

Amount in Rs Lakh

Sl. No.	Head of Work /Equipment	ACE Claimed (Projected)						Regulations under which claimed	Justification	Admitted Cost by the Commission, if any
		Accrual basis as per Ind AS	Ind AS Adjustment	Accrual basis as per IGAAP	Un-discharged Liability included in col. 3	Cash basis	IDC included in col. 3			
1	2	3	3A	3B=3+3A	4	5= (3-4)	6	7	8	9
A.	**Works eligible for RoE at Normal Rate**									
1	Upgradation of SG-DCS OF U#3&4	223.00		223.00		223.00		25(2)(c) read with 102	Detailed Justification provided at Sl No-A-3 of Form-9 24-25.	NA
2	Upgradation of TG-DCS OF U#3&4	300.00		300.00		300.00		25(2) (c) 26 (1) (b) read with 102	TG Digital Control System (DCS) is installed at the instant station for control, monitoring and protection of the 110 MW Skoda design Turbines (SKODA design & BHEL Manufactured) as a separate DCS package. The existing TG DCS is based on redundant CPU 414-H and ET200M I/O peripherals. The above has got obsolete and no further support is available from the OEM. It is further submitted that the existing system is not compliant with requirements of cyber security according to the IEC 62443 standard. The obsolescence certificate from OEM is attached as **Annexure-R/6**. Further, the upgradation of TG DCS control system is in mandated in compliance of the requirement as per the provisions of CEA (Cyber Security in Power Sector) Guidelines, 2021 (Attached as **Annexure-R/1 Colly**) and as per the provisions of directions from Govt of India in respect of cyber security of important installations including power plants issued vide its order No- 20(3)/2022-CERT-In GoI dated 28.04.2022 (attached as **Annexure-R2 Colly**.) In view of the above, it is humbly submitted that Hon'ble Commission may be pleased to allow the replacement of the work of Upgradation of TG DCS system.	NA
3	Upgradation of MAXDNA-DCS OF U#3&4	350.00		350.00		350.00		25(2) (c) 26 (1) (b) read with 102	The existing MAXDNA DCS is used for Automatic Closed Loop Control Systems such as control of Drum level, Furnace draft, Fuel firing , Airflow etc. MAXDNA DCS was supplied by M/s BHEL which has now got obsolete and no support is available from M/s BHEL. The obsolescence certificate is attached as **Annexure-R/7**. Further, the upgradation of TG DCS control system is in mandated in compliance of the requirement as per the provisions of CEA (Cyber Security in Power Sector) Guidelines, 2021 (Attached as **Annexure-R/1 Colly**) and the provisions of directions from Govt of India in respect of cyber security of important installations including power plants issued vide its order No- 20(3)/2022-CERT-In GoI dated 28.04.2022 (attached as **Annexure-R2 Colly.**) In view of the above, it is humbly submitted that Hon'ble Commission may be pleased to allow the replacement of the work of Upgradation of MAXDNA DCS system.	NA

PART-I
FORM- 9

Year wise Statement of Additional Capitalisation after COD

Name of the Petitioner	**NTPC Limited**
Name of the Generating Station	**Tanda Super Thermal Power Station Stage-I**
COD	**14-01-2000**
For Financial Year	**2025-26**

Amount in Rs Lakh

Sl. No.	Head of Work /Equipment	ACE Claimed (Projected)						Regulations under which claimed	Justification	Admitted Cost by the Commission, if any
		Accrual basis as per Ind AS	Ind AS Adjustment	Accrual basis as per IGAAP	Un-discharged Liability included in col. 3	Cash basis	IDC included in col. 3			
4	Upgradation of Fire detection and protection system Main Plant	100.00		100.00		100.00		25(2) (c) 26 (1) (b) read with 102	For Fire detection and protection, control panels are installed in the control room. The system works based on automatic detection of smoke and fire in the respective locations of the plant. According to feedback from smoke & fire detectors, the requisite action such as initiation of fire alarm and operation of hydrant, sprinkler etc is activated. The existing fire detection and protection system controllers and field instruments has got obsolete. Due to non availability of required spare part and support from OEM the healthiness of the fire safety system is at risk. Therefore, their upgradation is mandatory to ensure that fire fighting system is healthy and uptodate. The obsolescence certificate is attached as **Annexure-R/8.** Further CEA (Technical Standards for Construction of Electrical Plants and Electric Lines) Regulations, 2022 requires availability of comprehensive fire protection system at place to ensure safety of the plant. The relevant extract is produced as under: *"(5) Fire detection, alarm and protection system.— (i) A comprehensive fire detection, alarm as well as fire protection system shall be installed for the Station in conformity with relevant Indian Standard. (ii) Automatic fire detection and alarm system shall be intelligent and addressable type and shall be provided to facilitate detection of fire at the incipient stage and give warning to the firefighting staff. "* In view of the above, it is humbly submitted that Hon'ble Commission may be pleased to allow the said work under Regulations 25 (2) (c) with power to relax.	NA

PART-I
FORM- 9

Year wise Statement of Additional Capitalisation after COD

Name of the Petitioner	**NTPC Limited**
Name of the Generating Station	**Tanda Super Thermal Power Station Stage-I**
COD	**14-01-2000**
For Financial Year	**2025-26**

Amount in Rs Lakh

Sl. No.	Head of Work /Equipment	ACE Claimed (Projected)						Regulations under which claimed	Justification	Admitted Cost by the Commission, if any
		Accrual basis as per Ind AS	Ind AS Adjustment	Accrual basis as per IGAAP	Un-discharged Liability included in col. 3	Cash basis	IDC included in col. 3			
5	Upgradation of DM Plant PLC Controllers	60.00		60.00		60.00		25(2) (c) 26 (1) (b) read with 102	The existing Schneider make PLC systems were installed for monitoring, control & operation of DM plant at the instant station. These PLC systems were based on Schneider make Quantum PLC Controller. OEM M/s Schneider has declared them obsolete and discontinued support. The obsolescence letter fromOEM, M/s Schneider is attached as **Annexure-R/9 Colly.** Due to this, it is very difficult to maintain the control system healthy for ensuring safe and reliable operation of the DM Plant at the instant station. Further, CEA issued CEA (Cyber Security in Power Sector) Guidelines, 2021 (**Attached as Annexure-R/3**) in compliance of Govt of India policy for cyber security under Indian Computer Emergency Response Team (CERT_In). These guidelines require mandatory Compliance by all Responsible Entities. The scope under "Control Systems for System Operation and Operation Management" inter alia covers " Power Plant Control Systems". The CEA Guidelines (2021) for Cyber Security in the Power Sector mandates: *(i) Phasing out legacy systems,* *(ii) Hardening existing systems with additional security controls in consultation with the OEM, and* *(iii) Maintaining system logs for a minimum of six months.* Therefore, the upgradation of existing PLC systems for DM plant at the instant station is required due to its obsolescence and in compliance of CEA (Cyber Security in Power Sector) Guidelines, 2021 for ensuring safe and reliable operation of the Station. In view of the above, it is humbly submitted that Hon'ble Commission may be pleased to allow the said work under Regulations 25 (2) (c) with power to relax.	NA
6	Upgradation of Mechanical Type Positioners of Draft System	56.00		56.00		56.00		25(2)(c) read with 102	The resolution/ precision in the existing actuator is +/- 2.5%, so fine control of PA header pressure & furnace pressure control loop is difficult. Sometimes these control loops get disturbed especially during frequent Ramp up & Ramp Down of unit load to meet the generation schedule provided to the station from grid controller. Fine control of PA fan blade pitch & IGV of ID Fan is required for smooth control of PA header pressure and furnace draft. The existing IGV & Blade pitch actuators for controlling the furnace draft and PA header pressure were installed at the time of commissioning of the Unit. They have become obsolete as OEM ILK has discontinued support for them. The list of actuators for whose M/s ILK has discontinued the support is attached as **Annexure-R/10.** The role of these actuators is very critical for maintaining requisite air flow in proportionate with fuel input into the boiler for ensuring complete combustion and avoid any residual unburnt fuel inside furnace which may cause unsafe operation of boiler. In view of criticality of role of these actuators and the fact that OEM has discontinued their support for them, they need to be upgraded to ensure efficient & reliable operation of the Plant. In view of the above, it is humbly submitted that Hon'ble Commission may be pleased to allow the said work under Regulations 25 (2) (c) read with 102.	NA

PART-I
FORM- 9

Year wise Statement of Additional Capitalisation after COD

Name of the Petitioner	NTPC Limited
Name of the Generating Station	Tanda Super Thermal Power Station Stage-I
COD	14-01-2000
For Financial Year	2025-26

Amount in Rs Lakh

Sl. No.	Head of Work /Equipment	ACE Claimed (Projected)						Regulations under which claimed	Justification	Admitted Cost by the Commission, if any
		Accrual basis as per Ind AS	Ind AS Adjustment	Accrual basis as per IGAAP	Un-discharged Liability included in col. 3	Cash basis	IDC included in col. 3			
7	Replacement of Main Ejector with Vacuum pump	400.00		400.00		400.00		25(2)(c) read with 102	At instant station condenser vacuum is maintained by two sets of ejectors, one is starting ejectors used during unit start up and other is main ejector which is used to maintain condenser vacuum during normal operation. They work on ejector principle wherein steam is used as drive force to create vacuum inside the condensers. The steam for working of ejectors is taken from Aux PRDS system of the unit. Therefore, start up activity at TG side can only be started after charging of Aux PRDS when certain pressure is build up inside boiler. The existing ejector system is hardly in use in any of the latest plants. Support for the upkeep of the existing ejectors from OEM M/s BHEL has not there. Further, during unit start up when starting ejector is in service, the working steam is dumped to atmosphere causing enormous noise in the surroundings and loss of DM water. Tanda Stage-I being not pit head plant, frequent start up of all four Units is done to meet the beneficiary schedule. Considering the obsolescence of the ejector system and support from the OEM not being available and limitations of the ejector system during unit start up necessitates the replacement of existing steam ejectors with vacuum pump based system. Accordingly, same needs to be replaced with vacuum pump based system. In view of the above it is humbly submitted that Hon'ble Commission may be pleased to allow the work of Replacement of Ejector System with Vacuum pump.	NA

PART-I
FORM- 9

Year wise Statement of Additional Capitalisation after COD

Name of the Petitioner	**NTPC Limited**
Name of the Generating Station	**Tanda Super Thermal Power Station Stage-I**
COD	**14-01-2000**
For Financial Year	**2025-26**

Amount in Rs Lakh

Sl. No.	Head of Work /Equipment	ACE Claimed (Projected)						Regulations under which claimed	Justification	Admitted Cost by the Commission, if any
		Accrual basis as per Ind AS	Ind AS Adjustment	Accrual basis as per IGAAP	Un-discharged Liability included in col. 3	Cash basis	IDC included in col. 3			
8	Upgradation of CHP PLC Controllers	68.20		68.20		68.20		25(2) (c) 26 (1) (b) read with 102	The existing Schneider make PLC systems were installed for monitoring, control & operation of CHP at the instant station. These PLC systems were based on Schneider make Modicon Quantum PLC Controller. OEM M/s Schneider has declared them obsolete and discontinued their support. The obsolescence letter fromOEM, M/s Schneider is attached as **Annexure-R/9 Colly.** Due to this, it is very difficult to maintain the control system healthy for ensuring safe and reliable operation of the CHP. Further, CEA issued CEA (Cyber Security in Power Sector) Guidelines, 2021 (**Attached as Annexure-R/1 Colly**) in compliance of Govt of India policy for cyber security under Indian Computer Emergency Response Team (CERT_In). These guidelines require mandatory Compliance by all Responsible Entities. The scope under "Control Systems for System Operation and Operation Management" inter alia covers " Power Plant Control Systems". The CEA Guidelines (2021) for Cyber Security in the Power Sector mandates *(i) Phasing out legacy systems,* *(ii) Hardening existing systems with additional security controls in consultation with the OEM, and* *(iii) Maintaining system logs for a minimum of six months.* Therefore, the upgradation of existing PLC systems for CHP at the instant station is required due to its obsolescence and in compliance of CEA (Cyber Security in Power Sector) Guidelines, 2021 for ensuring safe and reliable operation of the Station. In view of the above, it is humbly submitted that Hon'ble Commission may be pleased to allow the said work under Regulations 25 (2) (c) read with Regulation 26 (1) (b).	NA
9	Stage 1 ash slurry line pipe replacement in culverts	75.00		75.00		75.00		25(2)(c) read with 102	Ash slurry pipes are used to dispose wet ash slurry from Ash slurry pit situated at Ash Handling Plant inside plant to Ash dyke. On the way from Ash Handling Plant to Ash Dyke, the ash slurry pipes pass through roads, culverts etc. The current ash slurry pipes are made of MS Pipes which are getting frequently eroded due to very corrosive nature of ash being pumped through them. The proposed work is to replace the MS make ash slurry pipes with cast basalt pipes which are highly resistant to abrasion and chemicals. This will help to reduced downtime of existing Ash slurry pipelines and also cut down maintenance cost of frequent rotation requirement and replacement of pipes. The major properties of Cast Basalt pipes is attached as **Annexure-R 11.** In view of the above it is humbly submitted that Hon'ble Commission may be pleased to allow the work of replacement of MS pipe with Cast basalt pipe .	NA

Signature Not Verified

Digitally signed by PARIMAL PIYUSH
Date: 2024.11.25 22:55:12 IST
Reason: AGM(Commercial)
Location: NTPC Limited

PART-I
FORM- 9

Year wise Statement of Additional Capitalisation after COD

Name of the Petitioner	**NTPC Limited**
Name of the Generating Station	**Tanda Super Thermal Power Station Stage-I**
COD	**14-01-2000**
For Financial Year	**2025-26**

Amount in Rs Lakh

Sl. No.	Head of Work /Equipment	ACE Claimed (Projected)						Regulations under which claimed	Justification	Admitted Cost by the Commission, if any
		Accrual basis as per Ind AS	Ind AS Adjustment	Accrual basis as per IGAAP	Un-discharged Liability included in col. 3	Cash basis	IDC included in col. 3			
10	Clarifiers replacement Stage-1	98.80		98.80		98.80		25(2) (c) & 26 (1) (d) read with 102	Clarifier-A civil structure has been critically corroded and very prone to collapse. Clarifier-B has faced such incidence in past. As recent residual life assessment of Stage I buildings & other Civil Structures by third Party M/s NCCBM it was recommended that the residual life of the structure has ended and needed strengthening. The clarifiers are used for treatment raw water and hence and necessary to ensure supply of required water for making of clarified water and DM water which is must to run the Units. The excerpts of the report by M/s NCCBM is attached as **Annexure-R12**. Accordingly, to ensure safety of plant and personnel same need to be replaced. In view of the above it is humbly submitted that Hon'ble Commission may be pleased to allow the work of replacement of Stage-1 Clarifiers.	NA
11	Repair/strengthening work of all RCC structures of Stage I buildings	2080.00		2,080.00		2,080.00		25(2) (c) & 26 (1) (d) read with 102	As per recommendations of residual life assessment of Stage I buildings by M/s NCCBM the residual life of the structure has ended and needed strengthening. These are not only to ensure availability of the plant but also is important from the perspective of the safety of the plant & personnel. Accordingly proposed expenditure to be carried out for ensuring structural soundness of the Stage-I buildings. The excerpts of the report by M/s NCCBM is attached as **Annexure-R13**. In view of the above it is humbly submitted that Hon'ble Commission may be pleased to allow the work of repair/strengthening work of all RCC structures of Stage I buildings	NA
Sub Total-A		**3811.00**	**0.00**	**3811.00**	**0.00**	**3811.00**	**0.00**			

PART-I
FORM- 9

Year wise Statement of Additional Capitalisation after COD

Name of the Petitioner	**NTPC Limited**
Name of the Generating Station	**Tanda Super Thermal Power Station Stage-I**
COD	**14-01-2000**
For Financial Year	**2025-26**

Amount in Rs Lakh

Sl. No.	Head of Work /Equipment	ACE Claimed (Projected)						Regulations under which claimed	Justification	Admitted Cost by the Commission, if any
		Accrual basis as per Ind AS	Ind AS Adjustment	Accrual basis as per IGAAP	Un-discharged Liability included in col. 3	Cash basis	IDC included in col. 3			
B.	**Works eligible for Return on Equity linked to SBI MCLR:**									
1	Augmentation of CCTV System	250.00		250.00		250.00		26 (1) (d) & 26 (1) (b)	It is submitted that a safety advisory mandating comprehensive monitoring of overhauling work and immediate action to address pulverized fuel leakage was issued by the Central Electricity Authority (CEA) on May 23, 2022 (**attached as Annexure-R/14**).To comply with these directives, comprehensive plant process monitoring at various locations within the facility has become essential. Further it is submitted that given the extensive nature of overhauling work and unpredictable occurrence of potential leakages, maintaining thorough physical surveillance is not feasible. Therefore, centralized round-the-clock CCTV monitoring of overhauling activities and critical vulnerable areas within the main plant and the Coal Handling Plant (CHP) area is proposed for implementation. In light of this, the Hon'ble Commission is respectfully requested to allow this under Regulation 26(1)(b) and 26(1)(d) of the Tariff Regulations 2024.	NA
Sub Total-B		**250.00**	**-**	**250.00**	**-**	**250.00**	**-**	**26 (1) (d) & 26 (1) (b)**		
Total Add. Cap. Claimed		**4,061.00**	**-**	**4,061.00**	**-**	**4,061.00**				

(Petitioner)

Signature Not Verified

Digitally signed by PARIMAL PIYUSH
Date: 2024.11.25 22:55:12 IST
Reason: AGM(Commercial)
Location: NTPC Limited

PART-I
FORM- 9

Year wise Statement of Additional Capitalisation after COD

Name of the Petitioner	NTPC Limited
Name of the Generating Station	Tanda Super Thermal Power Station Stage-I
COD	14-01-2000
For Financial Year	2026-27

Amount in Rs Lakh

Sl. No.	Head of Work /Equipment	ACE Claimed (Projected)						Regulations under which claimed	Justification	Admitted Cost by the Commission, if any
		Accrual basis as per Ind AS	Ind AS Adjustment	Accrual basis as per IGAAP	Un-discharged Liability included in col. 3	Cash basis	IDC included in col. 3			
1	2	3	3A	3B=3+3A	4	5= (3-4)	6	7	8	9
A.	Works eligible for RoE at Normal Rate									
1	Upgradation of SG-DCS OF U#3&4	246.00		246.00		246.00		25(2)(c) read with 102	Detailed Justification provided at Sl No-A-3 of Form-9 24-25.	NA
2	Upgradation of TG-DCS OF U#3&4	325.00		325.00		325.00		25(2)(c) read with 102	Detailed Justification provided at Sl No-A-2 of Form-9 25-26.	NA
3	Upgradation of MAXDNA-DCS OF U#3&4	400.00		400.00		400.00		25(2)(c) read with 102	Detailed Justification provided at Sl No-A-3 of Form-9 25-26.	NA
4	Upgradation of Fire detection and protection system Main Plant	100.00		100.00		100.00		25(2)(c) read with 102	Detailed Justification provided at Sl No-A-4 of Form-9 25-26.	NA
5	Upgradation of Mechanical Type Positioners	57.00		57.00		57.00		25(2)(c) read with 102	Detailed Justification provided at Sl No-A-6 of Form-9 25-26.	NA
6	Replacement of Ejector System with Vacuum pumps	400.00		400.00		400.00		25(2)(c) read with 102	Detailed Justification provided at Sl No-A-8 of Form-9 25-26.	NA
7	Replacement of switchyard Isolators Stage-I	64.00		64.00		64.00		25(2)(c) read with 102	Isolators of 220kV switchyard are more than 25 years old and out lived their life. The existing 220 KV switchyard not only cater to export of power from Stage-I to load centres but also acts as interchange of power during stage-I shutdown to ensure power flow. Therefore, to cater to the requirement of power flow, all the elements of switchyard including isolators need to be kept healthy. The existing isolators are old and obsolete and no support is available from the OEM. In view of the above it is humbly submitted that Hon'ble Commission may be pleased to allow the work of Replacement of switchyard Isolators Stage-I	NA
8	Upgradation of HT/LT Switchgear	143.50		143.50		143.50		25(2)(c) read with 102	The existing circuit breakers in LT & HT switchgear is of Minimum Oil Circuit Breaker (MOCB) type which are currently not being used for such use. The breaker is key element for switchgears as main switching device. Currently, vacuum circuit breakers are used for low, medium and high voltage switchgears. The MOCB breakers have become obsolete and support from OEM is not available. Therefore, upgradation of existing HT/LT switchgear is become necessary by replacing the MOCB circuit breakers with Vacuum breakers. In view of the above it is humbly submitted that Hon'ble Commission may be pleased to allow the work of Replacement of switchyard Isolators Stage-I	NA

PART-I
FORM- 9

Year wise Statement of Additional Capitalisation after COD

Name of the Petitioner	**NTPC Limited**
Name of the Generating Station	**Tanda Super Thermal Power Station Stage-I**
COD	**14-01-2000**
For Financial Year	**2026-27**

9	Upgradation of Generator & Busbar Protection System	159.84		159.84		159.84		25(2)(c) read with 102	The existing Generator protection of Unit-2 & 4 and bus bar protection relays are electromechanical type supplied by M/s ABB Ltd. These electromechanical type of relays have become obsolete and no further support is available for them. Due to technological obsolescence and the need to improve reliability, the complete GRP panel replacement for Units 2 and 4 is required. It is submitted that the work of replacement obsolete electromagnetic type protection relays in northern region with state-of-art numerical relays was deliberated in 11th TCC/12th NRPC Meeting held on 21st-22nd April 2009(copy attached as **Annexure-R/15**). In 20th TCC/22nd NRPC meeting, held on 28-29 June 2011 it was decided that utilities would submit the details of existing and planned numerical relays for their system (copy attached as **Annexure-R/16**). Further, The CEA "Standard Technical Specification for Sub- critical Thermal Power Project" under sub section 5.14.4 of Section-5 (Electrical Works) provides specification for Generator Protection and relay panel. CEA guidelines provides for installation of numerical relay based Generator protection system in order to meet the variety of functionalities with adequate accuracy and reliability (copy attached as **Annexure-R/17**). Further, Hon'ble Commission vide its order dated 17.04.2024 in Petition no-445/GT/2020 allowed the work of replacement of obsolete electromagnetic type relay based GRP with state of art numerical relays based GRP of Unit-1 & 3 of the instant station. In view of the above, it is humbly submitted that Hon'ble Commission may be pleased to allow the work of Upgradation of Generator & Busbar Protection System.	
10	Replacement of CRD - Retrofit of Energy chain for Trippers & Plough Feeders chp stg 1	196.00		196.00		196.00		25(2)(c) read with 102	Existing CRD system are in service for more than 15 years and have become obsolete. They are also energy intensive. No support is available from OEM. Therefore, Energy chain system to be installed for all moving trippers and plough feeders replacing the existing CRD system. In view of the above it is humbly submitted that Hon'ble Commission may be pleased to allow the work of Replacement of CRD -Retrofit of Energy chain for Trippers & Plough Feeders in CHP area.	NA
11	Fire Hyd and spray pumps replacement Stage-I	32.50		32.50		32.50		25(2)(c) read with 102	Hydrant and spray water pumps are main source of water for fire fighting system of entire plant. These fire Hydrant and spray water pumps are very old, and spares are not available. Considering their critical role in fire fighting system, their healthiness is of paramount importance. For the healthiness and availability of the fire water pumps the exiting fire hydrant and spray water pumps need to be replaced. In view of the above it is humbly submitted that Hon'ble Commission may be pleased to allow the Fire Hyd and spray pumps replacement	NA
12	Clarifiers replacement Stage-1	98.80		98.80		98.80		25(2) (c) & 26 (1) (d) read with 102	Detailed Justification provided at Sl No-A-10 of Form-9 25-26.	NA
13	Repair/strengthening work of all RCC structures of Stage I buildings as per RLA recommendations	520.00		520.00		520.00		25(2) (c) & 26 (1) (d) read with 102	Detailed Justification provided at Sl No-A-11 of Form-9 25-26.	NA
Sub Total-A		**2,742.64**	**-**	**2,742.64**	**-**	**2,742.64**				

PART-I
FORM- 9

Year wise Statement of Additional Capitalisation after COD

Name of the Petitioner	**NTPC Limited**
Name of the Generating Station	**Tanda Super Thermal Power Station Stage-I**
COD	**14-01-2000**
For Financial Year	**2026-27**

B.	**Works eligible for Return on Equity linked to SBI MCLR:**										
1	NA	-		-		-		NA	NA		NA
Sub Total-B		**-**	**-**	**-**	**-**	**-**					
Total Add. Cap. Claimed (A+B)		**2,742.64**	**-**	**2,742.64**	**-**	**2,742.64**					

(Petitioner)

Signature Not Verified

Digitally signed by PARIMAL PIYUSH
Date: 2024.11.25 22:55:12 IST
Reason: AGM(Commercial)
Location: NTPC Limited

PART-I
FORM- 9

Year wise Statement of Additional Capitalisation after COD

Name of the Petitioner	NTPC Limited
Name of the Generating Station	Tanda Super Thermal Power Station Stage-I
COD	14-01-2000
For Financial Year	2027-28

Amount in Rs Lakh

Sl. No.	Head of Work /Equipment	ACE Claimed (Projected)						Regulations under which claimed	Justification	Admitted Cost by the Commission, if any
		Accrual basis as per Ind AS	Ind AS Adjustment	Accrual basis as per IGAAP	Un-discharged Liability included in col. 3	Cash basis	IDC included in col. 3			
1	2	3	3A	3B=3+3A	4	5= (3-4)	6	7	8	9
A.	**Works eligible for RoE at Normal Rate**									
1	Upgradation of Generator & Busbar Protection System	130		130.00		130.00		25(2)(c) read with 102	Detailed Justification provided at Sl No-A9 of Form-9 26-27	NA
Sub Total-A		**130.00**		**130.00**		**130.00**				
B.	**Works eligble for Return on Equity linked to SBI MCLR:**									
1	NA	0.00		-		-		NA	NA	NA
Sub Total-B		**-**		**-**		**-**				
Total Add. Cap. Claimed (A+B)		**130.00**		**130.00**		**130.00**				

(Petitioner)

PART-I
FORM- 9

Year wise Statement of Additional Capitalisation after COD

Name of the Petitioner	NTPC Limited
Name of the Generating Station	Tanda Super Thermal Power Station Stage-I
COD	14-01-2000
For Financial Year	2028-29

Amount in Rs Lakh

Sl. No.	Head of Work /Equipment	ACE Claimed (Projected)						Regulations under which claimed	Justification	Admitted Cost by the Commission, if any
		Accrual basis as per Ind AS	Ind AS Adjustment	Accrual basis as per IGAAP	Un-discharged Liability included in col. 3	Cash basis	IDC included in col. 3			
1	2	3	3A	3B=3+3A	4	5= (3-4)	6	7	8	9
A.	Works eligble for RoE at Normal Rate									
1	NA	-		-		-		NA	NA	NA
Sub Total-A		-		-		-				
B.	Works eligble for Return on Equity linked to SBI MCLR:									
1	NA	-		-		-		NA	NA	NA
Sub Total-B		-		-		-				
Total Add. Cap. Claimed (A+B)		-	-	-	-	-				

(Petitioner)

Signature Not Verified

Digitally signed by PARIMAL PIYUSH
Date: 2024.11.25 22:55:12 IST
Reason: AGM(Commercial)
Location: NTPC Limited

Financing of Additional Capitalisation

PART-I
FORM- 10

Name of the Petitioner	**NTPC Limited**
Name of the Generating Station	**Tanda Super Thermal Power Station Stage-I**
Date of COD	**14-01-2000**

Amount in Rs Lakh

Financial Year (Starting from COD)1	Actual					Admitted				
	2024-25	**2025-26**	**2026-27**	**2027-28**	**2028-29**	**2024-25**	**2025-26**	**2026-27**	**2027-28**	**2028-29**
1		3	4	5	6	7	8	9	10	11
Amount capitalised in Work/ Equipment										
Financing Details	**SHALL BE PROVIDED AT THE TIME OF TRUE-UP.**									
Loan-1										
Loan-2										
Loan-3 and so on										
Total Loan2										
Equity Internal Resources										
Others (Pl. specify)										
Total										

(Petitioner)

Signature Not Verified

Digitally signed by PARIMAL PIYUSH
Date: 2024.11.25 22:55:12 IST
Reason: AGM(Commercial)
Location: NTPC Limited

Statement of Depreciation

PART-I
FORM- 12

Name of the Company : NTPC Limited

Name of the Power Station : Tanda Super Thermal Power Station Stage-I

(Amount in Rs Lakh)

S. No.	Particulars	Existing 2023-24	2024-25	2025-26	2026-27	2027-28	2028-29
1	2	3	4	5		6	8
1	Opening Capital Cost	1,24,216.34	1,24,753.82	1,24,753.82	1,24,753.82	1,24,753.82	1,24,753.82
2	Closing Capital Cost	1,24,753.82	1,24,753.82	1,24,753.82	1,24,753.82	1,24,753.82	1,24,753.82
3	Average Capital Cost	1,24,485.08	1,24,753.82	1,24,753.82	1,24,753.82	1,24,753.82	1,24,753.82
1a	Cost of IT Equipments & Software included in (1) above	188.23	186.98	186.98	186.98	186.98	186.98
2a	Cost of IT Equipments & Software included in (2) above	186.98	186.98	186.98	186.98	186.98	186.98
3a	Average Cost of IT Equipments & Software	187.61	186.98	186.98	186.98	186.98	186.98
4	Freehold land	1,674.71	1,674.71	1,674.71	1,674.71	1,674.71	1,674.71
5	Rate of depreciation	5.46%	5.46%	5.46%	5.46%	5.46%	5.46%
6	Depreciable value	**1,10,548.10**	**1,10,789.90**	**1,10,789.90**	**1,10,789.90**	**1,10,789.90**	**1,10,789.90**
7.	Balance useful life at the beginning of the period	1.79	0.79	-	-	-	-
8	Remaining depreciable value	8,011.15	4,017.56	-	-	-	-
9	Depreciation (for the period)	4,475.50	4,017.56	-	-	-	-
10	Depreciation (annualised)	**4,475.50**	**4,017.56**	**-**	**-**	**-**	**-**
11	Cumulative depreciation at the end of the period	1,07,012.45	1,10,789.90	1,10,789.90	1,10,789.90	1,10,789.90	1,10,789.90
12	Less: Cumulative depreciation adjustment on account of un-discharged liabilities deducted as on 01.04.2009	-	-	-	-	-	-
13	Add: Cumulative depreciation adjustment on account of liability Discharge	-	-	-	-	-	-
14	Less: Cumulative depreciation adjustment on account of de-capitalisation	240.11	-	-	-	-	-
15	Net Cumulative depreciation at the end of the period after adjustments	1,06,772.34	1,10,789.90	1,10,789.90	1,10,789.90	1,10,789.90	1,10,789.90

Statement of Depreciation- New Asset

PART-I
FORM- 12A

Name of the Company :	**NTPC Limited**
Name of the Power Station :	**Tanda Super Thermal Power Station Stage-I**

(Amount in Rs Lakh)

S. No.	Particulars	Existing 2023-24	2024-25	2025-26	2026-27	2027-28	2028-29
1	**2**	**3**	**4**	**5**		**6**	**8**
1	Opening Capital Cost	-	-	1,208.50	5,269.50	8,012.14	8,142.14
2	Add Cap During the Year		1,208.50	4,061.00	2,742.64	130.00	-
2	Closing Capital Cost	-	1,208.50	5,269.50	8,012.14	8,142.14	8,142.14
3	Average Capital Cost	-	604.25	3,239.00	6,640.82	8,077.14	8,142.14
1a	Cost of IT Equipments & Software included in (1) above	-	-	-	-	-	-
2a	Cost of IT Equipments & Software included in (2) above	-	-	-	-	-	-
3a	Average Cost of IT Equipments & Software	-	-	-	-	-	-
4	Freehold land	-	-	-	-	-	-
5	Rate of depreciation	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
6	Depreciable value	**-**	**543.83**	**2,915.10**	**5,976.74**	**7,269.43**	**7,327.93**
7.	Balance useful life at the beginning of the period	1.79	0.79	-	-	-	-
	Life of Station from COD	23.21	24.21	25.21	26.21	27.21	28.21
7a	Effective Balance useful life at the beginning of the period for Depreciation of New Asset	NA	10.79	9.79	8.79	7.79	6.79
8	Remaining depreciable value	-	543.83	2,864.70	5,633.72	6,285.49	5,537.12
9	Depreciation (for the period)	-	50.40	292.61	640.92	806.87	815.48
10	Depreciation (annualised)	**-**	**50.40**	**292.61**	**640.92**	**806.87**	**815.48**
11	Cumulative depreciation at the end of the period	-	50.40	343.02	983.94	1,790.81	2,606.29
12	Less: Cumulative depreciation adjustment on account of un-discharged liabilities deducted as on 01.04.2009	-	-	-	-	-	-
13	Add: Cumulative depreciation adjustment on account of liability Discharge	-	-	-	-	-	-
14	Less: Cumulative depreciation adjustment on account of de-capitalisation	-	-	-	-	-	-
15	Net Cumulative depreciation at the end of the period after adjustments	-	50.40	343.02	983.94	1,790.81	2,606.29

Petitioner

Signature Not Verified

Digitally signed by PARIMAL PIYUSH
Date: 2024.11.25 22:55:12 IST
Reason: AGM(Commercial)
Location: NTPC Limited

					PART-I FORM-13
Name of the Company	**NTPC Limited**				
Name of the Power Station	**Tanda Super Thermal Power Station Stage-I**				
					(Amount in lacs)
	2024-25	**2025-26**	**2026-27**	**2027-28**	**2028-29**
Bond 61					
OP Bal	533.33	533.33	533.33	266.67	266.67
Additions	0.00	0.00	0.00	0.00	0.00
Repayment	0.00	0.00	266.67	0.00	0.00
Cl Bal	533.33	533.33	266.67	266.67	266.67
Avg Loan	533.33	533.33	400.00	266.67	266.67
Int Rate	8.1300%	8.1300%	8.1300%	8.1300%	8.1300%
Interest	43.36	43.36	32.52	21.68	21.68
SBBJ, D-V (Repayment from 14.03.2020 - 10 yearly)					
OP Bal	5000.00	4000.00	3000.00	2000.00	1000.00
Additions	0.00	0.00	0.00	0.00	0.00
Repayment	1000.00	1000.00	1000.00	1000.00	1000.00
Cl Bal	4000.00	3000.00	2000.00	1000.00	0.00
Avg Loan	4500.00	3500.00	2500.00	1500.00	500.00
Int Rate	8.2000%	8.2000%	8.2000%	8.2000%	8.2000%
Interest	369.00	287.00	205.00	123.00	41.00
Punjab National Bank-III, D-4 (Repayment from 01.04.2022 - 9 yearly)					
OP Bal	6666.67	5555.56	4444.44	3333.33	2222.22
Additions	0.00	0.00	0.00	0.00	0.00
Repayment	1111.11	1111.11	1111.11	1111.11	1111.11
Cl Bal	5555.56	4444.44	3333.33	2222.22	1111.11
Avg Loan	6111.11	5000.00	3888.89	2777.78	1666.67
Int Rate	7.9000%	7.9000%	7.9000%	7.9000%	7.9000%
Interest	482.78	395.00	307.22	219.44	131.67
Bond 72 (Bullet repaymnet 25-10-2025)					
OP Bal	781.25	781.25	0.00	0.00	0.00

					PART-I FORM-13
Name of the Company	**NTPC Limited**				
Name of the Power Station	**Tanda Super Thermal Power Station Stage-I**				
					(Amount in lacs)
	2024-25	**2025-26**	**2026-27**	**2027-28**	**2028-29**
Additions	0.00	0.00	0.00	0.00	0.00
Repayment	0.00	781.25	0.00	0.00	0.00
Cl Bal	781.25	0.00	0.00	0.00	0.00
Avg Loan	781.25	390.63	0.00	0.00	0.00
Int Rate	6.41%	6.41%	6.41%	6.41%	6.41%
Interest	50.08	25.04	0.00	0.00	0.00
Bond 72 (Bullet repaymnet 25-10-2025)					
OP Bal	718.75	718.75	0.00	0.00	0.00
Additions	0.00	0.00	0.00	0.00	0.00
Repayment	0.00	718.75	0.00	0.00	0.00
Cl Bal	718.75	0.00	0.00	0.00	0.00
Avg Loan	718.75	359.38	0.00	0.00	0.00
Int Rate	5.48%	5.48%	5.48%	5.48%	5.48%
Interest	39.39	19.69	0.00	0.00	0.00
Total Loan					
OP Bal	13700.00	11588.89	7977.78	5600.00	3488.89
Additions	0.00	0.00	0.00	0.00	0.00
Repayment	2111.11	3611.11	2377.78	2111.11	2111.11
Cl Bal	11588.89	7977.78	5600.00	3488.89	1377.78
Avg Loan	12644.44	9783.33	6788.89	4544.44	2433.33
Int Rate	**7.7868%**	**7.8715%**	**8.0240%**	**8.0125%**	**7.9868%**
Interest	984.60	770.09	544.74	364.12	194.35

WAR						
BANK	**RATE OF INTEREST**	**From**	**To**	**No. of Days**	**Weight**	**WAR**
Punjab National Bank III	7.90%	01-Apr-23	31-Mar-24	366.00	28.91	
				366.00	**28.91**	**7.90%**
BANK	**RATE OF INTEREST**	**From**	**To**	**No. of Days**	**Weight**	**WAR**
State Bank of Bikaner & Jaipur	0.08	45017	45059	43.00	3.44	
State Bank of Bikaner & Jaipur	8.1000%	14-May-23	45151.00	92.00	7.45	
State Bank of Bikaner & Jaipur	8.1500%	14-Aug-23	45335.00	184.00	15.00	
State Bank of Bikaner & Jaipur	8.2000%	14-Feb-24	45382.00	47.00	3.85	
				366.00	**29.74**	**8.13%**

Details of Refinancing

Sr. No.	Bank	ROI on refinancing date	Date of refinancing	Refinanced with Bank	Refinanced Amount (Rs. In crore)	New Loan Amount (Rs. In crore)	ROI of relplaced Loan	savings	saving to be retained (Percent)	Remarks
1	Power Finance Corporation - V	7.31%	15-Oct-20	Bonds Series-72	4,000.00	4,000.00	5.45%	1.86%	0.9300%	Loan outstanding as on 14.10.2020 from PFC-V have been foreclosed by way of refinancing from Bond Series-72 at a concessional rate. One-half of the savings in the interest rate is added to the weighted average rate of loan.

Refinancing of PFC Loans 15.10.2020

BP NO.	DESCRIPTION	O/s amount	Interest rate benchmark and rate on swap date	Refinanced by Loan	Interest rate benchmark and rate on swap date
5070000011	Power Finance Corporation - V	41,66,66,66,668	3Y-AAA Bond rate +45bps	Bonds- Rs. 4000Cr , HDFC-IX-Rs. 166.66	5.45%/ Repo rate+195bps-5.95%

Details of Source wise Fuel for Computation of Energy Charges — **PART-I** **FORM- 15**

Name of the Company :			NTPC Limited				
Name of the Power Station :			Tanda Super Thermal Power Station Stage-I				
S. No.	Particulars	Unit	Apr-23				
			Domestic Coal-FSA	Domestic Coal-NTPC Mines	E-Auction Coal	Imported Coal	Bio-Mass
A)	**OPENING QUANTITY**						
1	Opening Quantity of Coal/ Lignite	(MT)	2,03,323	2,52,808	-	61,114	-
2	Value of Stock	(Rs.)	88,53,93,101	97,28,81,711	-	97,23,46,329	-
B)	**QUANTITY**						
3	Quantity of Coal supplied by Coal Company	(MT)	4,43,037	65,577	-	2,16,717	-
4	Adjustment (+/-) in quantity supplied made by Coal Company	(MT)	-	-503	-	-	-
5	Coal supplied by Coal Company (3+4)	(MT)	4,43,037	65,074	-	2,16,717	-
6	Normative Transit & Handling Losses	(MT)	3,544	525	-	433	-
7	Net coal / Lignite Supplied (5-6)	(MT)	4,39,493	64,549	-	2,16,284	-
C)	**PRICE**						
8	Amount charged by the Coal Company	(Rs.)	1,12,47,10,707	15,48,89,196	-	3,15,71,83,276	-
9	Adjustment (+/-) in amount charged made by Coal Company	(Rs.)	15,24,47,498	-12,14,977	-	-	-
10	Handling, Sampling and such other similar charges	(Rs.)	18,31,958	2,71,273	-	8,96,475	-
11	Total amount Charged (8+9+10)	(Rs.)	1,27,89,90,163	15,39,45,491	-	3,15,80,79,751	-
D)	**TRANSPORATION**						
12	Transportation charges by rail ship, road transport	(Rs.)	63,20,45,436	9,56,49,677	-	-	-
13	Adjustment (+/-) in amount charged made by Railways/ Transport Company	(Rs.)	-	-	-	-	-
14	Demurrage Charges, if any	(Rs.)	1,27,893	-	-	-	-
15	Cost of diesel in transporting coal through MGR system, if applicable	(Rs.)	-	-	-	-	-
16	Total Transportation Charges (12+13+14+15)	(Rs.)	63,19,17,543	9,56,49,677	-	-	-
17	Total amount Charged for coal supplied including Transportation (11+16)	(Rs.)	1,91,09,07,707	24,95,95,168	-	3,15,80,79,751	-
E)	**TOTAL COST**						
18	**Landed cost of coal (2+17)/(1+7)**	**Rs./MT**	**4,350**	**3,852**	**-**	**14,890**	**-**
19	Blending Ratio	%	1	0	-	0	-
20	Weighted average cost of coal	Rs./MT					**6,282**
F)	**QUALITY**						
21	GCV of Domestic Coal of the opening stock as per bill of Coal Company	(kCal/Kg)	4,197	4,601			
22	GCV of Domestic Coal supplied as per bill Coal Company	(kCal/Kg)	4,306	4,472			
23	GCV of Imported Coal of the opening stock as per bill of Coal Company	(kCal/Kg)				5,201	
24	GCV of Imported Coal supplied as per bill Coal Company	(kCal/Kg)				5,178	
25	Weighted average GCV of coal/ Lignite as Billed	(kCal/Kg)					**4,519**
26	GCV of Domestic Coal of opening stock as received at Station	(kCal/Kg)	3,613	3,873			
27	GCV of Domestic Coal supplied as received at Station	(kCal/Kg)	3,583	3,601			
28	GCV of Imported Coal of opening stock as received at Station	(kCal/Kg)	-	-	-	4,900	-
29	GCV of Imported Coal supplied as received at Station	(kCal/Kg)	-	-	-	4,963	-
30	**Weighted average GCV of coal/ Lignite as Received**	**(kCal/Kg)**					**3,907**

(Petitioner)

Details of Source wise Fuel for Computation of Energy Charges							PART-I FORM- 15
Name of the Company :			NTPC Limited				
Name of the Power Station :			Tanda Super Thermal Power Station Stage-I				
S. No.	Particulars	Unit	May-23				
			Domestic Coal-FSA	Domestic Coal-NTPC Mines	E-Auction Coal	Imported Coal	Bio-Mass
A)	**OPENING QUANTITY**						
1	Opening Quantity of Coal/ Lignite	(MT)	3,55,286	1,90,692	-	1,79,918	-
2	Value of Stock	(Rs.)	1,54,55,22,305	73,45,56,586	-	2,67,89,57,711	-
B)	**QUANTITY**						
3	Quantity of Coal supplied by Coal Company	(MT)	4,02,236	45,635	-	1,05,692	-
4	Adjustment (+/-) in quantity supplied made by Coal Company	(MT)	-	-	-	-	-
5	Coal supplied by Coal Company (3+4)	(MT)	4,02,236	45,635	-	1,05,692	-
6	Normative Transit & Handling Losses	(MT)	3,218	365	-	211	-
7	Net coal / Lignite Supplied (5-6)	(MT)	3,99,018	45,270	-	1,05,481	-
C)	**PRICE**						
8	Amount charged by the Coal Company	(Rs.)	1,06,96,25,872	10,66,93,156	-	1,54,32,30,620	-
9	Adjustment (+/-) in amount charged made by Coal Company	(Rs.)	5,42,19,585	-	-	-	-
10	Handling, Sampling and such other similar charges	(Rs.)	1,69,28,709	13,12,354	-	30,39,474	-
11	Total amount Charged (8+9+10)	(Rs.)	1,14,07,74,165	10,80,05,510	-	1,54,62,70,094	-
D)	**TRANSPORATION**						
12	Transportation charges by rail ship, road transport	(Rs.)	60,12,01,146	6,62,73,386	-	-	-
13	Adjustment (+/-) in amount charged made by Railways/ Transport Company	(Rs.)	-	-	-	-	-
14	Demurrage Charges, if any	(Rs.)	-	11,76,202	-	-	-
15	Cost of diesel in transporting coal through MGR system, if applicable	(Rs.)	-	-	-	-	-
16	Total Transportation Charges (12+13+14+15)	(Rs.)	60,12,01,146	6,50,97,184	-	-	-
17	Total amount Charged for coal supplied including Transportation (11+16)	(Rs.)	1,74,19,75,311	17,31,02,694	-	1,54,62,70,094	-
E)	**TOTAL COST**						
18	**Landed cost of coal (2+17)/(1+7)**	**Rs./MT**	**4,358**	**3,847**	**-**	**14,805**	**-**
19	Blending Ratio	%	1	0	-	0	-
20	Weighted average cost of coal	Rs./MT					**6,354**
F)	**QUALITY**						
21	GCV of Domestic Coal of the opening stock as per bill of Coal Company	(kCal/Kg)	4,273	4,575			
22	GCV of Domestic Coal supplied as per bill Coal Company	(kCal/Kg)	4,418	4,601			
23	GCV of Imported Coal of the opening stock as per bill of Coal Company	(kCal/Kg)				5,183	
24	GCV of Imported Coal supplied as per bill Coal Company	(kCal/Kg)				5,086	
25	Weighted average GCV of coal/ Lignite as Billed	(kCal/Kg)					**4,543**
26	GCV of Domestic Coal of opening stock as received at Station	(kCal/Kg)	3,592	3,818			
27	GCV of Domestic Coal supplied as received at Station	(kCal/Kg)	3,694	3,596			
28	GCV of Imported Coal of opening stock as received at Station	(kCal/Kg)	-	-	-	4,949	-
29	GCV of Imported Coal supplied as received at Station	(kCal/Kg)	-	-	-	4,910	-
30	**Weighted average GCV of coal/ Lignite as Received**	**(kCal/Kg)**					**3,921**

(Petitioner)

Details of Source wise Fuel for Computation of Energy Charges							PART-I FORM- 15
Name of the Company :			NTPC Limited				
Name of the Power Station :			Tanda Super Thermal Power Station Stage-I				
S. No.	Particulars	Unit	Jun-23				
			Domestic Coal-FSA	Domestic Coal-NTPC Mines	E-Auction Coal	Imported Coal	Bio-Mass
A)	**OPENING QUANTITY**						
1	Opening Quantity of Coal/ Lignite	(MT)	5,17,123	1,30,362	-	2,04,358	-
2	Value of Stock	(Rs.)	2,25,37,86,683	50,14,54,518	-	3,02,54,57,008	-
B)	**QUANTITY**						
3	Quantity of Coal supplied by Coal Company	(MT)	57,714	38,068	-	39,915	-
4	Adjustment (+/-) in quantity supplied made by Coal Company	(MT)	-	-71	-	-	-
5	Coal supplied by Coal Company (3+4)	(MT)	57,714	37,997	-	39,915	-
6	Normative Transit & Handling Losses	(MT)	3,208	305	-	80	-
7	Net coal / Lignite Supplied (5-6)	(MT)	3,97,849	37,693	-	39,835	-
C)	**PRICE**						
8	Amount charged by the Coal Company	(Rs.)	1,09,31,81,023	9,65,51,623	-	58,59,20,557	-
9	Adjustment (+/-) in amount charged made by Coal Company	(Rs.)	6,98,89,488	-1,71,221	-	-3,87,64,775	-
10	Handling, Sampling and such other similar charges	(Rs.)	2,98,40,853	28,32,469	-	29,69,867	-
11	Total amount Charged (8+9+10)	(Rs.)	1,19,29,11,364	9,92,12,871	-	55,01,25,649	-
D)	**TRANSPORATION**						
12	Transportation charges by rail ship, road transport	(Rs.)	63,45,34,477	5,44,87,734	-	-	-
13	Adjustment (+/-) in amount charged made by Railways/ Transport Company	(Rs.)	-	-	-	-	-
14	Demurrage Charges, if any	(Rs.)	8,59,856	-	-	-	-
15	Cost of diesel in transporting coal through MGR system, if applicable	(Rs.)	-	-	-	-	-
16	Total Transportation Charges (12+13+14+15)	(Rs.)	63,36,74,621	5,44,87,734	-	-	-
17	Total amount Charged for coal supplied including Transportation (11+16)	(Rs.)	1,82,65,85,985	15,37,00,605	-	55,01,25,649	-
E)	**TOTAL COST**						
18	**Landed cost of coal (2+17)/(1+7)**	**Rs./MT**	**4,460**	**3,898**	**-**	**14,642**	**-**
19	Blending Ratio	%	1	0	0.00%	0	-
20	Weighted average cost of coal	Rs./MT					**6,462**
F)	**QUALITY**						
21	GCV of Domestic Coal of the opening stock as per bill of Coal Company	(kCal/Kg)	4,351	4,580			
22	GCV of Domestic Coal supplied as per bill Coal Company	(kCal/Kg)	4,487	4,601			
23	GCV of Imported Coal of the opening stock as per bill of Coal Company	(kCal/Kg)				5,147	
24	GCV of Imported Coal supplied as per bill Coal Company	(kCal/Kg)				5,081	
25	Weighted average GCV of coal/ Lignite as Billed	(kCal/Kg)					**4,563**
26	GCV of Domestic Coal of opening stock as received at Station	(kCal/Kg)	3,646	3,776			
27	GCV of Domestic Coal supplied as received at Station	(kCal/Kg)	3,639	3,546			
28	GCV of Imported Coal of opening stock as received at Station	(kCal/Kg)	-	-	-	4,935	-
29	GCV of Imported Coal supplied as received at Station	(kCal/Kg)	-	-	-	4,971	-
30	**Weighted average GCV of coal/ Lignite as Received**	**(kCal/Kg)**					**3,906**

(Petitioner)

Details of Source wise Fuel for Computation of Energy Charges							PART-I FORM- 15
Name of the Company :			NTPC Limited				
Name of the Power Station :			Tanda Super Thermal Power Station Stage-I				
S. No.	Particulars	Unit	Jul-23				
			Domestic Coal-FSA	Domestic Coal-NTPC Mines	E-Auction Coal	Imported Coal	Bio-Mass
A)	**OPENING QUANTITY**						
1	Opening Quantity of Coal/ Lignite	(MT)	5,86,007	74,053	-	1,51,877	-
2	Value of Stock	(Rs.)	2,61,33,33,841	28,86,95,045	-	2,22,38,51,228	-
B)	**QUANTITY**						
3	Quantity of Coal supplied by Coal Company	(MT)	3,84,090	31,012	-	31,652	-
4	Adjustment (+/-) in quantity supplied made by Coal Company	(MT)	-	-	-	-	-
5	Coal supplied by Coal Company (3+4)	(MT)	3,84,090	31,012	-	31,652	-
6	Normative Transit & Handling Losses	(MT)	3,073	248	-	63	-
7	Net coal / Lignite Supplied (5-6)	(MT)	3,81,017	30,764	-	31,589	-
C)	**PRICE**						
8	Amount charged by the Coal Company	(Rs.)	1,12,47,01,382	10,66,60,306	-	46,18,86,933	-
9	Adjustment (+/-) in amount charged made by Coal Company	(Rs.)	6,46,76,648	-	-	-2,98,830	-
10	Handling, Sampling and such other similar charges	(Rs.)	44,50,714	3,59,375	-	3,66,789	-
11	Total amount Charged (8+9+10)	(Rs.)	1,19,38,28,743	10,70,19,681	-	46,19,54,892	-
D)	**TRANSPORATION**						
12	Transportation charges by rail ship, road transport	(Rs.)	50,85,42,013	1,38,63,324	-	-	-
13	Adjustment (+/-) in amount charged made by Railways/ Transport Company	(Rs.)	-	-	-	-	-
14	Demurrage Charges, if any	(Rs.)	5,72,421	-	-	-	-
15	Cost of diesel in transporting coal through MGR system, if applicable	(Rs.)	-	-	-	-	-
16	Total Transportation Charges (12+13+14+15)	(Rs.)	50,79,69,592	1,38,63,324	-	-	-
17	Total amount Charged for coal supplied including Transportation (11+16)	(Rs.)	1,70,17,98,335	12,08,83,005	-	46,19,54,892	-
E)	**TOTAL COST**						
18	**Landed cost of coal (2+17)/(1+7)**	**Rs./MT**	**4,462**	**3,908**	**-**	**14,639**	**-**
19	Blending Ratio	%	1	0	-	0	-
20	Weighted average cost of coal	Rs./MT					**6,247**
F)	**QUALITY**						
21	GCV of Domestic Coal of the opening stock as per bill of Coal Company	(kCal/Kg)	4,411	4,585			
22	GCV of Domestic Coal supplied as per bill Coal Company	(kCal/Kg)	4,360	4,601			
23	GCV of Imported Coal of the opening stock as per bill of Coal Company	(kCal/Kg)				5,136	
24	GCV of Imported Coal supplied as per bill Coal Company	(kCal/Kg)				5,049	
25	Weighted average GCV of coal/ Lignite as Billed	(kCal/Kg)					**4,547**
26	GCV of Domestic Coal of opening stock as received at Station	(kCal/Kg)	3,643	3,725			
27	GCV of Domestic Coal supplied as received at Station	(kCal/Kg)	3,608	3,381			
28	GCV of Imported Coal of opening stock as received at Station	(kCal/Kg)	-	-	-	4,941	-
29	GCV of Imported Coal supplied as received at Station	(kCal/Kg)	-	-	-	4,833	-
30	**Weighted average GCV of coal/ Lignite as Received**	**(kCal/Kg)**					**3,863**

(Petitioner)

Details of Source wise Fuel for Computation of Energy Charges							PART-I FORM- 15
Name of the Company :			NTPC Limited				
Name of the Power Station :			Tanda Super Thermal Power Station Stage-I				
S. No.	Particulars	Unit	Aug-23				
			Domestic Coal-FSA	Domestic Coal-NTPC Mines	E-Auction Coal	Imported Coal	Bio-Mass
A)	**OPENING QUANTITY**						
1	Opening Quantity of Coal/ Lignite	(MT)	5,55,072	47,694	-	99,227	-
2	Value of Stock	(Rs.)	2,47,68,87,830	18,63,64,306	-	1,45,26,08,292	-
B)	**QUANTITY**						
3	Quantity of Coal supplied by Coal Company	(MT)	4,55,393	44,299	-	67,905	-
4	Adjustment (+/-) in quantity supplied made by Coal Company	(MT)	-	-	-	-	-
5	Coal supplied by Coal Company (3+4)	(MT)	4,55,393	44,299	-	67,905	-
6	Normative Transit & Handling Losses	(MT)	3,643	354	-	136	-
7	Net coal / Lignite Supplied (5-6)	(MT)	4,51,750	43,945	-	67,769	-
C)	**PRICE**						
8	Amount charged by the Coal Company	(Rs.)	1,31,11,23,795	15,37,21,880	-	99,45,45,576	-
9	Adjustment (+/-) in amount charged made by Coal Company	(Rs.)	8,25,95,769	-	-	-	-
10	Handling, Sampling and such other similar charges	(Rs.)	1,37,37,391	13,36,337	-	20,48,420	-
11	Total amount Charged (8+9+10)	(Rs.)	1,40,74,56,955	15,50,58,217	-	99,65,93,996	-
D)	**TRANSPORATION**						
12	Transportation charges by rail ship, road transport	(Rs.)	65,16,24,007	1,98,79,803	-	-	-
13	Adjustment (+/-) in amount charged made by Railways/ Transport Company	(Rs.)	-	-	-	-	-
14	Demurrage Charges, if any	(Rs.)	1,09,463	-	-	-	-
15	Cost of diesel in transporting coal through MGR system, if applicable	(Rs.)	-	-	-	-	-
16	Total Transportation Charges (12+13+14+15)	(Rs.)	65,15,14,544	1,98,79,803	-	-	-
17	Total amount Charged for coal supplied including Transportation (11+16)	(Rs.)	2,05,89,71,500	17,49,38,020	-	99,65,93,996	-
E)	**TOTAL COST**						
18	**Landed cost of coal (2+17)/(1+7)**	**Rs./MT**	**4,505**	**3,943**	**-**	**14,666**	**-**
19	Blending Ratio	%	1	-	-	0	-
20	Weighted average cost of coal	Rs./MT					**6,522**
F)	**QUALITY**						
21	GCV of Domestic Coal of the opening stock as per bill of Coal Company	(kCal/Kg)	4,375	4,632			
22	GCV of Domestic Coal supplied as per bill Coal Company	(kCal/Kg)	4,383	4,601			
23	GCV of Imported Coal of the opening stock as per bill of Coal Company	(kCal/Kg)				5,121	
24	GCV of Imported Coal supplied as per bill Coal Company	(kCal/Kg)				4,777	
25	Weighted average GCV of coal/ Lignite as Billed	(kCal/Kg)					**4,498**
26	GCV of Domestic Coal of opening stock as received at Station	(kCal/Kg)	3,634	3,620			
27	GCV of Domestic Coal supplied as received at Station	(kCal/Kg)	3,607	3,655			
28	GCV of Imported Coal of opening stock as received at Station	(kCal/Kg)	-	-	-	4,922	-
29	GCV of Imported Coal supplied as received at Station	(kCal/Kg)	-	-	-	4,827	-
30	**Weighted average GCV of coal/ Lignite as Received**	**(kCal/Kg)**					**3,872**

(Petitioner)

Details of Source wise Fuel for Computation of Energy Charges							PART-I FORM- 15
Name of the Company :			NTPC Limited				
Name of the Power Station :			Tanda Super Thermal Power Station Stage-I				
S. No.	Particulars	Unit	Sep-23				
			Domestic Coal-FSA	Domestic Coal-NTPC Mines	E-Auction Coal	Imported Coal	Bio-Mass
A)	**OPENING QUANTITY**						
1	Opening Quantity of Coal/ Lignite	(MT)	5,15,471	29,639	-	58,859	-
2	Value of Stock	(Rs.)	2,32,22,62,147	11,68,55,856	-	86,32,38,745	-
B)	**QUANTITY**						
3	Quantity of Coal supplied by Coal Company	(MT)	3,88,367	19,432	-	55,853	-
4	Adjustment (+/-) in quantity supplied made by Coal Company	(MT)	-	-288	-	-	-
5	Coal supplied by Coal Company (3+4)	(MT)	3,88,367	19,144	-	55,853	-
6	Normative Transit & Handling Losses	(MT)	3,107	155	-	112	-
7	Net coal / Lignite Supplied (5-6)	(MT)	3,85,260	18,989	-	55,742	-
C)	**PRICE**						
8	Amount charged by the Coal Company	(Rs.)	1,29,08,74,526	5,22,55,566	-	79,08,85,739	-
9	Adjustment (+/-) in amount charged made by Coal Company	(Rs.)	3,65,82,221	-7,21,103	-	-3,58,96,499	-
10	Handling, Sampling and such other similar charges	(Rs.)	2,07,68,120	10,39,118	-	29,86,786	-
11	Total amount Charged (8+9+10)	(Rs.)	1,34,82,24,867	5,25,73,581	-	75,79,76,027	-
D)	**TRANSPORATION**						
12	Transportation charges by rail ship, road transport	(Rs.)	51,15,98,384	84,61,880	-	-	-
13	Adjustment (+/-) in amount charged made by Railways/ Transport Company	(Rs.)	-	-	-	-	-
14	Demurrage Charges, if any	(Rs.)	3,23,665	-	-	-	-
15	Cost of diesel in transporting coal through MGR system, if applicable	(Rs.)	-	-	-	-	-
16	Total Transportation Charges (12+13+14+15)	(Rs.)	51,12,74,719	84,61,880	-	-	-
17	Total amount Charged for coal supplied including Transportation (11+16)	(Rs.)	1,85,94,99,586	6,10,35,461	-	75,79,76,027	-
E)	**TOTAL COST**						
18	**Landed cost of coal (2+17)/(1+7)**	**Rs./MT**	**4,643**	**3,658**	**-**	**14,147**	**-**
19	Blending Ratio	%	1	-	-	0	-
20	Weighted average cost of coal	Rs./MT					**6,532**
F)	**QUALITY**						
21	GCV of Domestic Coal of the opening stock as per bill of Coal Company	(kCal/Kg)	4,379	4,617			
22	GCV of Domestic Coal supplied as per bill Coal Company	(kCal/Kg)	4,692	4,601			
23	GCV of Imported Coal of the opening stock as per bill of Coal Company	(kCal/Kg)				4,980	
24	GCV of Imported Coal supplied as per bill Coal Company	(kCal/Kg)				4,763	
25	Weighted average GCV of coal/ Lignite as Billed	(kCal/Kg)					**4,585**
26	GCV of Domestic Coal of opening stock as received at Station	(kCal/Kg)	3,616	3,671			
27	GCV of Domestic Coal supplied as received at Station	(kCal/Kg)	3,617	3,544			
28	GCV of Imported Coal of opening stock as received at Station	(kCal/Kg)	-	-	-	4,879	-
29	GCV of Imported Coal supplied as received at Station	(kCal/Kg)	-	-	-	4,838	-
30	**Weighted average GCV of coal/ Lignite as Received**	**(kCal/Kg)**					**3,863**

(Petitioner)

Details of Source wise Fuel for Computation of Energy Charges							PART-I FORM- 15
Name of the Company :			NTPC Limited				
Name of the Power Station :			Tanda Super Thermal Power Station Stage-I				
S. No.	Particulars	Unit	Oct-23				
			Domestic Coal-FSA	Domestic Coal-NTPC Mines	E-Auction Coal	Imported Coal	Bio-Mass
A)	**OPENING QUANTITY**						
1	Opening Quantity of Coal/ Lignite	(MT)	3,76,643	28,627	-	10,023	-
2	Value of Stock	(Rs.)	1,74,86,11,468	10,47,25,977	-	14,17,85,967	-
B)	**QUANTITY**						
3	Quantity of Coal supplied by Coal Company	(MT)	4,52,502	1,26,937	-	15,790	-
4	Adjustment (+/-) in quantity supplied made by Coal Company	(MT)	-	-3,090	-	-	-
5	Coal supplied by Coal Company (3+4)	(MT)	4,52,502	1,23,848	-	15,790	-
6	Normative Transit & Handling Losses	(MT)	3,620	1,016	-	32	-
7	Net coal / Lignite Supplied (5-6)	(MT)	4,48,882	1,22,832	-	15,759	-
C)	**PRICE**						
8	Amount charged by the Coal Company	(Rs.)	1,37,77,58,482	35,78,60,644	-	20,18,97,514	-
9	Adjustment (+/-) in amount charged made by Coal Company	(Rs.)	3,53,91,826	-77,41,074	-	-	-
10	Handling, Sampling and such other similar charges	(Rs.)	1,37,10,017	38,47,415	-	4,78,597	-
11	Total amount Charged (8+9+10)	(Rs.)	1,42,68,60,325	35,39,66,985	-	20,23,76,111	-
D)	**TRANSPORATION**						
12	Transportation charges by rail ship, road transport	(Rs.)	54,13,66,536	13,21,68,109	-	-	-
13	Adjustment (+/-) in amount charged made by Railways/ Transport Company	(Rs.)	-	-	-	-	-
14	Demurrage Charges, if any	(Rs.)	-	-	-	-	-
15	Cost of diesel in transporting coal through MGR system, if applicable	(Rs.)	-	-	-	-	-
16	Total Transportation Charges (12+13+14+15)	(Rs.)	54,13,66,536	13,21,68,109	-	-	-
17	Total amount Charged for coal supplied including Transportation (11+16)	(Rs.)	1,96,82,26,861	48,61,35,094	-	20,23,76,111	-
E)	**TOTAL COST**						
18	**Landed cost of coal (2+17)/(1+7)**	**Rs./MT**	**4,502**	**3,901**	**-**	**13,349**	**-**
19	Blending Ratio	%	1	0	-	0	-
20	Weighted average cost of coal	Rs./MT					**5,075**
F)	**QUALITY**						
21	GCV of Domestic Coal of the opening stock as per bill of Coal Company	(kCal/Kg)	4,519	4,611			
22	GCV of Domestic Coal supplied as per bill Coal Company	(kCal/Kg)	4,354	4,601			
23	GCV of Imported Coal of the opening stock as per bill of Coal Company	(kCal/Kg)				4,873	
24	GCV of Imported Coal supplied as per bill Coal Company	(kCal/Kg)				4,749	
25	Weighted average GCV of coal/ Lignite as Billed	(kCal/Kg)					**4,464**
26	GCV of Domestic Coal of opening stock as received at Station	(kCal/Kg)	3,634	3,684			
27	GCV of Domestic Coal supplied as received at Station	(kCal/Kg)	3,757	4,084			
28	GCV of Imported Coal of opening stock as received at Station	(kCal/Kg)	-	-	-	4,859	-
29	GCV of Imported Coal supplied as received at Station	(kCal/Kg)	-	-	-	4,927	-
30	**Weighted average GCV of coal/ Lignite as Received**	**(kCal/Kg)**					**3,801**

(Petitioner)

Details of Source wise Fuel for Computation of Energy Charges							PART-I FORM- 15
Name of the Company :			NTPC Limited				
Name of the Power Station :			Tanda Super Thermal Power Station Stage-I				
S. No.	Particulars	Unit	Nov-23				
			Domestic Coal-FSA	Domestic Coal-NTPC Mines	E-Auction Coal	Imported Coal	Bio-Mass
A)	**OPENING QUANTITY**						
1	Opening Quantity of Coal/ Lignite	(MT)	2,49,091	1,41,459	-	5,781	-
2	Value of Stock	(Rs.)	1,12,15,04,769	55,18,49,881	-	7,71,76,241	-
B)	**QUANTITY**						
3	Quantity of Coal supplied by Coal Company	(MT)	3,86,490	1,22,191	-	73,029	-
4	Adjustment (+/-) in quantity supplied made by Coal Company	(MT)	-	-	-	-	-
5	Coal supplied by Coal Company (3+4)	(MT)	3,86,490	1,22,191	-	73,029	-
6	Normative Transit & Handling Losses	(MT)	3,092	978	-	146	-
7	Net coal / Lignite Supplied (5-6)	(MT)	3,83,398	1,21,213	-	72,883	-
C)	**PRICE**						
8	Amount charged by the Coal Company	(Rs.)	1,24,25,65,718	33,03,42,967	-	97,46,36,535	-
9	Adjustment (+/-) in amount charged made by Coal Company	(Rs.)	4,01,77,265	-	-	-4,81,84,289	-
10	Handling, Sampling and such other similar charges	(Rs.)	20,69,217	5,45,725	-	3,22,777	-
11	Total amount Charged (8+9+10)	(Rs.)	1,28,48,12,200	33,08,88,692	-	92,67,75,023	-
D)	**TRANSPORATION**						
12	Transportation charges by rail ship, road transport	(Rs.)	51,44,04,242	14,91,76,125	-	-	-
13	Adjustment (+/-) in amount charged made by Railways/ Transport Company	(Rs.)	-	-	-	-	-
14	Demurrage Charges, if any	(Rs.)	67,725	-	-	-	-
15	Cost of diesel in transporting coal through MGR system, if applicable	(Rs.)	-	-	-	-	-
16	Total Transportation Charges (12+13+14+15)	(Rs.)	51,43,36,517	14,91,76,125	-	-	-
17	Total amount Charged for coal supplied including Transportation (11+16)	(Rs.)	1,79,91,48,718	48,00,64,817	-	92,67,75,023	-
E)	**TOTAL COST**						
18	**Landed cost of coal (2+17)/(1+7)**	**Rs./MT**	**4,618**	**3,929**	**-**	**12,762**	**-**
19	Blending Ratio	%	1	0	-	0	-
20	Weighted average cost of coal	Rs./MT					**5,724**
F)	**QUALITY**						
21	GCV of Domestic Coal of the opening stock as per bill of Coal Company	(kCal/Kg)	4,430	4,603			
22	GCV of Domestic Coal supplied as per bill Coal Company	(kCal/Kg)	4,206	3,763			
23	GCV of Imported Coal of the opening stock as per bill of Coal Company	(kCal/Kg)				4,793	
24	GCV of Imported Coal supplied as per bill Coal Company	(kCal/Kg)				4,614	
25	Weighted average GCV of coal/ Lignite as Billed	(kCal/Kg)					**4,337**
26	GCV of Domestic Coal of opening stock as received at Station	(kCal/Kg)	3,779	4,083			
27	GCV of Domestic Coal supplied as received at Station	(kCal/Kg)	3,599	3,567			
28	GCV of Imported Coal of opening stock as received at Station	(kCal/Kg)	-	-	-	4,903	-
29	GCV of Imported Coal supplied as received at Station	(kCal/Kg)	-	-	-	4,764	-
30	**Weighted average GCV of coal/ Lignite as Received**	**(kCal/Kg)**					**3,834**

(Petitioner)

Details of Source wise Fuel for Computation of Energy Charges							PART-I FORM- 15
Name of the Company :			NTPC Limited				
Name of the Power Station :			Tanda Super Thermal Power Station Stage-I				
S. No.	Particulars	Unit	Dec-23				
			Domestic Coal-FSA	Domestic Coal-NTPC Mines	E-Auction Coal	Imported Coal	Bio-Mass
A)	**OPENING QUANTITY**						
1	Opening Quantity of Coal/ Lignite	(MT)	2,64,558	1,34,530	-	4,794	-
2	Value of Stock	(Rs.)	1,18,64,70,242	61,78,29,364	-	6,11,76,888	-
B)	**QUANTITY**						
3	Quantity of Coal supplied by Coal Company	(MT)	3,25,961	3,89,891	-	81,240	-
4	Adjustment (+/-) in quantity supplied made by Coal Company	(MT)	-	-8,799	-	-	-
5	Coal supplied by Coal Company (3+4)	(MT)	3,25,961	3,81,092	-	81,240	-
6	Normative Transit & Handling Losses	(MT)	2,608	3,119	-	162	-
7	Net coal / Lignite Supplied (5-6)	(MT)	3,23,354	3,77,973	-	81,078	-
C)	**PRICE**						
8	Amount charged by the Coal Company	(Rs.)	91,16,80,500	1,03,79,37,938	-	1,10,52,47,846	-
9	Adjustment (+/-) in amount charged made by Coal Company	(Rs.)	6,09,82,798	-2,20,95,157	-	-1,67,95,374	-
10	Handling, Sampling and such other similar charges	(Rs.)	1,14,47,450	1,21,33,363	-	25,28,192	-
11	Total amount Charged (8+9+10)	(Rs.)	98,41,10,748	1,02,79,76,143	-	1,09,09,80,664	-
D)	**TRANSPORATION**						
12	Transportation charges by rail ship, road transport	(Rs.)	36,97,15,702	47,35,18,930	-	-	-
13	Adjustment (+/-) in amount charged made by Railways/ Transport Company	(Rs.)	-	-	-	-	-
14	Demurrage Charges, if any	(Rs.)	92,454	-	-	-	-
15	Cost of diesel in transporting coal through MGR system, if applicable	(Rs.)	-	-	-	-	-
16	Total Transportation Charges (12+13+14+15)	(Rs.)	36,96,23,248	47,35,18,930	-	-	-
17	Total amount Charged for coal supplied including Transportation (11+16)	(Rs.)	1,35,37,33,997	1,50,14,95,074	-	1,09,09,80,664	-
E)	**TOTAL COST**						
18	**Landed cost of coal (2+17)/(1+7)**	**Rs./MT**	**4,321**	**4,135**	**-**	**13,417**	**-**
19	Blending Ratio	%	1	0	-	0	-
20	Weighted average cost of coal	Rs./MT					**6,107**
F)	**QUALITY**						
21	GCV of Domestic Coal of the opening stock as per bill of Coal Company	(kCal/Kg)	4,294	4,223			
22	GCV of Domestic Coal supplied as per bill Coal Company	(kCal/Kg)	3,959	4,051			
23	GCV of Imported Coal of the opening stock as per bill of Coal Company	(kCal/Kg)				4,625	
24	GCV of Imported Coal supplied as per bill Coal Company	(kCal/Kg)				4,632	
25	Weighted average GCV of coal/ Lignite as Billed	(kCal/Kg)					**4,212**
26	GCV of Domestic Coal of opening stock as received at Station	(kCal/Kg)	3,761	4,001			
27	GCV of Domestic Coal supplied as received at Station	(kCal/Kg)	3,487	3,728			
28	GCV of Imported Coal of opening stock as received at Station	(kCal/Kg)	-	-	-	4,772	-
29	GCV of Imported Coal supplied as received at Station	(kCal/Kg)	-	-	-	4,849	-
30	**Weighted average GCV of coal/ Lignite as Received**	**(kCal/Kg)**					**3,874**

(Petitioner)

Details of Source wise Fuel for Computation of Energy Charges							PART-I FORM- 15
Name of the Company :			NTPC Limited				
Name of the Power Station :			Tanda Super Thermal Power Station Stage-I				
S. No.	Particulars	Unit	Jan-24				
			Domestic Coal-FSA	Domestic Coal-NTPC Mines	E-Auction Coal	Imported Coal	Bio-Mass
A)	**OPENING QUANTITY**						
1	Opening Quantity of Coal/ Lignite	(MT)	1,69,761	4,01,530	-	11,733	-
2	Value of Stock	(Rs.)	73,34,90,014	1,66,04,27,585	-	15,74,30,224	-
B)	**QUANTITY**						
3	Quantity of Coal supplied by Coal Company	(MT)	4,38,552	1,95,038	-	1,05,835	-
4	Adjustment (+/-) in quantity supplied made by Coal Company	(MT)	-	-7,924	-	-	-
5	Coal supplied by Coal Company (3+4)	(MT)	4,38,552	1,87,113	-	1,05,835	-
6	Normative Transit & Handling Losses	(MT)	3,508	1,497	-	212	-
7	Net coal / Lignite Supplied (5-6)	(MT)	4,35,044	1,85,616	-	1,05,623	-
C)	**PRICE**						
8	Amount charged by the Coal Company	(Rs.)	1,34,13,38,526	53,63,93,236	-	1,50,21,49,957	-
9	Adjustment (+/-) in amount charged made by Coal Company	(Rs.)	2,98,35,335	-1,98,74,423	-	-	-
10	Handling, Sampling and such other similar charges	(Rs.)	1,50,96,858	67,24,121	-	36,48,756	-
11	Total amount Charged (8+9+10)	(Rs.)	1,38,62,70,720	52,32,42,933	-	1,50,57,98,713	-
D)	**TRANSPORATION**						
12	Transportation charges by rail ship, road transport	(Rs.)	60,62,79,320	22,25,98,609	-	-	-
13	Adjustment (+/-) in amount charged made by Railways/ Transport Company	(Rs.)	-	-	-	-	-
14	Demurrage Charges, if any	(Rs.)	2,08,846	-	-	-	-
15	Cost of diesel in transporting coal through MGR system, if applicable	(Rs.)	-	-	-	-	-
16	Total Transportation Charges (12+13+14+15)	(Rs.)	60,60,70,474	22,25,98,609	-	-	-
17	Total amount Charged for coal supplied including Transportation (11+16)	(Rs.)	1,99,23,41,194	74,58,41,542	-	1,50,57,98,713	-
E)	**TOTAL COST**						
18	**Landed cost of coal (2+17)/(1+7)**	**Rs./MT**	**4,507**	**4,098**	**-**	**14,172**	**-**
19	Blending Ratio	%	1	0	-	0	-
20	Weighted average cost of coal	Rs./MT					**6,313**
F)	**QUALITY**						
21	GCV of Domestic Coal of the opening stock as per bill of Coal Company	(kCal/Kg)	4,105	4,102			
22	GCV of Domestic Coal supplied as per bill Coal Company	(kCal/Kg)	4,251	4,269			
23	GCV of Imported Coal of the opening stock as per bill of Coal Company	(kCal/Kg)				4,632	
24	GCV of Imported Coal supplied as per bill Coal Company	(kCal/Kg)				4,635	
25	Weighted average GCV of coal/ Lignite as Billed	(kCal/Kg)					**4,279**
26	GCV of Domestic Coal of opening stock as received at Station	(kCal/Kg)	3,620	3,843			
27	GCV of Domestic Coal supplied as received at Station	(kCal/Kg)	3,516	3,715			
28	GCV of Imported Coal of opening stock as received at Station	(kCal/Kg)	-	-	-	4,887	-
29	GCV of Imported Coal supplied as received at Station	(kCal/Kg)	-	-	-	4,831	-
30	**Weighted average GCV of coal/ Lignite as Received**	**(kCal/Kg)**					**3,876**

(Petitioner)

Details of Source wise Fuel for Computation of Energy Charges							PART-I FORM- 15
Name of the Company :			NTPC Limited				
Name of the Power Station :			Tanda Super Thermal Power Station Stage-I				
S. No.	Particulars	Unit	Feb-24				
			Domestic Coal-FSA	Domestic Coal-NTPC Mines	E-Auction Coal	Imported Coal	Bio-Mass
A)	**OPENING QUANTITY**						
1	Opening Quantity of Coal/ Lignite	(MT)	3,31,989	4,27,149	-	46,946	-
2	Value of Stock	(Rs.)	1,49,62,59,863	1,75,05,58,604	-	66,53,34,039	-
B)	**QUANTITY**						
3	Quantity of Coal supplied by Coal Company	(MT)	4,27,290	1,74,661	-	16,333	-
4	Adjustment (+/-) in quantity supplied made by Coal Company	(MT)	-	-3,201	-	-	-
5	Coal supplied by Coal Company (3+4)	(MT)	4,27,290	1,71,460	-	16,333	-
6	Normative Transit & Handling Losses	(MT)	3,418	1,372	-	33	-
7	Net coal / Lignite Supplied (5-6)	(MT)	4,23,872	1,70,088	-	16,300	-
C)	**PRICE**						
8	Amount charged by the Coal Company	(Rs.)	1,36,04,52,008	45,18,56,373	-	23,21,10,457	-
9	Adjustment (+/-) in amount charged made by Coal Company	(Rs.)	19,12,508	-78,49,445	-	-3,68,07,697	-
10	Handling, Sampling and such other similar charges	(Rs.)	1,65,65,951	60,24,059	-	5,63,311	-
11	Total amount Charged (8+9+10)	(Rs.)	1,37,89,30,467	45,00,30,987	-	19,58,66,071	-
D)	**TRANSPORATION**						
12	Transportation charges by rail ship, road transport	(Rs.)	61,75,51,154	23,25,49,203	-	-	-
13	Adjustment (+/-) in amount charged made by Railways/ Transport Company	(Rs.)	-	-	-	-	-
14	Demurrage Charges, if any	(Rs.)	2,27,432	-	-	-	-
15	Cost of diesel in transporting coal through MGR system, if applicable	(Rs.)	-	-	-	-	-
16	Total Transportation Charges (12+13+14+15)	(Rs.)	61,73,23,722	23,25,49,203	-	-	-
17	Total amount Charged for coal supplied including Transportation (11+16)	(Rs.)	1,99,62,54,189	68,25,80,190	-	19,58,66,071	-
E)	**TOTAL COST**						
18	**Landed cost of coal (2+17)/(1+7)**	**Rs./MT**	**4,621**	**4,074**	**-**	**13,617**	**-**
19	Blending Ratio	%	1	0	-	0	-
20	Weighted average cost of coal	Rs./MT					**6,079**
F)	**QUALITY**						
21	GCV of Domestic Coal of the opening stock as per bill of Coal Company	(kCal/Kg)	4,214	4,152			
22	GCV of Domestic Coal supplied as per bill Coal Company	(kCal/Kg)	3,902	4,151			
23	GCV of Imported Coal of the opening stock as per bill of Coal Company	(kCal/Kg)				4,635	
24	GCV of Imported Coal supplied as per bill Coal Company	(kCal/Kg)				4,901	
25	Weighted average GCV of coal/ Lignite as Billed	(kCal/Kg)					**4,192**
26	GCV of Domestic Coal of opening stock as received at Station	(kCal/Kg)	3,639	3,843			
27	GCV of Domestic Coal supplied as received at Station	(kCal/Kg)	3,131	3,555			
28	GCV of Imported Coal of opening stock as received at Station	(kCal/Kg)	-	-	-	4,924	-
29	GCV of Imported Coal supplied as received at Station	(kCal/Kg)	-	-	-	4,964	-
30	**Weighted average GCV of coal/ Lignite as Received**	**(kCal/Kg)**					**3,759**

(Petitioner)

Details of Source wise Fuel for Computation of Energy Charges							PART-I FORM- 15
Name of the Company :			NTPC Limited				
Name of the Power Station :			Tanda Super Thermal Power Station Stage-I				
S. No.	Particulars	Unit	Mar-24				
			Domestic Coal-FSA	Domestic Coal-NTPC Mines	E-Auction Coal	Imported Coal	Bio-Mass
A)	**OPENING QUANTITY**						
1	Opening Quantity of Coal/ Lignite	(MT)	4,38,732	4,01,270	-	5,235	-
2	Value of Stock	(Rs.)	2,02,71,94,454	1,63,47,71,000	-	7,12,78,187	-
B)	**QUANTITY**						
3	Quantity of Coal supplied by Coal Company	(MT)	5,51,675	1,40,572	-	-	350
4	Adjustment (+/-) in quantity supplied made by Coal Company	(MT)	-	-2,543	-	-	-
5	Coal supplied by Coal Company (3+4)	(MT)	5,51,675	1,38,029	-	-	350
6	Normative Transit & Handling Losses	(MT)	4,413	1,104	-	-	-
7	Net coal / Lignite Supplied (5-6)	(MT)	5,47,262	1,36,925	-	-	350
C)	**PRICE**						
8	Amount charged by the Coal Company	(Rs.)	2,08,61,25,292	33,28,08,265	-	-	40,68,565
9	Adjustment (+/-) in amount charged made by Coal Company	(Rs.)	39,81,855	-64,02,571	-	-12,52,724	-
10	Handling, Sampling and such other similar charges	(Rs.)	3,21,42,112	81,90,125	-	-	20,417
11	Total amount Charged (8+9+10)	(Rs.)	2,12,22,49,259	33,45,95,819	-	-12,52,724	40,88,982
D)	**TRANSPORATION**						
12	Transportation charges by rail ship, road transport	(Rs.)	77,14,41,942	22,46,33,383	-	-	-
13	Adjustment (+/-) in amount charged made by Railways/ Transport Company	(Rs.)	-	-	-	-	-
14	Demurrage Charges, if any	(Rs.)	3,47,292	-	-	-	-
15	Cost of diesel in transporting coal through MGR system, if applicable	(Rs.)	-	-	-	-	-
16	Total Transportation Charges (12+13+14+15)	(Rs.)	77,10,94,650	22,46,33,383	-	-	-
17	Total amount Charged for coal supplied including Transportation (11+16)	(Rs.)	2,89,33,43,909	55,92,29,202	-	-12,52,724	40,88,982
E)	**TOTAL COST**						
18	**Landed cost of coal (2+17)/(1+7)**	**Rs./MT**	**4,990**	**4,077**	**-**	**13,377**	**11,668**
19	Blending Ratio	%	1	-	-	0	0
20	Weighted average cost of coal	Rs./MT					**5,788**
F)	**QUALITY**						
21	GCV of Domestic Coal of the opening stock as per bill of Coal Company	(kCal/Kg)	4,036	4,152			
22	GCV of Domestic Coal supplied as per bill Coal Company	(kCal/Kg)	4,601	3,783			3,410
23	GCV of Imported Coal of the opening stock as per bill of Coal Company	(kCal/Kg)				4,706	
24	GCV of Imported Coal supplied as per bill Coal Company	(kCal/Kg)					
25	Weighted average GCV of coal/ Lignite as Billed	(kCal/Kg)					**4,375**
26	GCV of Domestic Coal of opening stock as received at Station	(kCal/Kg)	3,406	3,776			
27	GCV of Domestic Coal supplied as received at Station	(kCal/Kg)	3,731	3,624			3,410
28	GCV of Imported Coal of opening stock as received at Station	(kCal/Kg)	-	-	-	4,935	-
29	GCV of Imported Coal supplied as received at Station	(kCal/Kg)	-	-	-		-
30	**Weighted average GCV of coal/ Lignite as Received**	**(kCal/Kg)**					**3,707**

Signature Not Verified
Digitally signed by PARIMAL PIYUSH
Date: 2024.11.25 22:55:12 IST
Reason: AGM(Commercial)
Location: NTPC Limited

(Petitioner)

PART-I
FORM- 15A

Details of Secondary Fuel for Computation of Energy Charges

Name of the Company	**NTPC Limited**
Name of the Power Station	**Tanda Super Thermal Power Station Stage-I**

Amount in Rs

Sl.No.	Month	Unit	Apr-23	
			HFO	LDO
1	Opening Quantity of Oil	KL	0	4,980.13
2	Value of Opening	(Rs)	-	43,49,02,434.45
3	Quantity of Oil supplied by Oil Company	KL	-	3,034.91
4	Adjustment (+/-) in quantity supplied made by Oil Company	KL		
5	**Oil supplied by oil company (3+4)**	KL	**-**	**3,034.91**
6	Normative Transit & Handling Losses	KL	-	
7	Net Oil Supplied (5-6)	KL	-	3,034.91
8	Amount charged by the Oil Company	(Rs)	-	23,06,12,622.00
9	Adjustment(+/-) in amount charged made by Oil Company	(Rs)	-	
10	Handling, Sampling and such other Similar Charges	(Rs)	-	
11	**Total amount charged (8+9+10)**	(Rs)	**-**	**23,06,12,622.00**
12	Transportation charges by rail / ship / road transport			
	By Rail	(Rs)	-	
	By Road	(Rs)	-	
	By Ship	(Rs)	-	
13	Adjustment (+/-) in amount charged made by Railways/Transport Company	(Rs)	-	
14	Demurrage Charges, if any	(Rs)	-	
15	Cost of diesel in transporting Oil through MGR system, if applicable	(Rs)	-	
16	Total Transportation Charges (12+/-13-14+15)	(Rs)	-	-
17	**Total amount Charged for fuel supplied including Transportation (11+16)**	(Rs)	**-**	**23,06,12,622.00**
18	Landed Cost of Oil (LDO/HFO) (2+17)/(1+7)	(Rs)		83,033.31
19	Blending Ratio		-	100%
20	Weighted average cost of Secondary Fuel/ For Month	(kCal/Ltr)	83033.31	
21	GCV of Oil of the Opening stock as per bill of Oil company	(kCal/Ltr)		
22	GCV of oil supplied as per bill of oil company	(kCal/Ltr)		
23	GCV if Imported coal of the opening stock as per bill of Oil company	(kCal/Ltr)		
24	GCV of Imported Oil supplied as per bill of coal company	(kCal/Ltr)		
25	Weighted average GCV if Oil as billed	(kCal/Ltr)		
26	GCV of Oil of the Opening stock as received at station	(kCal/Ltr)		
27	GCV of Oil supplied	(kCal/Ltr)		
28	GCV of Imported coal of the Opening stock as received at station	(kCal/Ltr)		
29	GCV of Imported coal supplied as received at station	(kCal/Ltr)		
30	Weighted Average GCV of Secondary Fuel/ as recevied	(kCal/Ltr)	9380.00	

PETITIONER

			PART-I FORM- 15A	
Details of Secondary Fuel for Computation of Energy Charges				
Name of the Company			**NTPC Limited**	
Name of the Power Station			**Tanda Super Thermal Power Station Stage-I**	
			Amount in Rs	
Sl.No.	**Month**	Unit	**May-23**	
			HFO	**LDO**
1	Opening Quantity of Oil	KL		7,470.037
2	Value of Opening	(Rs)		62,02,61,901.958
3	Quantity of Oil supplied by Oil Company	KL		-
4	Adjustment (+/-) in quantity supplied made by Oil Company	KL		
5	**Oil supplied by oil company (3+4)**	KL		**-**
6	Normative Transit & Handling Losses	KL		
7	Net Oil Supplied (5-6)	KL		-
8	Amount charged by the Oil Company	(Rs)		-
9	Adjustment(+/-) in amount charged made by Oil Company	(Rs)		
10	Handling, Sampling and such other Similar Charges	(Rs)		
11	**Total amount charged (8+9+10)**	(Rs)		**-**
12	Transportation charges by rail / ship / road transport			
	By Rail	(Rs)		
	By Road	(Rs)		
	By Ship	(Rs)		
13	Adjustment (+/-) in amount charged made by Railways/Transport Company	(Rs)		
14	Demurrage Charges, if any	(Rs)		
15	Cost of diesel in transporting Oil through MGR system, if applicable	(Rs)		
16	Total Transportation Charges (12+/-13-14+15)	(Rs)	-	-
17	**Total amount Charged for fuel supplied including Transportation (11+16)**	(Rs)	**-**	**-**
18	Landed Cost of Oil (LDO/HFO) (2+17)/(1+7)	(Rs)		83,033.31
19	Blending Ratio		-	100%
20	Weighted average cost of Secondary Fuel/ For Month	(kCal/Ltr)	83033.31	
21	GCV of Oil of the Opening stock as per bill of Oil company	(kCal/Ltr)		
22	GCV of oil supplied as per bill of oil company	(kCal/Ltr)		
23	GCV if Imported coal of the opening stock as per bill of Oil company	(kCal/Ltr)		
24	GCV of Imported Oil supplied as per bill of coal company	(kCal/Ltr)		
25	Weighted average GCV if Oil as billed	(kCal/Ltr)		
26	GCV of Oil of the Opening stock as received at station	(kCal/Ltr)		
27	GCV of Oil supplied	(kCal/Ltr)		
28	GCV of Imported coal of the Opening stock as received at station	(kCal/Ltr)		
29	GCV of Imported coal supplied as received at station	(kCal/Ltr)		
30	Weighted Average GCV of Secondary Fuel/ as recevied	(kCal/Ltr)	9380.00	

PETITIONER

			PART-I FORM- 15A	
Details of Secondary Fuel for Computation of Energy Charges				
Name of the Company			**NTPC Limited**	
Name of the Power Station			**Tanda Super Thermal Power Station Stage-I**	
			Amount in Rs	
Sl.No.	**Month**	Unit	**Jun-23**	
			HFO	**LDO**
1	Opening Quantity of Oil	KL		6,404.04
2	Value of Opening	(Rs)		53,17,48,392.43
3	Quantity of Oil supplied by Oil Company	KL	-	-
4	Adjustment (+/-) in quantity supplied made by Oil Company	KL		
5	**Oil supplied by oil company (3+4)**	KL	**-**	**-**
6	Normative Transit & Handling Losses	KL	-	
7	Net Oil Supplied (5-6)	KL	-	-
8	Amount charged by the Oil Company	(Rs)	-	-
9	Adjustment(+/-) in amount charged made by Oil Company	(Rs)		
10	Handling, Sampling and such other Similar Charges	(Rs)		
11	**Total amount charged (8+9+10)**	(Rs)	**-**	**-**
12	Transportation charges by rail / ship / road transport			
	By Rail	(Rs)		
	By Road	(Rs)		
	By Ship	(Rs)		
13	Adjustment (+/-) in amount charged made by Railways/Transport Company	(Rs)		
14	Demurrage Charges, if any	(Rs)		
15	Cost of diesel in transporting Oil through MGR system, if applicable	(Rs)		
16	Total Transportation Charges (12+/-13-14+15)	(Rs)	-	-
17	**Total amount Charged for fuel supplied including Transportation (11+16)**	(Rs)	**-**	**-**
18	Landed Cost of Oil (LDO/HFO) (2+17)/(1+7)	(Rs)		83,033.31
19	Blending Ratio		-	100%
20	Weighted average cost of Secondary Fuel/ For Month	(kCal/Ltr)	83033.31	
21	GCV of Oil of the Opening stock as per bill of Oil company	(kCal/Ltr)		
22	GCV of oil supplied as per bill of oil company	(kCal/Ltr)		
23	GCV if Imported coal of the opening stock as per bill of Oil company	(kCal/Ltr)		
24	GCV of Imported Oil supplied as per bill of coal company	(kCal/Ltr)		
25	Weighted average GCV if Oil as billed	(kCal/Ltr)		
26	GCV of Oil of the Opening stock as received at station	(kCal/Ltr)		
27	GCV of Oil supplied	(kCal/Ltr)		
28	GCV of Imported coal of the Opening stock as received at station	(kCal/Ltr)		
29	GCV of Imported coal supplied as received at station	(kCal/Ltr)		
30	Weighted Average GCV of Secondary Fuel/ as recevied	(kCal/Ltr)	9380.00	

PETITIONER

PART-I
FORM- 15A

Details of Secondary Fuel for Computation of Energy Charges

Name of the Company	**NTPC Limited**
Name of the Power Station	**Tanda Super Thermal Power Station Stage-I**

Amount in Rs

Sl.No.	Month	Unit	Jul-23	
			HFO	LDO
1	Opening Quantity of Oil	KL		5,933.04
2	Value of Opening	(Rs)		49,26,39,703.42
3	Quantity of Oil supplied by Oil Company	KL	-	-
4	Adjustment (+/-) in quantity supplied made by Oil Company	KL		
5	**Oil supplied by oil company (3+4)**	KL	**-**	**-**
6	Normative Transit & Handling Losses	KL	-	
7	Net Oil Supplied (5-6)	KL	-	-
8	Amount charged by the Oil Company	(Rs)	-	-
9	Adjustment(+/-) in amount charged made by Oil Company	(Rs)		
10	Handling, Sampling and such other Similar Charges	(Rs)		
11	**Total amount charged (8+9+10)**	(Rs)	**-**	**-**
12	Transportation charges by rail / ship / road transport			
	By Rail	(Rs)		
	By Road	(Rs)		
	By Ship	(Rs)		
13	Adjustment (+/-) in amount charged made by Railways/Transport Company	(Rs)		
14	Demurrage Charges, if any	(Rs)		
15	Cost of diesel in transporting Oil through MGR system, if applicable	(Rs)		
16	Total Transportation Charges (12+/-13-14+15)	(Rs)	-	-
17	**Total amount Charged for fuel supplied including Transportation (11+16)**	(Rs)	**-**	**-**
18	Landed Cost of Oil (LDO/HFO) (2+17)/(1+7)	(Rs)		83,033.31
19	Blending Ratio		-	100%
20	Weighted average cost of Secondary Fuel/ For Month	(kCal/Ltr)	83033.31	
21	GCV of Oil of the Opening stock as per bill of Oil company	(kCal/Ltr)		
22	GCV of oil supplied as per bill of oil company	(kCal/Ltr)		
23	GCV if Imported coal of the opening stock as per bill of Oil company	(kCal/Ltr)		
24	GCV of Imported Oil supplied as per bill of coal company	(kCal/Ltr)		
25	Weighted average GCV if Oil as billed	(kCal/Ltr)		
26	GCV of Oil of the Opening stock as received at station	(kCal/Ltr)		
27	GCV of Oil supplied	(kCal/Ltr)		
28	GCV of Imported coal of the Opening stock as received at station	(kCal/Ltr)		
29	GCV of Imported coal supplied as received at station	(kCal/Ltr)		
30	Weighted Average GCV of Secondary Fuel/ as recevied	(kCal/Ltr)	9380.00	

PETITIONER

			PART-I FORM- 15A	
Details of Secondary Fuel for Computation of Energy Charges				
Name of the Company			**NTPC Limited**	
Name of the Power Station			**Tanda Super Thermal Power Station Stage-I**	
			Amount in Rs	
Sl.No.	**Month**	Unit	**Aug-23**	
			HFO	**LDO**
1	Opening Quantity of Oil	KL		5,442.04
2	Value of Opening	(Rs)		45,18,70,348.21
3	Quantity of Oil supplied by Oil Company	KL		-
4	Adjustment (+/-) in quantity supplied made by Oil Company	KL		
5	**Oil supplied by oil company (3+4)**	KL		**-**
6	Normative Transit & Handling Losses	KL		
7	Net Oil Supplied (5-6)	KL		-
8	Amount charged by the Oil Company	(Rs)		-
9	Adjustment(+/-) in amount charged made by Oil Company	(Rs)		
10	Handling, Sampling and such other Similar Charges	(Rs)		
11	**Total amount charged (8+9+10)**	(Rs)		**-**
12	Transportation charges by rail / ship / road transport			
	By Rail	(Rs)		
	By Road	(Rs)		
	By Ship	(Rs)		
13	Adjustment (+/-) in amount charged made by Railways/Transport Company	(Rs)		
14	Demurrage Charges, if any	(Rs)		
15	Cost of diesel in transporting Oil through MGR system, if applicable	(Rs)		
16	Total Transportation Charges (12+/-13-14+15)	(Rs)	-	-
17	**Total amount Charged for fuel supplied including Transportation (11+16)**	(Rs)	**-**	**-**
18	Landed Cost of Oil (LDO/HFO) (2+17)/(1+7)	(Rs)		83,033.31
19	Blending Ratio		-	100%
20	Weighted average cost of Secondary Fuel/ For Month	(kCal/Ltr)	83033.31	
21	GCV of Oil of the Opening stock as per bill of Oil company	(kCal/Ltr)		
22	GCV of oil supplied as per bill of oil company	(kCal/Ltr)		
23	GCV if Imported coal of the opening stock as per bill of Oil company	(kCal/Ltr)		
24	GCV of Imported Oil supplied as per bill of coal company	(kCal/Ltr)		
25	Weighted average GCV if Oil as billed	(kCal/Ltr)		
26	GCV of Oil of the Opening stock as received at station	(kCal/Ltr)		
27	GCV of Oil supplied	(kCal/Ltr)		
28	GCV of Imported coal of the Opening stock as received at station	(kCal/Ltr)		
29	GCV of Imported coal supplied as received at station	(kCal/Ltr)		
30	Weighted Average GCV of Secondary Fuel/ as recevied	(kCal/Ltr)	9380.00	

PETITIONER

				PART-I **FORM- 15A**
Details of Secondary Fuel for Computation of Energy Charges				
Name of the Company			**NTPC Limited**	
Name of the Power Station			**Tanda Super Thermal Power Station Stage-I**	
				Amount in Rs
Sl.No.	**Month**	Unit	**Sep-23**	
			HFO	**LDO**
1	Opening Quantity of Oil	KL		5,115.04
2	Value of Opening	(Rs)		42,47,18,455.52
3	Quantity of Oil supplied by Oil Company	KL		
4	Adjustment (+/-) in quantity supplied made by Oil Company	KL		
5	**Oil supplied by oil company (3+4)**	KL		**-**
6	Normative Transit & Handling Losses	KL		
7	Net Oil Supplied (5-6)	KL		-
8	Amount charged by the Oil Company	(Rs)		
9	Adjustment(+/-) in amount charged made by Oil Company	(Rs)		6,66,282.00
10	Handling, Sampling and such other Similar Charges	(Rs)		
11	**Total amount charged (8+9+10)**	(Rs)		**6,66,282.00**
12	Transportation charges by rail / ship / road transport			
	By Rail	(Rs)		
	By Road	(Rs)		
	By Ship	(Rs)		
13	Adjustment (+/-) in amount charged made by Railways/Transport Company	(Rs)		
14	Demurrage Charges, if any	(Rs)		
15	Cost of diesel in transporting Oil through MGR system, if applicable	(Rs)		
16	Total Transportation Charges (12+/-13-14+15)	(Rs)	-	-
17	**Total amount Charged for fuel supplied including Transportation (11+16)**	(Rs)	**-**	**6,66,282.00**
18	Landed Cost of Oil (LDO/HFO) (2+17)/(1+7)	(Rs)		83,163.57
19	Blending Ratio		-	100%
20	Weighted average cost of Secondary Fuel/ For Month	(kCal/Ltr)	83163.57	
21	GCV of Oil of the Opening stock as per bill of Oil company	(kCal/Ltr)		
22	GCV of oil supplied as per bill of oil company	(kCal/Ltr)		
23	GCV if Imported coal of the opening stock as per bill of Oil company	(kCal/Ltr)		
24	GCV of Imported Oil supplied as per bill of coal company	(kCal/Ltr)		
25	Weighted average GCV if Oil as billed	(kCal/Ltr)		
26	GCV of Oil of the Opening stock as received at station	(kCal/Ltr)		
27	GCV of Oil supplied	(kCal/Ltr)		
28	GCV of Imported coal of the Opening stock as received at station	(kCal/Ltr)		
29	GCV of Imported coal supplied as received at station	(kCal/Ltr)		
30	Weighted Average GCV of Secondary Fuel/ as recevied	(kCal/Ltr)	9380.00	

PETITIONER

			PART-I FORM- 15A	
Details of Secondary Fuel for Computation of Energy Charges				
Name of the Company			**NTPC Limited**	
Name of the Power Station			**Tanda Super Thermal Power Station Stage-I**	
			Amount in Rs	
Sl.No.	**Month**	Unit	**Oct-23**	
			HFO	**LDO**
1	Opening Quantity of Oil	KL		4,762.04
2	Value of Opening	(Rs)		39,60,27,997.31
3	Quantity of Oil supplied by Oil Company	KL	-	-
4	Adjustment (+/-) in quantity supplied made by Oil Company	KL		
5	**Oil supplied by oil company (3+4)**	KL	**-**	**-**
6	Normative Transit & Handling Losses	KL	-	
7	Net Oil Supplied (5-6)	KL	-	-
8	Amount charged by the Oil Company	(Rs)	-	-
9	Adjustment(+/-) in amount charged made by Oil Company	(Rs)		
10	Handling, Sampling and such other Similar Charges	(Rs)		
11	**Total amount charged (8+9+10)**	(Rs)	**-**	**-**
12	Transportation charges by rail / ship / road transport			
	By Rail	(Rs)		
	By Road	(Rs)		
	By Ship	(Rs)		
13	Adjustment (+/-) in amount charged made by Railways/Transport Company	(Rs)		
14	Demurrage Charges, if any	(Rs)		
15	Cost of diesel in transporting Oil through MGR system, if applicable	(Rs)		
16	Total Transportation Charges (12+/-13-14+15)	(Rs)	-	-
17	**Total amount Charged for fuel supplied including Transportation (11+16)**	(Rs)	**-**	**-**
18	Landed Cost of Oil (LDO/HFO) (2+17)/(1+7)	(Rs)		83,163.57
19	Blending Ratio		-	100%
20	Weighted average cost of Secondary Fuel/ For Month	(kCal/Ltr)	83163.57	
21	GCV of Oil of the Opening stock as per bill of Oil company	(kCal/Ltr)		
22	GCV of oil supplied as per bill of oil company	(kCal/Ltr)		
23	GCV if Imported coal of the opening stock as per bill of Oil company	(kCal/Ltr)		
24	GCV of Imported Oil supplied as per bill of coal company	(kCal/Ltr)		
25	Weighted average GCV if Oil as billed	(kCal/Ltr)		
26	GCV of Oil of the Opening stock as received at station	(kCal/Ltr)		
27	GCV of Oil supplied	(kCal/Ltr)		
28	GCV of Imported coal of the Opening stock as received at station	(kCal/Ltr)		
29	GCV of Imported coal supplied as received at station	(kCal/Ltr)		
30	Weighted Average GCV of Secondary Fuel/ as recevied	(kCal/Ltr)	9380.00	

PETITIONER

			PART-I FORM- 15A	
Details of Secondary Fuel for Computation of Energy Charges				
Name of the Company			**NTPC Limited**	
Name of the Power Station			**Tanda Super Thermal Power Station Stage-I**	
				Amount in Rs
Sl.No.	**Month**	Unit	**Nov-23**	
			HFO	**LDO**
1	Opening Quantity of Oil	KL		3,400.04
2	Value of Opening	(Rs)		28,27,59,214.97
3	Quantity of Oil supplied by Oil Company	KL	-	-
4	Adjustment (+/-) in quantity supplied made by Oil Company	KL		
5	**Oil supplied by oil company (3+4)**	KL	**-**	**-**
6	Normative Transit & Handling Losses	KL	-	
7	Net Oil Supplied (5-6)	KL	-	-
8	Amount charged by the Oil Company	(Rs)	-	-
9	Adjustment(+/-) in amount charged made by Oil Company	(Rs)		
10	Handling, Sampling and such other Similar Charges	(Rs)		
11	**Total amount charged (8+9+10)**	(Rs)	**-**	**-**
12	Transportation charges by rail / ship / road transport			
	By Rail	(Rs)		
	By Road	(Rs)		
	By Ship	(Rs)		
13	Adjustment (+/-) in amount charged made by Railways/Transport Company	(Rs)		
14	Demurrage Charges, if any	(Rs)		
15	Cost of diesel in transporting Oil through MGR system, if applicable	(Rs)		
16	Total Transportation Charges (12+/-13-14+15)	(Rs)	-	-
17	**Total amount Charged for fuel supplied including Transportation (11+16)**	(Rs)	**-**	**-**
18	Landed Cost of Oil (LDO/HFO) (2+17)/(1+7)	(Rs)		83,163.57
19	Blending Ratio		-	100%
20	Weighted average cost of Secondary Fuel/ For Month	(kCal/Ltr)	83163.57	
21	GCV of Oil of the Opening stock as per bill of Oil company	(kCal/Ltr)		
22	GCV of oil supplied as per bill of oil company	(kCal/Ltr)		
23	GCV if Imported coal of the opening stock as per bill of Oil company	(kCal/Ltr)		
24	GCV of Imported Oil supplied as per bill of coal company	(kCal/Ltr)		
25	Weighted average GCV if Oil as billed	(kCal/Ltr)		
26	GCV of Oil of the Opening stock as received at station	(kCal/Ltr)		
27	GCV of Oil supplied	(kCal/Ltr)		
28	GCV of Imported coal of the Opening stock as received at station	(kCal/Ltr)		
29	GCV of Imported coal supplied as received at station	(kCal/Ltr)		
30	Weighted Average GCV of Secondary Fuel/ as recevied	(kCal/Ltr)	9380.00	

PETITIONER

PART-I
FORM- 15A

Details of Secondary Fuel for Computation of Energy Charges

Name of the Company	**NTPC Limited**
Name of the Power Station	**Tanda Super Thermal Power Station Stage-I**

Amount in Rs

Sl.No.	Month	Unit	Dec-23	
			HFO	LDO
1	Opening Quantity of Oil	KL		2,827.04
2	Value of Opening	(Rs)		23,51,06,489.36
3	Quantity of Oil supplied by Oil Company	KL		3,097.62
4	Adjustment (+/-) in quantity supplied made by Oil Company	KL		
5	**Oil supplied by oil company (3+4)**	KL		**3,097.62**
6	Normative Transit & Handling Losses	KL		
7	Net Oil Supplied (5-6)	KL		3,097.62
8	Amount charged by the Oil Company	(Rs)		27,51,49,937.55
9	Adjustment(+/-) in amount charged made by Oil Company	(Rs)		
10	Handling, Sampling and such other Similar Charges	(Rs)		
11	**Total amount charged (8+9+10)**	(Rs)		**27,51,49,937.55**
12	Transportation charges by rail / ship / road transport			
	By Rail	(Rs)		
	By Road	(Rs)		
	By Ship	(Rs)		
13	Adjustment (+/-) in amount charged made by Railways/Transport Company	(Rs)		
14	Demurrage Charges, if any	(Rs)		
15	Cost of diesel in transporting Oil through MGR system, if applicable	(Rs)		
16	Total Transportation Charges (12+/-13-14+15)	(Rs)	-	-
17	**Total amount Charged for fuel supplied including Transportation (11+16)**	(Rs)	**-**	**27,51,49,937.55**
18	Landed Cost of Oil (LDO/HFO) (2+17)/(1+7)	(Rs)		86,124.214
19	Blending Ratio		-	100%
20	Weighted average cost of Secondary Fuel/ For Month	(kCal/Ltr)	86124.21	
21	GCV of Oil of the Opening stock as per bill of Oil company	(kCal/Ltr)		
22	GCV of oil supplied as per bill of oil company	(kCal/Ltr)		
23	GCV if Imported coal of the opening stock as per bill of Oil company	(kCal/Ltr)		
24	GCV of Imported Oil supplied as per bill of coal company	(kCal/Ltr)		
25	Weighted average GCV if Oil as billed	(kCal/Ltr)		
26	GCV of Oil of the Opening stock as received at station	(kCal/Ltr)		
27	GCV of Oil supplied	(kCal/Ltr)		
28	GCV of Imported coal of the Opening stock as received at station	(kCal/Ltr)		
29	GCV of Imported coal supplied as received at station	(kCal/Ltr)		
30	Weighted Average GCV of Secondary Fuel/ as recevied	(kCal/Ltr)	9380.00	

PETITIONER

PART-I
FORM- 15A

Details of Secondary Fuel for Computation of Energy Charges

Name of the Company	**NTPC Limited**
Name of the Power Station	**Tanda Super Thermal Power Station Stage-I**

Amount in Rs

Sl.No.	Month	Unit	Jan-24	
			HFO	LDO
1	Opening Quantity of Oil	KL		5,540.66
2	Value of Opening	(Rs)		47,71,84,728.73
3	Quantity of Oil supplied by Oil Company	KL		-
4	Adjustment (+/-) in quantity supplied made by Oil Company	KL		
5	**Oil supplied by oil company (3+4)**	KL		**-**
6	Normative Transit & Handling Losses	KL		
7	Net Oil Supplied (5-6)	KL		-
8	Amount charged by the Oil Company	(Rs)		-
9	Adjustment(+/-) in amount charged made by Oil Company	(Rs)		-2,88,62,688.55
10	Handling, Sampling and such other Similar Charges	(Rs)		
11	**Total amount charged (8+9+10)**	(Rs)		**-2,88,62,688.55**
12	Transportation charges by rail / ship / road transport			
	By Rail	(Rs)		
	By Road	(Rs)		
	By Ship	(Rs)		
13	Adjustment (+/-) in amount charged made by Railways/Transport Company	(Rs)		
14	Demurrage Charges, if any	(Rs)		
15	Cost of diesel in transporting Oil through MGR system, if applicable	(Rs)		
16	Total Transportation Charges (12+/-13-14+15)	(Rs)	-	-
17	**Total amount Charged for fuel supplied including Transportation (11+16)**	(Rs)	**-**	**-2,88,62,688.55**
18	Landed Cost of Oil (LDO/HFO) (2+17)/(1+7)	(Rs)		80,914.96
19	Blending Ratio		-	100%
20	Weighted average cost of Secondary Fuel/ For Month	(kCal/Ltr)		80914.96
21	GCV of Oil of the Opening stock as per bill of Oil company	(kCal/Ltr)		
22	GCV of oil supplied as per bill of oil company	(kCal/Ltr)		
23	GCV if Imported coal of the opening stock as per bill of Oil company	(kCal/Ltr)		
24	GCV of Imported Oil supplied as per bill of coal company	(kCal/Ltr)		
25	Weighted average GCV if Oil as billed	(kCal/Ltr)		
26	GCV of Oil of the Opening stock as received at station	(kCal/Ltr)		
27	GCV of Oil supplied	(kCal/Ltr)		
28	GCV of Imported coal of the Opening stock as received at station	(kCal/Ltr)		
29	GCV of Imported coal supplied as received at station	(kCal/Ltr)		
30	Weighted Average GCV of Secondary Fuel/ as recevied	(kCal/Ltr)		9380.00

PETITIONER

			PART-I FORM- 15A	
Details of Secondary Fuel for Computation of Energy Charges				
Name of the Company			**NTPC Limited**	
Name of the Power Station			**Tanda Super Thermal Power Station Stage-I**	
			Amount in Rs	
Sl.No.	**Month**	Unit	**Feb-24**	
			HFO	**LDO**
1	Opening Quantity of Oil	KL		4,906.66
2	Value of Opening	(Rs)		39,70,21,955.54
3	Quantity of Oil supplied by Oil Company	KL	-	-
4	Adjustment (+/-) in quantity supplied made by Oil Company	KL		
5	**Oil supplied by oil company (3+4)**	KL	**-**	**-**
6	Normative Transit & Handling Losses	KL		
7	Net Oil Supplied (5-6)	KL	-	-
8	Amount charged by the Oil Company	(Rs)	-	-
9	Adjustment(+/-) in amount charged made by Oil Company	(Rs)		
10	Handling, Sampling and such other Similar Charges	(Rs)		
11	**Total amount charged (8+9+10)**	(Rs)	**-**	**-**
12	Transportation charges by rail / ship / road transport			
	By Rail	(Rs)		
	By Road	(Rs)		
	By Ship	(Rs)		
13	Adjustment (+/-) in amount charged made by Railways/Transport Company	(Rs)		
14	Demurrage Charges, if any	(Rs)		
15	Cost of diesel in transporting Oil through MGR system, if applicable	(Rs)		
16	Total Transportation Charges (12+/-13-14+15)	(Rs)		-
17	**Total amount Charged for fuel supplied including Transportation (11+16)**	(Rs)	**-**	**-**
18	Landed Cost of Oil (LDO/HFO) (2+17)/(1+7)	(Rs)		80,914.96
19	Blending Ratio		-	100%
20	Weighted average cost of Secondary Fuel/ For Month	(kCal/Ltr)	80914.96	
21	GCV of Oil of the Opening stock as per bill of Oil company	(kCal/Ltr)		
22	GCV of oil supplied as per bill of oil company	(kCal/Ltr)		
23	GCV if Imported coal of the opening stock as per bill of Oil company	(kCal/Ltr)		
24	GCV of Imported Oil supplied as per bill of coal company	(kCal/Ltr)		
25	Weighted average GCV if Oil as billed	(kCal/Ltr)		
26	GCV of Oil of the Opening stock as received at station	(kCal/Ltr)		
27	GCV of Oil supplied	(kCal/Ltr)		
28	GCV of Imported coal of the Opening stock as received at station	(kCal/Ltr)		
29	GCV of Imported coal supplied as received at station	(kCal/Ltr)		
30	Weighted Average GCV of Secondary Fuel/ as recevied	(kCal/Ltr)	9380.00	

PETITIONER

				PART-I **FORM- 15A**
Details of Secondary Fuel for Computation of Energy Charges				
Name of the Company			**NTPC Limited**	
Name of the Power Station			**Tanda Super Thermal Power Station Stage-I**	
				Amount in Rs
Sl.No.	**Month**	Unit	**Mar-24**	
			HFO	**LDO**
1	Opening Quantity of Oil	KL		4,025.66
2	Value of Opening	(Rs)		32,57,35,867.69
3	Quantity of Oil supplied by Oil Company	KL		-
4	Adjustment (+/-) in quantity supplied made by Oil Company	KL		
5	**Oil supplied by oil company (3+4)**	KL		**-**
6	Normative Transit & Handling Losses	KL		
7	Net Oil Supplied (5-6)	KL		-
8	Amount charged by the Oil Company	(Rs)		-
9	Adjustment(+/-) in amount charged made by Oil Company	(Rs)		
10	Handling, Sampling and such other Similar Charges	(Rs)		
11	**Total amount charged (8+9+10)**	(Rs)		**-**
12	Transportation charges by rail / ship / road transport			
	By Rail	(Rs)		
	By Road	(Rs)		
	By Ship	(Rs)		
13	Adjustment (+/-) in amount charged made by Railways/Transport Company	(Rs)		
14	Demurrage Charges, if any	(Rs)		
15	Cost of diesel in transporting Oil through MGR system, if applicable	(Rs)		
16	Total Transportation Charges (12+/-13-14+15)	(Rs)	-	-
17	**Total amount Charged for fuel supplied including Transportation (11+16)**	(Rs)	**-**	**-**
18	Landed Cost of Oil (LDO/HFO) (2+17)/(1+7)	(Rs)		80,914.96
19	Blending Ratio		-	100%
20	Weighted average cost of Secondary Fuel/ For Month	(kCal/Ltr)	80914.96	
21	GCV of Oil of the Opening stock as per bill of Oil company	(kCal/Ltr)		
22	GCV of oil supplied as per bill of oil company	(kCal/Ltr)		
23	GCV if Imported coal of the opening stock as per bill of Oil company	(kCal/Ltr)		
24	GCV of Imported Oil supplied as per bill of coal company	(kCal/Ltr)		
25	Weighted average GCV if Oil as billed	(kCal/Ltr)		
26	GCV of Oil of the Opening stock as received at station	(kCal/Ltr)		
27	GCV of Oil supplied	(kCal/Ltr)		
28	GCV of Imported coal of the Opening stock as received at station	(kCal/Ltr)		
29	GCV of Imported coal supplied as received at station	(kCal/Ltr)		
30	Weighted Average GCV of Secondary Fuel/ as recevied	(kCal/Ltr)	9380.00	

PETITIONER

Computation of Energy Charges

Name of the Company	**NTPC Limited**
Name of the Power Station	**Tanda Super Thermal Power Station Stage-I**

Computation of Energy Charges

				2024-25	2025-26	2026-27	2027-28	2028-29
1	Rate of Energy Charge from Sec. Fuel Oil/ Alternate Fuel (p/kwh)	$(REC)_s$	$= (Q_s)_n \times P_s$	4.140	4.140	4.140	4.140	4.140
2	Heat Contribution from SFO / Alternate Fuel	(H_s)	$= (Qs)_n \times (GCV)_s$	4.690	4.690	4.690	4.690	4.690
3	Heat Contribution from coal	$(H_p)_s$	$= GHR - H_s$	2745.31	2745.31	2745.31	2745.31	2745.31
4	Specific Primary Fuel Consumption	$(Qp)_n$	$= H_p / (GCV)_p$	0.729	0.729	0.729	0.729	0.729
5	Rate of Energy charge from Primary Fuel (p/kwh)	$(REC)_p$		446.692	446.692	446.692	446.692	446.692
6	Rate of Energy charge ex-bus (p/kWh)	(REC)	$= ((REC)_s + (REC)_p / (1-(AUX))$	451.373	451.373	451.373	451.373	451.373

Computation of Energy Charges

NTPC Limited

Tanda Super Thermal Power Station Stage-I

		2024-25	2025-26	2026-27	2027-28	2028-29
No of Days in the period	Days	365	365	365	366	365
No of Days in the year	Days	365	365	365	366	365
Sp. Oil consumption	ml/kwh	0.5	0.5	0.5	0.5	0.5
Auxiliary consumption	%	12.00%	12.00%	12.00%	12.00%	12.00%
Heat Rate	Kcal/Kwh	2,750.00	2,750.00	2,750.00	2,750.00	2,750.00
Computation of Variable Charges						
Variable Charge (Coal)	p/kwh	507.604	507.604	507.604	507.604	507.604
Variable Charge (Oil)	p/kwh	4.704	4.704	4.704	4.704	4.704
Total	p/kwh	512.308	512.308	512.308	512.308	512.308
Price of fuel from Form-15/15A						
Coal Cost	(Rs./MT)	6123.76	6123.76	6123.76	6123.76	6123.76
Oil Cost	(Rs./KL)	82793.86	82793.86	82793.86	82793.86	82793.86
Computation of Fuel Expenses for Calculation of IWC:						
ESO in a year	(MUs)	2883.09	2883.09	2883.09	2890.99	2883.09
ESO for 50 days	(MUs)	394.944	394.944	394.944	394.944	394.944
Cost of coal for 50 Days	**(Rs. Lakh)**	**20047.52**	**20047.52**	**20047.52**	**20047.52**	**20047.52**
Cost of oil for 2 months	**(Rs. Lakh)**	**226.04**	**226.04**	**226.04**	**226.66**	**226.04**
Energy Expenses for 45 days	**(Rs. Lakh)**	**18209.98**	**18209.98**	**18209.98**	**18209.98**	**18209.98**
Coal		**2024-25**	**2025-26**	**2026-27**	**2027-28**	**2028-29**
Wtd. Avg. Price of Coal	Rs./MT	6123.76	6123.76	6123.76	6123.76	6123.76
Wtd. Avg. GCV of Coal as received	kCal/Kg	3848.58	3848.58	3848.58	3848.58	3848.58
Wtd. Avg. GCV of Coal as received after adjustement of 85 kcal/kg	kCal/Kg	**3763.58**	**3763.58**	**3763.58**	**3763.58**	**3763.58**
Sec. Oil						
Wtd. Avg. Price of Secondary Fuel	Rs/KL	82793.86	82793.86	82793.86	82793.86	82793.86
Wtd. Avg. GCV of Secondary Fuel	kCal/L	9380.00	9380.00	9380.00	9380.00	9380.00

PART-I
FORM- L

Statement of Capital cost

Name of the Petitioner	NTPC Limited
Name of the Generating Station	Tanda Super Thermal Power Station Stage-I
COD	14-01-2000
For Financial Year	2024-29

(Rs Lakh)

Sl. No.	Particulars	2024-25			2025-26			2026-27			2027-28			2028-29		
		Accrual Basis	Un-discharged Liabilities	Cash Basis	Accrual Basis	Un-discharged Liabilities	Cash Basis	Accrual Basis	Un-discharged Liabilities	Cash Basis	Accrual Basis	Un-discharged Liabilities	Cash Basis	Accrual Basis	Un-discharged Liabilities	Cash Basis
A	a) Opening Gross Block Amount as per books	1,47,804.53	546.48	1,47,258.05	SHALL BE PROVIDED AT THE TIME OF TRUE-UP.											
	b) Amount of IDC in A(a) above	4,058.92		4,058.92												
	c) Amount of FC in A(a) above	0.00		-												
	d) Amount of FERV in A(a) above	4,120.65		4,120.65												
	e) Amount of Hedging Cost in A(a) above	0.00		-												
	f) Amount of IEDC in A(a) above	0.00		-												
B	a) Addition in Gross Block Amount during the period (Direct purchases)	SHALL BE PROVIDED AT THE TIME OF TRUE-UP.														
	b) Amount of IDC in B(a) above															
	c) Amount of FC in B(a) above															
	d) Amount of FERV in B(a) above															
	e) Amount of Hedging Cost in B(a) above															
	f) Amount of IEDC in B(a) above															
C	a) Addition in Gross Block Amount during the period (Transferred from CWIP)															
	b) Amount of IDC in C(a) above															
	c) Amount of FC in C(a) above															
	d) Amount of FERV in C(a) above															
	e) Amount of Hedging Cost in C(a) above															
	f) Amount of IEDC in C(a) above															
D	a) Deletion in Gross Block Amount during the period															
	b) Amount of IDC in D(a) above															
	c) Amount of FC in D(a) above															
	d) Amount of FERV in D(a) above															
	e) Amount of Hedging Cost in D(a) above															
	f) Amount of IEDC in D(a) above															
E	a) Closing Gross Block Amount as per books															
	b) Amount of IDC in E(a) above															
	c) Amount of FC in E(a) above															
	d) Amount of FERV in E(a) above															
	e) Amount of Hedging Cost in E(a) above															
	f) Amount of IEDC in E(a) above															

Petitioner

Signature Not Verified

Digitally signed by PARIMAL PIYUSH
Date: 2024.11.25 22:55:12 IST
Reason: AGM(Commercial)
Location: NTPC Limited

PART-I
FORM- M

Statement of Capital Works in Progress

Name of the Petitioner	NTPC Limited
Name of the Generating Station	Tanda Super Thermal Power Station Stage-I
COD	14-01-2000
For Financial Year	2024-29

(Amount in Rs Lakh)

Sl. No.	Particulars	2024-25			2025-26			2026-27			2027-28			2028-29		
		Accrual Basis	Un-discharged Liabilities	Cash Basis	Accrual Basis	Un-discharged Liabilities	Cash Basis	Accrual Basis	Un-discharged Liabilities	Cash Basis	Accrual Basis	Un-discharged Liabilities	Cash Basis	Accrual Basis	Un-discharged Liabilities	Cash Basis
A	a) Opening CWIP as per books	2,514.70	249.55	2,265.15	SHALL BE PROVIDED AT THE TIME OF TRUE-UP.											
	b) Amount of IDC in A(a) above	-		-												
	c) Amount of FC in A(a) above	-		-												
	d) Amount of FERV in A(a) above	-		-												
	e) Amount of Hedging Cost in A(a) above	-		-												
	f) Amount of IEDC in A(a) above	-		-												
B	a) Addition in CWIP during the period	SHALL BE PROVIDED AT THE TIME OF TRUE-UP.														
	b) Amount of IDC in B(a) above															
	c) Amount of FC in B(a) above															
	d) Amount of FERV in B(a) above															
	e) Amount of Hedging Cost in B(a) above															
	f) Amount of IEDC in B(a) above															
C	a) Transferred to Gross Block Amount during the															
	b) Amount of IDC in C(a) above															
	c) Amount of FC in C(a) above															
	d) Amount of FERV in C(a) above															
	e) Amount of Hedging Cost in C(a) above															
	f) Amount of IEDC in C(a) above															
D	a) Deletion in CWIP during the period															
	b) Amount of IDC in D(a) above															
	c) Amount of FC in D(a) above															
	d) Amount of FERV in D(a) above															
	e) Amount of Hedging Cost in D(a) above															
	f) Amount of IEDC in D(a) above															
E	a) Closing CWIP as per books															
	b) Amount of IDC in E(a) above															
	c) Amount of FC in E(a) above															
	d) Amount of FERV in E(a) above															
	e) Amount of Hedging Cost in E(a) above															
	f) Amount of IEDC in E(a) above															

Petitioner

PART-I
FORM- N

Calculation of Interest on Normative Loan

Name of the Company :		**NTPC Limited**
Name of the Power Station :		**Tanda Super Thermal Power Station Stage-I**

(Amount in Rs Lakh)

S. No.	Particulars		Existing 2023-24	2024-25	2025-26	2026-27	2027-28	2028-29
1	**2**		**3**	**4**	**5**		**6**	**8**
1	Gross Normative loan – Opening	A	86,951.44	87,327.68	88,173.63	91,016.33	92,936.17	93,027.17
2	Cumulative repayment of Normative loan up to previous year	B	86,951.44	87,327.68	88,173.63	88,466.24	89,107.16	89,914.03
3	**Net Normative loan – Opening**	**C=A-B**	-	-	-	2,550.09	3,829.01	3,113.14
4	Add: Increase due to addition during the year / period	D	561.32	845.95	2,842.70	1,919.85	91.00	-
5	Less: Decrease due to de-capitalisation during the year / period	E	191.25	-	-	-	-	-
6	Less: Decrease due to reversal during the year / period	F		-	-	-	-	-
7	Add: Increase due to discharges during the year / period	G	6.17	-	-	-	-	-
8	Normative Loan Closing	H=C+D-E-F+G	376.23	845.95	2842.70	4469.93	3920.01	3113.14
9	Repayment of Loan during the year	I	376.23	845.95	292.61	640.92	806.87	815.48
10	Repayment adjustment on account of decapitalization	J	0.00	0.00	0.00	0.00	0.00	0.00
11	Net Repayment of loan during the year	K=I-J	376.23	845.95	292.61	640.92	806.87	815.48
12	**Net Normative loan - Closing**	**L=H-K**	-	-	2,550.09	3,829.01	3,113.14	2,297.66
13	**Average Normative loan**	**M=Average(C,L)**	-	-	1,275.04	3,189.55	3,471.08	2,705.40
14	Weighted average rate of interest	N	7.7980%	7.7868%	7.8715%	8.0240%	8.0125%	7.9868%
15	**Interest on Loan**	**O=MxN**	**0.00**	**0.00**	**100.36**	**255.93**	**278.12**	**216.08**
15	Cumulative repayment of Normative loan at the end of the period	P=B+K	87,327.68	88,173.63	88,466.24	89,107.16	89,914.03	90,729.51

(Petitioner)

PART 1
FORM- O

Calculation of Interest on Working Capital

Name of the Company :	**NTPC Limited**
Name of the Power Station :	**Tanda Super Thermal Power Station Stage-I**

(Amount in Rs Lakh)

S. No.	Particulars	Existing 2023-24	2024-25	2025-26	2026-27	2027-28	2028-29
1	2	3	4	5	6	7	8
1	Cost of Coal/Lignite	18,798.11	20047.52	20047.52	20047.52	20047.52	20047.52
2	Cost of Main Secondary Fuel Oil	226.37	226.04	226.04	226.04	226.66	226.04
3	Fuel Cost						
4	Liquid Fuel Stock						
5	O & M Expenses	1,833.18	1824.75	1841.31	1859.07	1878.12	1898.56
6	Maintenance Spares	4,399.63	4379.40	4419.15	4461.77	4507.48	4556.53
7	Receivables	21,897.35	23007.53	22591.80	22706.20	22756.79	22794.92
8	Total Working Capital	47154.64	49485.24	49125.83	49300.60	49416.57	49523.58
9	Rate of Interest	12.00%	11.90%	11.90%	11.90%	11.90%	11.90%
10	**Interest on Working Capital**	**5658.56**	**5888.74**	**5845.97**	**5866.77**	**5880.57**	**5893.31**

Signature Not Verified

Digitally signed by PARIMAL PIYUSH
Date: 2024.11.25 22:55:12 IST
Reason: AGM(Commercial)
Location: NTPC Limited

Summary of issue involved in the petition						PART 1 FORM-T
Name of the Company :		**NTPC Limited**				
Name of the Power Station :		**Tanda Super Thermal Power Station Stage-I**				
1	**Petitioner:**	**NTPC Limited**				
2	**Subject**	**Determination of Tariff for 2024-29 period**				
3	**Prayer:** i)Approve tariff of Tanda Super Thermal Power Station Stage-I (4x110 MW) for the period from 01.04.2024 to 31.03.2029. ii)Allow the recovery of filing fees as & when paid to the Hon'ble Commission and publication expenses from the beneficiaries. iii)Allow reimbursement of Ash Transportation Charges directly from the beneficiaries on monthly basis, subject to true up. iv)Grant liberty to approach the Hon'ble Commission to allow for the recovery of pay/wage revision due in 2024-29 period as additional O&M over and above the normative O&M. v)Pass any other order as it may deem fit in the circumstances mentioned above					
4	**Respondents**					
	Name of Respondents					
	1. Uttar Pradesh Power Corp. Ltd. (UPPCL)					
	2. Rajasthan Urja Vikas Nigam Limited (RUVNL)					
	3. Tata Power Delhi Distribution Limited					
	4. BSES Rajdhani Power Limited.					
	5. BSES Yamuna Power Limited,					
	6. Haryana Power Purchase Centre					
	7. Punjab State Power Corporation Limited,					
	8. Himachal Pradesh State Electricity Board Limited,					
	9. Power Development Department (J&K)					
	10. Electricity Department, Union Territory of Chandigarh					
	11. Uttarakhand Power Corporation Limited.					
5	**Project Scope**					
	Capital Cost as on 01.04.2024 (Rs. Lakh)	**124753.82**				
	Date of Station COD	**14-01-2000**				
	Claim (Rs Lakh)	**2024-25**	**2025-26**	**2026-27**	**2027-28**	**2028-29**
	AFC	38,929.73	35,541.40	36,469.31	36,980.73	37,188.98
	Closing Capital Cost	1,25,962.32	1,30,023.32	1,32,765.96	1,32,895.96	1,32,895.96
	Initial spare	**N/A**				
	NAPAF (Gen)	**85%**				
	Any Specific					

Petitioner

Signature Not Verified

Digitally signed by PARIMAL PIYUSH
Date: 2024.11.25 22:55:12 IST
Reason: AGM(Commercial)
Location: NTPC Limited

ANNEXURE-R1

भारत सरकार
Government of India
विद्युत मंत्रालय
Ministry of Power
केन्द्रीय विद्युत प्राधिकरण
Central Electricity Authority
सूचना प्रौद्योगिकी एवं साइबर सुरक्षा प्रभाग
Information Technology & Cyber Security Division
****

विषय : CEA (Cyber Security in Power Sector) Guidelines, 2021.

CEA is mandated to prepare 'Guidelines on Cyber Security' in Power Sector under the provision of regulation (10) of the Central Electricity Authority (Technical Standards for Connectivity to the Grid) (Amendment) Regulations, 2019. Guidelines on Cyber Security in Power Sector incorporating the cardinal principles has been prepared by CEA. In compliance to the provision of the above regulation, **CEA (Cyber Security in Power Sector) Guidelines, 2021** are issued for compliance by all entities listed in the clause 2.3 (Applicability of the Guidelines) of the guidelines.

Encl: Guidelines on Cyber Security

07/10/21
(V.K Mishra)
Secretary CEA

CEA (Cyber Security in Power Sector) Guidelines, 2021

1.0 Background

1.1 Cyber intrusion attempts and Cyber-attacks in any critical sector are carried out with a malicious intent. In Power Sector it's either to compromise the Power Supply System or to render the grid operation in-secure. Any such compromise, may result in mal-operations of equipments, equipment damages or even in a cascading grid brownout/blackout. The much hyped air gap myth between IT and OT Systems now stands shattered. The artificial air gap created by deploying firewalls between any IT and OT System can be jumped by any insider or an outsider through social engineering. Cyber-attacks are staged through tactics & techniques of Initial Access, Execution, Persistence, Privilege Escalation, Defence Evasion, Command and Control, Exfiltration. After gaining the entry inside the system through privilege escalation, the control of IT network and operations of OT systems can be taken over even remotely by any cyber adversary. The gain of sensitive operational data through such intrusions may help the Nation/State sponsored or non-sponsored adversaries and cyber attackers to design more sinister and advanced cyber-attacks.

1.2 Government of India has set up the Indian Computer Emergency Response Team (CERT-In) for Early Warning and Response to cyber security incidents and to have collaboration at National and International level for information sharing on mitigation of cyber threats. CERT-In regularly issues advisories on safeguarding computer systems and publishes Security Guidelines which are widely circulated for compliances. All Central Government Ministries/ Departments and State/Union Territory Governments have been advised to conduct cyber security audit of their entire Cyber Infrastructure including websites at regular interval through CERT-In empanelled Auditors so as to identify gaps and appropriate corrective actions to be taken in cyber security practices. CERT-In extends supports to enable Responsible Entity in conducting cyber security mock drills and in assessment of their preparation to withstand cyber-attacks. The Responsible Entity must submit Reports of Cyber Audit of cyber security controls, architecture, vulnerability management, network security and periodic cyber security drills to sectoral CERT as well as CERT-In. Team of experts shall review these reports and shortcomings if any in the compliances shall be flagged by them. CERT-In on regular basis also conducts workshops and training programs to enhance Cyber awareness of all Stakeholders.

1.3 Ministry of Power has created 6(six) sectoral CERTs namely Thermal, Hydro, Transmission, Grid Operation, RE and Distribution for ensuring cyber security in Indian Power Sector. Each Sectoral CERT has prepared their sub-sector specific model Cyber Crisis Management Plan(C-CMP) for countering cyber-attacks and cyber terrorism. Each Sectoral CERT has circulated their model C-CMPs for preparation and implementation of organization specific C-CMP by each of their Constituent Utility.

1.4 All Responsible Entities, Service Providers, Equipment Suppliers/Vendors and Consultants engaged in Power Sector are equally responsible for ensuring cyber security of the Indian Power Supply System. They are to act timely upon each threat intelligence,

advisories and other inputs received from authenticated sources, for continuous improvement in their cyber security posture.

1.5 In the current Indian scenario though many cyber security directives and guidelines exists, but none of them are power sector specific. Ministry of Power has directed CEA to prepare Regulation on Cyber Security in Power Sector. And as an interim measures CEA has been directed to issue Guideline on Cyber Security in Power Sector, under the provision of Regulation 10 on Cyber Security in the "Central Electricity Authority (Technical Standards for Connectivity to the Grid) (Amendment) Regulations, 2019".

1.6 The Guidelines on Cyber Security, in the form of Articles written below, requires mandatory Compliance by all Responsible Entities. The Guidelines shall come into effect from the date of issue by Central Electricity Authority, New Delhi.

2.0 Hereby the Guidelines on Cyber Security are drawn in the form of Articles for compliance by the Requester as well as User under the following provision of Regulation 10 on Cyber Security, in the "Central Electricity Authority (Technical Standards for Connectivity to the Grid) (Amendment) Regulations, 2019".

"The requester and the user shall comply with cyber security guidelines issued by the Central Government, from time to time, and the technical standards for communication system in Power Sector laid down by the Authority."

2.1 **Objective of issuing Guideline**:

a) Creating cyber security awareness
b) Creating a secure cyber ecosystem,
c) Creating a cyber-assurance framework,
d) Strengthening the regulatory framework,
e) Creating mechanisms for security threat early warning, vulnerability management and response to security threats,
f) Securing remote operations and services,
g) Protection and resilience of critical information infrastructure,
h) Reducing cyber supply chain risks,
i) Encouraging use of open standards,
j) Promotion of research and development in cyber security,
k) Human resource development in the domain of Cyber Security,
l) Developing effective public private partnerships,
m) Information sharing and cooperation
n) Operationalization of the National Cyber Security Policy

2.2 Within the text of these Articles, '**Responsible Entity'** shall mean all:

a) Transmission Utilities as well as Transmission Licensees,
b) Load despatch centres (State, Regional and National),
c) Generation utilities (Hydro, Thermal, Nuclear, RE),
d) Distribution Utilities
e) Generation Aggregators,
f) Trading Exchanges,
g) Regional Power Committees, and
h) Regulatory Commissions.

2.3 **Applicability:**

All Responsible Entities as well as System Integrators, Equipment Manufacturers, Suppliers/Vendors, Service Providers, IT Hardware and Software OEMs engaged in the Indian Power Supply System.

2.4 **Scope:**

2.4.1 **Control Systems for System Operation and Operation Management.**

a) Grid Control and Management Systems,
b) Power Plant Control Systems,
c) Central Systems used to monitor and control of distributed generation and loads e.g. virtual power plants, storage management, central control rooms for hydroelectric plants, photovoltaic/wind power installations,
d) Systems for fault management and work force management,
e) Metering and measurement management systems,
f) Data archiving systems,
g) Parameterisation, configuration and programming systems,
h) Supporting systems required for operation of the above mentioned systems,

2.4.2 **Communication System.**

a) Routers switches and firewalls,
b) Communication technology-related network components,
c) Wireless digital systems.
d) Control Centre to Control Centre Communications for data exchange on ICCP. **(IEC 61850/60850-5/TASE.2/)**

2.4.3 **Secondary, Automation and Tele control technologies**

a) Control and Automation components,
b) Control and field devices,
c) Tele control devices,
d) Programmable logic controllers / Remote Terminal Units, including digital sensor and actuators elements,
e) Protection devices,
f) Safety components,
g) Digital measurement and metering installations,
h) Synchronisation devices,
i) Excitation Systems,

3.0 Definition of Terms:

1. **Access Management**: shall mean set of policies and procedures of the Responsible Entity for allowing Personnel, devices and IoT to securely perform a broad range of operational, maintenance, and asset management tasks either on site or remotely as laid down in Clause 5.2.5 of IS 16335.
2. **Accreditation:** shall mean the process of verifying that an organisation is capable of conducting the tests and assessments against a product/process that are required to be certified.

3. **Accreditation Body:** shall mean an organisation that has been accredited to verify the credentials and capabilities of the organisations that wish to become a certification body.
4. **Act:** shall mean the Information Technology Act, 2000 (21 of 2000)
5. **Asset**: shall mean anything that has value to the organization.
6. **Certification:** shall mean the process of verifying that a product has been manufactured in conformance with a set of predefined standards and/or regulations by an organisation, that is accredited to conduct the certification process
7. **Certification Body:** shall mean an organisation that has been accredited by an accreditation body to certify products / process against a certification scheme.
8. **Certification Scheme:** shall mean the processes, paperwork, tools, and documentation that define how a product or manufacturer is certified
9. **Chief Information Security Officer:** shall means the designated employee of Senior management level directly reporting to Managing Director/Chief Executive Officer/Secretary of the Responsible Entity, having knowledge of Information Security and related issues, responsible for cyber security efforts and initiatives including planning, developing, maintaining, reviewing and implementation of Information Security Policies
10. **Critical Assets:** shall mean the facilities, systems and equipment which, if destroyed, degraded or otherwise declared unavailable, would affect the reliability or operability of the Power Supply System.
11. **Critical System:** shall mean cyber assets essential to the reliable operation of critical asset. Critical System consists of those cyber assets that have at least one of the following characteristics:
    a) The cyber asset uses a routable protocol to communicate outside the electronic security perimeter.
    b) The cyber asset uses a routable protocol within a control centre.
    c) The cyber asset is dial-up accessible.
12. **Critical Information Infrastructure*:*** shall mean Critical Information Infrastructure as defined in explanation of sub-section (1) of Section 70 of the Act.
13. **Cyber Assets**: shall mean the programmable electronic devices, including the hardware, software and data in those devices that are connected over a network, such as LAN, WAN and HAN.
14. **Cyber Crisis Management Plan:** shall mean a framework for dealing with cyber related incidents for a coordinated, multi-disciplinary and broad-based approach for rapid identification, information exchange, swift response and remedial actions to mitigate and recover from malicious cyber related incidents impacting critical processes.
15. **Cyber Security Breach**: shall mean any cyber incident or cyber security violation that results in unauthorized or illegitimate access or use by a person as well as an entity, of data, applications, services, networks and/or devices through bypass of the underlying cyber security protocols, policies and mechanisms resulting in the compromise of the confidentiality, integrity or availability of data/information maintained in a computer resource or cyber asset.
16. **Cyber Security Incident:** shall mean any real or suspected adverse cyber security event that violates, explicitly or implicitly, cyber security policy of Responsible Entity resulting in unauthorized access, denial of service or disruption, unauthorized use of computer resource for processing or storage of information or changes to data or information

without authorization, leading to harm to the power grid or its critical sub-sectoral elements Generation, Transmission and Distribution.

17. **Cyber Security Policy:** shall mean documented set of business rules and processes for protecting information, computer resources, networks, devices, Industrial Control Systems and other OT resources.
18. **Electronic Security Perimeter:** shall mean the logical border surrounding a network to which the Cyber Systems of Power Supply System are connected using a routable protocol.
19. **Information Security Division:** shall mean a division accountable for cyber security and protection of the Critical System of the Responsible Entity.
20. **Protected System:** shall mean any computer, computer system or computer network of the Responsible Entity notified under section 70 of the Act, in the official gazette by appropriate Government.
21. **Security Architecture:** shall mean a framework and guidance to implement and operate a system using the appropriate security controls with the goal to maintain the system's quality attributes like confidentiality, integrity, availability, accountability and assurance.
22. **Vulnerability:** shall mean intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence
23. **Vulnerability Assessment:** shall mean a process of identifying and quantifying vulnerabilities

4.0 Standards

Reference	Description
ISO/IEC 15408	Common Criteria Certification Standard
ISO/IEC 17011	General requirements for accreditation bodies accrediting conformity assessment bodies
ISO/IEC 17025	General requirements for the competence of testing and calibration laboratories
ISO/IEC 21827	Systems Security Engineering - Capability Maturity Model (SSE-CMM)
ISO/IEC 24748-1	Systems and software engineering — Life cycle management — Part 1: Guidelines for life cycle management.
ISO 27001/2	Information Security Management
ISO/ IEC 27019	Information technology — Security techniques — Information Security controls for the energy utility industry
ISO/IEC 61508	Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related Systems
IEC 61850	Communication networks and systems for power utility automation
IEC 62351	Standards for Securing Power System Communications
IEC 62443	Cyber Security for Industrial Control Systems
IS 16335	Power Control Systems – Security Requirements.

5.0 Abbreviations

Abbreviations		Description
a)	BES	Bulk Electric System

b)	CDAC	Centre for Development of Advanced Computing
c)	CEA	Central Electricity Authority
d)	CERC	Central Electricity Regulatory Commission
e)	CERT	Computer Emergency Response Team
f)	CERT-In	Indian Computer Emergency Response Team
g)	CII	Critical Information Infrastructure
h)	CISO	Chief Information Security Officer
i)	CSK	Cyber Swachhta Kendra
j)	COTS	Commercial off-the Shelf
k)	ESP	Electronic Security perimeter
l)	ICS	Industrial Control Systems
m)	ICT	Information and Communications Technology
n)	IEC	International Electro Technical Commission
o)	ISAC	Information Sharing and Analysis Centre
p)	ISD	Information Security Division
q)	ISO	International Organization for Standardization
r)	ISMS	Information Security Management System
s)	IT	Information Technology
t)	FAT	Factory Acceptance Test
u)	NABL	National Accreditation Board for Testing and Calibration Laboratories
v)	NCIIPC	National Critical Information Infrastructure Protection Centre
w)	NLDC	National Load Dispatch Centre
x)	NPTI	National Power Training Institute
y)	NSCS	National Security Council Secretariat
z)	OEM	Original Equipment Manufacturer
aa)	OT	Operational Technology
bb)	RLDC	Regional Load Dispatch Centres
cc)	SAT	Site Acceptance Test
dd)	SERC	State Electricity Regulatory Commission
ee)	SCADA	Supervisory Control and Data Acquisition Systems
ff)	SIEM	Security Information and Event Management
gg)	SLA	Service Level Agreement
hh)	SLDC	State Load Dispatch Centre
ii)	QCI	Quality Council of India

CEA (Cyber Security in Power Sector) Guidelines, 2021

Article 1. Cyber Security Policy.

a. Cardinal Principles: The Responsible entity will strictly adhere to following cardinal principles while framing cyber security policy:

i. There is hard isolation of their OT Systems from any internet facing IT system.
ii. May keep only one of their IT systems with internet facing at any of their site/location if required which is isolated from all OT zones and kept in a separate room under the security and control of CISO.
iii. Downloading/Uploading of any data/information from their internet facing IT system is done only through an identifiable whitelisted device followed by scanning of both for any vulnerability/malware as per the SOP laid down and for all such activities digital logs are maintained and retained under the custody of CISO for at least 6 months. The log shall be readily to carry out the forensic analysis if asked by investigation agency.
iv. List of whitelisted IP addresses for each firewall is maintained by CISO and each firewall is configured for allowing communication with the whitelisted IP addresses only.
v. Communication between OT equipment/systems is done through the secure channel preferably of POWERTEL through the fibre optic cable. Security configuration of the communication channel is also to be ensured.
vi. All ICT based equipment/system deployed in infrastructure/system mandatorily CII are sourced from the list of the "Trusted Sources" as and when drawn by MoP/CEA.

b. The Responsible Entity shall be ISO/IEC 27001 certified (including sector specific controls as per ISO/IEC 27019).
c. The Responsible Entity shall have a Cyber Security Policy drawn upon the guidelines issued by NCIIPC.
d. The Responsible Entity shall ensure annual review of their Cyber Security Policy by subject matter expert and changes shall be made therein only after obtaining the due approval from Board of Directors.
e. The process of Access Management for all Cyber Assets owned or under control of the Responsible Entity shall be detailed in the Cyber Security Policy.
f. The Cyber Security Policy shall leverage state-of-art cyber security technologies and relevant processes at multiple layers to mitigate the cyber security risks.
g. The Responsible Entity shall be solely responsible to get Cyber Security Policy implemented through its Information Security Division (ISD).
h. The CISO shall record the reason(s) for exemption required, if any, in case, unable to comply with any of the provision(s) of the Cyber Security Policy. Any exception shall be allowed only after an approval of provisions of compensatory control(s) to mitigate residual cyber security risks.

i. The CISO shall record the exemptions sought in statement of applicability controls, while getting the ISO 27001 certified. All exemptions and its justification need to be in conformance with Cyber Security Policy of the Responsible Entity.
j. The Responsible Entity shall allocate sufficient Annual budget for enhancing cyber security posture, enhanced year over year.
k. The Responsible Entity shall work in collaboration with other Industry Stakeholders as well as Academia to promote R&D activity in the domain of cyber security.
l. The Responsible Entity shall ensure that cyber security issues are taken up as agenda items in their Board meetings once in every three months.

Article 2 Appointment of CISO.

a) The Responsible Entity shall mandatorily appoint a CISO and shall confirm to qualification, if any, **laid** by Quality Council of India (QCI). In absence, the work of CISO shall be looked upon by Alternate CISO. In case qualification for appointment of Alternate CISO has been relaxed for reasons recorded thereof, Alternate CISO has to mandatorily acquire the minimum required cyber security skill sets within six months from the date of his appointment.
b) The Responsible Entity shall regularly update details of CISO and Alternate CISO, with the Sectoral CERT, as well as on ISAC-Power Portal.
c) Roles and Responsibility of CISOs shall be as laid by CERT-In and ring-fenced to ensure cyber security of the Cyber Assets of the Responsible Entity.

Article 3: Identification of Critical Information Infrastructure (CII).

a) The Responsible Entity shall submit to NCIIPC through Sectoral CERT, details of Cyber Assets which uses a routable protocol to communicate outside the Electronic Security Perimeter drawn by the Responsible Entity or a routable protocol within a control centre and dial-up accessible Cyber Assets, within 30 days from the date of their commissioning in the System.
b) The Responsible Entity shall submit details of Critical Business Processes and underlying information infrastructure along with mapped impact and Risk Profile to NCIIPC and shall get their CIIs identified in consultation with NCIIPC. The process of the notification/declaration by Appropriate Government shall follow thereafter.
c) The Responsible Entity shall review their declared/notified CIIs at least once a year to examine changes if any in the functional dependencies, protocols and technologies or upon any change in security architecture. The Responsible Entity shall review their declared/notified CIIs once in every 6 months, in case if NCIIPC has directed them to constitute an Information Security Steering Committee.
d) The Responsible Entity shall ensure that all cyber assets of their identified/notified CIIs are recorded in the asset register and considered for risk assessment as well as for finalization of controls in statement of applicability.

Article 4. Electronic Security Perimeter

a) The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all Access Points to the perimeter(s).

b) The Responsible Entity shall follow procedure of identifying "Electronic Security Perimeter" in case of distributed and/or hybrid information infrastructure, as per IEC 62443 / IS16335 (as amended from time to time).
c) The Responsible Entity shall ensure that every Critical System resides within an Electronic Security Perimeter.
d) The Responsible Entity shall perform a cyber-Vulnerability Assessment of each electronic Access Points to the Electronic Security Perimeter(s) at least once in every 6 (six) months and/or after any change in Security Architecture.
e) The Responsible Entity shall ensure that all critical, high and medium vulnerabilities identified as a result of cyber Vulnerability Assessment shall be closed and verified for the effective closure.

Article 5. Cyber Security Requirements

a) The Responsible Entity shall have an Information Security Division (ISD), headed by CISO.
b) The Responsible Entity shall ensure that the ISD must be functional on 24x7x365 basis and is manned by sufficient numbers of Engineers having valid certificate of successful completion of course on cyber security of Power Sector from the Training Institutes designated by CEA.
c) The Responsible Entity shall ensure that ISD
   1) has on-boarded Cyber Swachhta Kendra(CSK) of CERT-In, if they have public IPs.
   2) has timely acted upon the advisories, guidelines and directive of NCIIPC, CSK, CERT-In and Sectoral CERTs,
   3) has deployed an Intrusion Detection System and Intrusion Prevention System capable of identifying behavioural anomaly in both IT as well as OT Systems.
   4) shares reports on incident response and targeted malware samples with CERT-In,
   5) updates the firmware/software with the digitally signed OEM validated patches only.
   6) enables only those ports and services that are required for normal operations. In case of any emergency the procedure as laid in Access management be followed.
   7) maintains firewall logs for the last 6 months duration. Firewall logs shall be analysed and all critical and high severity comments shall be addressed for effective closure.
   8) retains document of FAT, SAT test results and report/ certificate of cyber tests carried out for compliance of Government Orders and Cyber Security Audit.*
   9) maintains all cyber logs and cyber forensic records of any incident for at least** 90 days.

      * FAT, SAT must include comprehensive cyber security tests of the component/equipment/system to be delivered/delivered at site.
      ** 90 days from date of the commissioning of the system/recovery from any incident, whichever is later.

d) The Responsible Entity shall routinely audit and test security properties of the Critical System and must act upon, in case if any new vulnerabilities is identified through testing or by the equipment manufacturer.

e) The Responsible Entity shall design a secure architecture for control system appropriate for their process control environment*.
f) All State Load Dispatch Centres(SLDCs) shall comply with the directions issued by the National Load Dispatch Centre(NLDC) as well as Regional Load Dispatch Centres(RLDCs) U/s 29 (1) of the Electricity Act, 2003 to ensure stability and cyber security of grid operation and achieve efficiency in the grid operation. In case of any non-compliance, the Head of SLDC shall be responsible and shall be liable for Penalty as per the provision of CERC/SERC.

*There are so many different types of systems in existence and so many possible solutions, it is important that the selection process ensures that the level of protection is commensurate with the business risk and the Responsible Entity shall not rely on one single security measure for its defence. *(Reference IEC/TR62351-10* Edition1.0 2012-10 *Power systems management and associated information exchange –Data and communications security – Part 10: Security architecture guidelines).*

Article 6 Cyber Risk Assessment and Mitigation Plan

a) The Responsible Entity shall document in their Cyber Security Policy a Cyber Risk Assessment and Mitigation Plans drawn upon the best practises being followed in the Power Sector, and the same shall be approved by Board of Directors.
b) The Cyber Risk Assessment and Mitigation Plans shall clearly define the matrix for assessing the cyber risk of both IT and OT environment and risk acceptance criteria.
c) The Cyber Risk Assessment Plan shall be capable to demonstrate that repeated cyber security risk assessment delivers consistent, valid and comparable results.
d) The review of cyber risk assessment shall be carried out at least once in a Quarter. The actionable of risk treatment and mitigation shall be tracked in this review for their effectiveness.
e) The CISO shall be responsible for implementation and regular review, on the basis of internal and external feedbacks, of the Cyber Risk Assessment and Mitigation Plans.

Article 7 Phasing out of Legacy System

a) As the life cycle of the Power System Equipment/System is longer than that of IT Systems deployed therein, the Responsible Entity shall ensure that all IT technologies in the Power System Equipment/System should have the ability to be upgraded.
b) The Responsible Entity shall ensure that the Information Security Division shall draw the list of all communicable equipments/systems nearing end life or are left without support from OEM. Thereafter CISO shall identify equipment/systems to be phased out from the list drawn, firm up their replacement plan and put up the replacement plan for approval before the Board of Directors.
c) The CISO shall ensure that till equipments/systems nearing end life or left without support from OEM are not replaced, their cyber security is hardened and ensured through additional controls provisioned in consultation with the OEM or alternate Supplier(s)*.
*e.g. Use of CDAC developed AppSamvid and whitelisting of applications installed may be explored across all legacy systems.
d) The Responsible Entity shall document in their Cyber Security Policy a Standard Operating Procedure for safe and secure disposal of outlived or legacy systems.

Article 8. Cyber Security Training.

a) The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized physical access (unescorted or escorted) to their Critical Systems.
b) The Responsible Entity shall review annually their cyber security training program and shall update it whenever necessary. Annual Review shall record evaluation of the effectiveness of the trainings held.
c) The Responsible Entity shall ensure that Cyber Security training program designed for their IT as well as OT O&M Personnel must include following topics and as per their functional requirements and security concerns additional topics shall be added:
    1) User authentication and authorization.
    2) Cyber Security and Protection mechanisms of IT/OT/ICS Systems.
    3) Introduction to various standards i.e. ISO/IEC:15408, ISO/IEC:24748-1, ISO: 27001, ISO: 27002, ISO 27019, IS 16335, IEC/ISO:62443.
    4) Training on implementation of ISO/IEC 27001 and awareness on IEC 62443.
    5) Vulnerability Assessment in the Critical System.
    6) Monitoring and preserving of electronic logs of access of Critical Assets.
    7) Detecting cyber-attacks on SCADA and ICS systems
    8) The handling of Critical System during cyber crisis.
    9) Action plans and procedures to recover or re-establish normal functioning of Critical Assets and access thereto following a Cyber Security Incident.
    10) Hands on SCADA operation at any of the Regional Load Dispatch Centre.
    11) Handling of risks involved in the procurement of COTS Products.

d) All Personnel engaged in O&M of IT & OT Systems shall mandatorily undergo courses on cyber security of Power Sector from any of the training institute designated by CEA, immediately within 90 days from the notification of CEA Guidelines on Cyber Security in Power Sector.
e) The Responsible Entity shall ensure that none of their newly hired or the current Personnel have access to the Critical System, prior to the satisfactory completion of cyber security training programme from the Training Institutes designated in India, except in specified circumstances such as cyber crisis or an emergency.
f) NPTI in consultation with CEA shall identify and design domain specific courses on Cyber Security for different target groups. The "Governing Board for PSO Training and Certification" shall approve the content, duration etc of these courses and shall review it Annually. NPTI shall conduct these courses at all of their branches on regular basis and shall maintain the list of the Participants successfully completing the course.

Article 9 Cyber Supply Chain Risk Management

a) The Responsible Entity shall ensure that, as and when Ministry of Power, Government of India notifies the Model Contractual Clauses on cyber security, these clauses are included in their every Bid invited for procurement of any ICT based components/equipments/System to be used for Power System.
b) The Responsible Entity shall ensure that all the Communicable Intelligent Equipments and the Service Level Agreements (SLAs) for their Critical Systems shall be sourced from the list of the "Trusted Sources" as and when drawn by MoP/CEA.

c) The Responsible Entity shall ensure that, in case, for the any Communicable Intelligent Devices, if no Trusted Source has been identified, then the successful bidder in compliance with the provisions made in MoP order dated 2.7.2020 and any other relevant MoP order has got the product cyber tested for any kind of embedded malware/Trojan/cyber threat and for adherence to Indian Standards at the designated lab.

d) The Responsible Entity shall ensure that the essential cyber security tests are carried out successfully during FAT, SAT as detailed in **Annexure A.** The equipment/System besides for functionality shall also be tested in the factory for vulnerabilities, design flaws, parts being counterfeit or tainted, so as to minimize problems during on-site-testing and installation. Cyber Security Conformance Testing are to be carried out in the designated Lab as listed in **Annexure-I of MoP Order No. 12/13/2020-T&R dt. 8th June, 2021(Order at Annexure-B).**

e) The Responsible Entity shall ensure that the Equipment/System supplied by the successful bidder shall accompany with a certificate[$, #] obtained by OEM from a certification body accredited to assess devices and process for conformances to IEC 62443-4 standards during design and manufacture. The Responsible Entity shall accept the certificate submitted along with the supplied Equipment/System only if it's in line with the Testing Protocol as notified by Ministry of Power, Government of India, from time to time.

f) The Responsible Entity in compliance to the requirement of Article 9(e) shall also accept, till the setting up of an adequate certification facility in the India, a digitally signed self-declaration of conformance to the IEC 62443-4 standards during design and manufacture of the equipment/system, if submitted by the OEM.

g) The Responsible Entity shall dispose all unserviceable or obsolete Communicable Intelligent Devices as per the procedure laid in their Cyber Risk Assessment and Mitigation Plans which shall be in line with the prevailing best practices.

$ The National & International certification may be specified in the tender for critical systems/sub-systems being procured by the Responsible Entity.

Certification Schemes:
Embedded Device Security Assurance Certification is for an individual product,
System Security Assurance Certification is for a set of products in a system (possibly from different vendors)
Security Development Lifecycle Assurance Certification is for the development processes that a manufacturer uses for developing products.

Article 10 Cyber Security Incident Report and Response Plan

a) The CISO of the Responsible Entity shall report in the formats prescribed by CERT-In, all Cyber Security Incidents, classified as reportable events.

b) Root cause analysis for all reportable events shall be carried out and corrective action taken, so as to ensure that any re-occurrence of such event can be managed with ease.

c) The Responsible Entity shall mandatorily define in their Cyber Security Policy, criteria(s) identified on the basis of impact analysis, for declaring the occurrence of

Cyber Security Incident(s) as a Cyber Crisis in the System owned or controlled by them.

d) The Responsible Entity shall mandatorily designate an Officer along with his/her standby by name and designation and empower them to declare an occurrence of the incident(s) as "Cyber Crisis". The contact details of these Officers shall be updated in the C-CMP within 15 days of changes if any due to transfer or superannuation etc.
e) The CISO shall ensure that during any Cyber Security Incident, ISD monitors and minutely records every details of cyber security events and incidents in both IT as well as the OT System owned or controlled by the Responsible Entity.
f) The CISO shall ensure that each cyber incident is handled strictly as per Cyber Security Incident Response Plan detailed in the latest C-CMP approved by the Board of Directors.
g) The Responsible Entity shall ensure that the efficacy of the Cyber Security Incident Response Plan is tested annually through mock drill(s) carried out, if feasible, as simulation exercise(s) or as table top exercise(s) with wider participation of their employees, in consultation with CERT-In and sectoral CERT. In case if any shortcoming is observed in the Cyber Security Incident Response Plan suitable changes shall be made in it.
h) The Responsible Entity shall ensure that the CISO compiles details of incident detection, incident handling, learnings from each incident and damage claims made if any and shall report to CERT-In as well as upload information on ISAC-Power Portal.

Article 11 Cyber Crisis Management Plan(C-CMP)

a) The Responsible Entity shall prepare a Cyber Crisis Management Plan and submit to their sectoral-CERT for review with intimation to Ministry of Power/CISO-MoP. Responsible Entity shall update their C-CMP on the basis of comments made by sectoral-CERT and then submit for vetting to CERT-In. The C-CMP shall be updated once again to include the observations made by CERT-In before seeking approval of Board of Directors for implementation of C-CMP.
b) The Responsible Entity shall ensure that the C-CMP is reviewed at least annually. The CISO shall ensure that all changes are made in C-CMP only with the due approval of Board of Directors and the changes made in C-CMP have been communicated through a verifiable means to all the concerned Personnel of the Responsible Entity.
c) The CISOs shall be the custodian of all the cyber security related documents including Cyber Crisis Management Plan, Risk Treatment Plan, Statement of Applicability of controls, and compliance to regulator's requirement.
d) The CISO shall be accountable for ensuring enforcement of C-CMP by Information Security Division of the Responsible Entity, during a cyber-crisis, as and when declared by the designated Officer. (refer Article 10(d))

Article 12: Sabotage Reporting%

a) The Responsible Entity shall incorporate procedure for identifying and reporting of sabotage in their Cyber Security Policy within 30 days from issue of the Guidelines, or grant of licence under the appropriate legal provisions to the Responsible Entity.
b) The CISO shall be held liable for non-reporting of identified sabotage(s) as per procedure laid for identifying and reporting of sabotage in the Cyber Security Policy of the Responsible Entity.

c) The CISO shall prepare a detailed report on disturbances or unusual occurrences, identified, suspected or determined to be caused by sabotage in the Critical System of the Responsible Entity, and shall submit the report to the Sectoral CERT as well as to CERT-In within 24 hours of its occurrence.
d) The CISO shall submit to NCIIPC within 24 hours of occurrence the report on every sabotage classified as cyber incidents(s) on "Protected System".
e) The CISO upon occurrence on every sabotage shall take custody of all log records as well as digital forensic records of affected Cyber Assets, Intrusion Detection System, Intrusion Protection System, SIEM and shall preserve them for at least 90 days and shall make them available as and when called upon for investigation by the concerned Agencies.

%Disturbances or unusual occurrences, suspected or determined to be caused by sabotage.
Sabotage e.g. can be a forced intrusion in un-manned/manned facility and taking control of operation of Critical System through a communicating device.

Article 13 Security and Testing of Cyber Assets

a) The Responsible Entity shall ensure security of all in-service phase as well as standby Cyber Assets through regular firmware/Software updates and patching, Vulnerability management, Penetration testing (of combined installations), securing configuration, supplementing security controls. CISO shall maintain details of update version of each firmware and software and their certification if received from OEMs.
b) The Responsible Entity shall carry out regularly Vulnerability Assessment of all Cyber Assets owned or under their control. If a Cyber Asset is found vulnerable to any exploits or upon any patch updates or major configuration changes, then further Penetration Testing may be carried out offline or in a suitably configured laboratory test-bed to determine other vulnerabilities that may have not been identified so far.
c) The Responsible Entity shall specify security requirement and evaluation criteria during each phase of their procurement Process.
d) The Responsible Entity shall ensure that all Cyber Assets being procured shall conform to the type tests as mentioned in the specification for type testing listed in the bid document. Type test reports of tests conducted in NABL accredited Labs or internationally accredited labs (with in last 5 years from the date of bid opening) shall be mandated to be submitted along with bid. In case, the submitted Type Test reports are not as per specification, the re-tests shall be conducted without any cost implication to the Responsible Entity.
e) The Responsible Entity shall ensure that all Communicable devices are tested for communication protocol as per the ISO/IEC/IS standards listed in **MoP Order No. 12/13/2020-T&R dated 8th June, 2021(Annexure-B).**
f) The Responsible Entity shall ensure that all Critical Systems designed with Open Source Software are adequately cyber secured.
g) The Responsible Entity as a best practise upon any incidence of Cyber Security Breach shall carry out cyber security tests at any lab designated for cyber testing by Ministry of Power. These tests shall be similar to Pre Commissioning Security Test and those essential for carrying out Post Incident Forensics Analysis.

Article 14 Cyber Security Audit

a) The Responsible Entity shall implement Information Security Management System (ISMS) covering all its Critical Systems.
b) The Responsible Entity shall through a CERT-In Empanelled Cyber Security OT Auditor shall get their IT as well as OT System audited at least once in every 6 (six) months and shall close all critical and high vulnerabilities within a period of one month and medium as well as low non-conformity before the next audit. Effective closure of all non-conformities shall be verified during the next audit.
c) The Cyber Security Audit shall be as per ISO/IEC 27001 along with sector specific standard ISO/IEC 27019, IS 16335 and other guidelines issued by appropriate Authority if any. These mentioned standards shall be current with all amendments if any and in case if any standard is superseded, the new standard shall be applicable. CISO shall ensure immediate closure of non-conformance, based on the criticality and by means all non-conformances are to be closed before the next audit.
d) The Responsible Entity shall ensure that CISO has all the required systems and documents in place, as mandated by NSCS for base line cyber security audit.

No. 20(3)/2022-CERT-In
Government of India
Ministry of Electronics and Information Technology (MeitY)
Indian Computer Emergency Response Team (CERT-In)

Electronics Niketan,
6 CGO Complex,
New Delhi-110003

Dated: 28 April, 2022

Subject: Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.

Whereas, the Central Government in terms of the provisions of sub-section (1) of section 70B of Information Technology (IT) Act, 2000 (IT Act, 2000) has appointed "Indian Computer Emergency Response Team (CERT-In)" vide notification dated 27th October 2009 published in the official Gazette and as per provisions of sub-section (4) of section 70B of IT Act, 2000 The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security:-

a) collection, analysis and dissemination of information on cyber incidents;
b) forecast and alerts of cyber security incidents;
c) emergency measures for handling cyber security incidents;
d) coordination of cyber incidents response activities;
e) issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
f) such other functions relating to cyber security as may be prescribed.

And whereas, "The Information Technology (The Indian Computer Emergency Response Team and Manner of performing functions and duties) Rules, 2013" were notified and published vide notification dated 16.01.2014 by the Central Government in exercise of the powers conferred by clause (zf) of sub-section (2) of section 87 read with sub-section (5) of section 70B of the IT Act, 2000.

And whereas, as per provisions of sub-section (6) of section 70B of the IT Act, 2000, CERT-In is empowered and competent to call for information and give directions to the service providers, intermediaries, data centres, body corporate and any other person for carrying out the activities enshrined in sub-section (4) of section 70B of the IT Act, 2000.

And whereas, various instances of cyber incidents and cyber security incidents have been and continue to be reported from time to time and in order to coordinate response activities as well as emergency measures with respect to cyber security incidents, the requisite information is either sometime not found available or readily not available with service providers/data centres/body corporate and the said primary information is essential to carry out the analysis, investigation and coordination as per the process of law.

And whereas, it is considered expedient in the interest of the sovereignty or integrity of India, defence of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence using computer resource or for handling of any cyber incident, that following directions are issued to augment and strengthen the cyber security in the country:

(i) All service providers, intermediaries, data centres, body corporate and Government organisations shall connect to the Network Time Protocol (NTP) Server of National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP servers traceable to these NTP servers, for synchronisation of all their ICT systems clocks. Entities having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC, however it is to be ensured that their time source shall not deviate from NPL and NIC.

(ii) Any service provider, intermediary, data centre, body corporate and Government organisation shall mandatorily report cyber incidents as mentioned in Annexure I to CERT-In within 6 hours of noticing such incidents or being brought to notice about such incidents. The incidents can be reported to CERT-In via email (incident@cert-in.org.in), Phone (1800-11-4949) and Fax (1800-11-6969). The details regarding methods and formats of reporting cyber security incidents is also published on the website of CERT-In www.cert-in.org.in and will be updated from time to time.

(iii) When required by order/direction of CERT-In, for the purposes of cyber incident response, protective and preventive actions related to cyber incidents, the service provider/intermediary/data centre/body corporate is mandated to take action or provide information or any such assistance to CERT-In, which may contribute towards cyber security mitigation actions and enhanced cyber security situational awareness. The order / direction may include the format of the information that is required (up to and including near real-time), and a specified timeframe in which it is required, which should be adhered to and compliance provided to CERT-In, else it would be treated as non-compliance of this direction. The service providers, intermediaries, data centres, body corporate and Government organisations shall designate a Point of Contact to interface with CERT-In. The Information relating to a Point of Contact shall be sent to CERT-In in the format specified at Annexure II and shall be updated from time to time. All communications from CERT-In seeking information and providing directions for compliance shall be sent to the said Point of Contact.

(iv) All service providers, intermediaries, data centres, body corporate and Government organisations shall mandatorily enable logs of all their ICT systems and maintain them securely for a rolling period of 180 days and the same shall be maintained within the Indian jurisdiction. These should be provided to CERT-In along with reporting of any incident or when ordered / directed by CERT-In.

(v) Data Centres, Virtual Private Server (VPS) providers, Cloud Service providers and Virtual Private Network Service (VPN Service) providers, shall be required to register the following accurate information which must be maintained by them for a period of 5 years or longer duration as mandated by the law after any cancellation or withdrawal of the registration as the case may be:

a. Validated names of subscribers/customers hiring the services
b. Period of hire including dates
c. IPs allotted to / being used by the members
d. Email address and IP address and time stamp used at the time of registration / on-boarding
e. Purpose for hiring services
f. Validated address and contact numbers
g. Ownership pattern of the subscribers / customers hiring services

(vi) The virtual asset service providers, virtual asset exchange providers and custodian wallet providers (as defined by Ministry of Finance from time to time) shall mandatorily maintain all information obtained as part of Know Your Customer (KYC) and records of financial transactions for a period of five years so as to ensure cyber security in the area of payments and financial markets for citizens while protecting their data, fundamental rights and economic freedom in view of the growth of virtual assets.

For the purpose of KYC, the Reserve Bank of India (RBI) Directions 2016 / Securities and Exchange Board of India (SEBI) circular dated April 24, 2020 / Department of Telecom (DoT) notice September 21, 2021 mandated procedures as amended from time to time may be referred to as per Annexure III.

With respect to transaction records, accurate information shall be maintained in such a way that individual transaction can be reconstructed along with the relevant elements comprising of, but not limited to, information relating to the identification of the relevant parties including IP addresses along with timestamps and time zones, transaction ID, the public keys (or equivalent identifiers), addresses or accounts involved (or equivalent identifiers), the nature and date of the transaction, and the amount transferred.

And whereas, the meaning to the terms 'cyber incident' or 'cyber security incident' or 'computer resource' or other terms may be ascribed as defined in the IT Act, 2000 or "The Information Technology (The Indian Computer Emergency Response Team and Manner of performing functions and duties) Rules, 2013" as the case may be.

And whereas, in case of any incident, the above-referred entities must furnish the details as called for by CERT-In. The failure to furnish the information or non-compliance with the ibid. directions, may invite punitive action under sub-section (7) of the section 70B of the IT Act, 2000 and other laws as applicable.

This direction will become effective after 60 days from the date on which it is issued.

*****

Annexure I

Types of cyber security incidents mandatorily to be reported by service providers, intermediaries, data centres, body corporate and Government organisations to CERT-In:

[Refer Rule 12(1)(a) of The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013]

i. Targeted scanning/probing of critical networks/systems
ii. Compromise of critical systems/information
iii. Unauthorised access of IT systems/data
iv. Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.
v. Malicious code attacks such as spreading of virus/worm/Trojan/Bots/ Spyware/Ransomware/Cryptominers
vi. Attack on servers such as Database, Mail and DNS and network devices such as Routers
vii. Identity Theft, spoofing and phishing attacks
viii. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
ix. Attacks on Critical infrastructure, SCADA and operational technology systems and Wireless networks
x. Attacks on Application such as E-Governance, E-Commerce etc.
xi. Data Breach
xii. Data Leak
xiii. Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers
xiv. Attacks or incident affecting Digital Payment systems
xv. Attacks through Malicious mobile Apps
xvi. Fake mobile Apps
xvii. Unauthorised access to social media accounts
xviii. Attacks or malicious/ suspicious activities affecting Cloud computing systems/servers/software/applications
xix. Attacks or malicious/suspicious activities affecting systems/ servers/ networks/ software/ applications related to Big Data, Block chain, virtual assets, virtual asset exchanges, custodian wallets, Robotics, 3D and 4D Printing, additive manufacturing, Drones

xx. Attacks or malicious/ suspicious activities affecting systems/ servers/software/ applications related to Artificial Intelligence and Machine Learning

The incidents can be reported to CERT-In via email (incident@cert-in.org.in), Phone (1800-11-4949) and Fax (1800-11-6969). The details regarding methods and formats of reporting cyber security incidents is also published on the website of CERT-In www.cert-in.org.in and will be updated from time to time.

*****

Annexure II

Format for providing Point of Contact (PoC) information by Service providers, intermediaries, data centres, body corporate and Government organisations to CERT-In

The Information relating to the Point of Contact shall be sent to CERT-In via email (info@cert-in.org.in) in the format specified below and shall be updated from time to time:

Name	
Designation	
Organisation Name	
Office Address	
Email ID	
Mobile No.	
Office Phone	
Office Fax	

*****

Annexure III

KYC Requirements

For the purpose of KYC, any of following Officially Valid Document (OVD) as a measure of identification procedure prescribed by the Reserve Bank of India (Know Your Customer (KYC)) Directions, 2016 / Securities and Exchange Board of India Clarification on Know Your Client (KYC) Process and Use of Technology for KYC vide Circular SEBI/HO/MIRSD/DOP/CIR/P/2020/73 dated April 24, 2020 / The Department of Telecom File No: 800-12/2021- AS.II dated September 21, 2021 on Self-KYC (S-KYC) as an alternate process for issuing of new mobile connections to Local and Outstation category customers, shall be used and maintained:

a. The passport,
b. The driving license,
c. Proof of possession of Aadhaar number,
d. The Voter's Identity Card issued by the Election Commission of India,
e. Job card issued by NREGA duly signed by an officer of the State Government and
f. Letter issued by the National Population Register containing details of name and address.
g. Validated phone number
h. Trading account number and details, Bank account number and bank details

For the purpose of KYC for business entities (B2B), documents mentioned in the Customer Due Diligence (CDD) process prescribed in Reserve Bank of India Master Direction - Know Your Customer (KYC) Direction, 2016 as updated from time to time shall be used and maintained.

*****

Windows XP

ANNEXURE-R3

Windows XP follows the Fixed Lifecycle Policy.

This applies to the following editions: Home, Professional, Professional for Embedded Systems, Professional x64, Starter

> **Important**
>
> Support for this product has ended. See migration guidance below.

Support dates are shown in the Pacific Time Zone (PT) - Redmond, WA, USA.

Support Dates

Listing	Start Date	Mainstream End Date	Extended End Date
Windows XP	Dec 31, 2001	Apr 14, 2009	Apr 8, 2014

Releases

Version	Start Date	End Date
Service Pack 3	Apr 21, 2008	Apr 8, 2014
Service Pack 2	Sep 17, 2004	Jul 13, 2010
Service Pack 1a	Feb 3, 2003	Oct 10, 2006
Service Pack 1	Aug 30, 2002	Oct 10, 2006
Original Release	Dec 31, 2001	Aug 30, 2005

Links

- Migration guidance
- Service pack policy

> **Note**
>
> The start date for Microsoft Windows XP Professional x64 Edition was April 24, 2005.

Editions

- Home
- Professional
- Professional for Embedded Systems
- Professional x64
- Starter

रजिस्ट्री सं. डी.एल.- 33004/99 REGD. No. D. L.-33004/99

भारत का राजपत्र
The Gazette of India

सी.जी.-डी.एल.-अ.-02012023-241581
CG-DL-E-02012023-241581

असाधारण
EXTRAORDINARY

भाग III—खण्ड 4
PART III—Section 4

प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 699] नई दिल्ली, मंगलवार, दिसम्बर 27, 2022/पौष 6, 1944
No. 699] NEW DELHI, TUESDAY, DECEMBER 27, 2022/PAUSHA 6, 1944

केंद्रीय विद्युत प्राधिकरण

अधिसूचना

नई दिल्ली, 23 दिसम्बर, 2022

केविप्रा-टीएच-17/1/2021-टीईटीडी प्रभाग.—विद्युत अधिनियम, 2003 (2003 का 36) की धारा 177 के उप धारा (3) के साथ पठित विद्युत (पिछले प्रकाशन की प्रक्रिया) नियम, 2005 के नियम (3) के उप नियम (2) द्वारा यथाअपेक्षित केंद्रीय विद्युत प्राधिकरण (विद्युत संयंत्रों और विद्युत लाइनों के निर्माण के लिए तकनीकी मानक) विनियम, 2022 का प्रारूप छः दैनिक समाचार पत्रों में प्रकाशित किया गया था, उन सभी व्यक्तियों से, जिनके उनसे प्रभावित होने की संभावना थी, उस तारीख से जिसको उक्त प्रारूप विनियमों से युक्त समाचार पत्र की प्रतियां जनता को उपलब्ध करा दी गई थीं, सैंतालीस दिन की अवधि के समाप्ति से पूर्व आक्षेप और सुझाव आमंत्रित किये गये थे;

और उक्त समाचार पत्रों की प्रतियां, जिनमें सार्वजनिक सूचनाएं और उक्त प्रारूप विनियम सम्मिलित हैं, केंद्रीय विद्युत प्राधिकरण की वेबसाइट पर 30 दिसंबर, 2021 को जनता को उपलब्ध करा दिए गए थे;

और उक्त प्रारूप विनियमों पर जनता से प्राप्त आपत्तियों और सुझावों पर केंद्रीय विद्युत प्राधिकरण द्वारा विचार कर लिया गया था;

अतः, विद्युत अधिनियम, 2003 (2003 का 36) की धारा 177 की उप-धारा (1) के साथ पठित उक्त अधिनियम की धारा 73 के खण्ड (ख) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए, केंद्रीय विद्युत प्राधिकरण निम्नलिखित विनियम बनाता है, अर्थात्: -

अध्याय 1

1. संक्षिप्त नाम, प्रारंभ और लागू होना - (1) इन विनियमों का संक्षिप्त नाम केंद्रीय विद्युत प्राधिकरण (विद्युत संयंत्रों और विद्युत लाइनों के निर्माण के लिए तकनीकी मानक) विनियम, 2022 है।

mineralised water of the Station in twenty hours of operation of the de-mineralised plant.

(c) Adequate redundancy shall be provided in the number of de-mineralising streams.

(ii) The demineralized water shall be stored in minimum two nos. de-mineralised water storage tanks of total storage capacity equal to twenty four hour Station requirement.

(e) Waste Water Treatment System.—

The waste water generated at various locations shall be segregated at the source of generation according to its type:

Provided that similar type of waste water shall be collected at one point and suitably treated for reuse in the plant:

Provided further that the treatment of plant waste water shall be in accordance with the statutory requirements.

(5) **Fire detection, alarm and protection system.—**

(i) A comprehensive fire detection, alarm as well as fire protection system shall be installed for the Station in conformity with relevant Indian Standard.

(ii) Automatic fire detection and alarm system shall be intelligent and addressable type and shall be provided to facilitate detection of fire at the incipient stage and give warning to the firefighting staff.

(iii) Major equipment to be used for fire detection and protection system shall be in accordance with relevant Indian Standard or Underwriters Laboratories, USA or Factory Mutuals, USA or Loss Prevention Certification Board, United Kingdom or VDS (Germany).

(iv) Dedicated fire water storage and pumping facilities of adequate capacities shall be provided for the fire fighting system as per Tariff Advisory Committee guidelines:

Provided that the main fire water pumps shall be electrically driven and standby pumps shall be diesel engine driven.

(v) Necessary hydrant system, complying with Tariff Advisory Committee guidelines, shall be provided at various locations to cover the entire Station.

(vi) All major and minor fire risks in the Station shall be protected against fire by suitable automatic fire protection systems:

Provided that the following systems shall be generally adopted for various fire risks:

(a) Each transformer and reactor shall be provided as per Central Electricity Authority (Measures relating to Safety and Electric Supply) Regulations, 2010 or any successor or subsequent Regulations in this regard.

(b) Automatic high velocity water spray system as per IS 15325, shall be provided for the following areas namely: -

(ba) Lubricating oil systems including storage tanks, purifier units, coolers, turbine oil canal pipelines;

(bb) Generator seal oil system tanks, coolers;

(bc) Steam generator burner fronts.

(c) Steam turbine bearing housing and air pre-heater shall be provided with manually actuated high velocity water spray system.

(d) Automatic medium velocity water spray system, complying with Tariff Advisory Committee guidelines, shall be provided for the areas relating to:

(da) Cable galleries, cable vaults, cable spreader rooms, cable risers, cable shafts etc.;

(db) Coal conveyors, transfer points, crusher houses etc.;

(dc) Fuel oil pumping stations;

(dd) Light Diesel Oil and day oil tanks;

(de) Reliable standby power supply system building.

(e) Automatic foam system shall be provided for fuel oil storage tanks as per National Fire Protection Association guidelines.

(f) Automatic inert gas flooding system, comprising of 2x100% inert gas cylinder batteries conforming to National Fire Protection Association, shall be provided for Unit control rooms, control equipment rooms and area above false ceiling of these rooms.

(vii) Portable fire extinguisher as per Tariff Advisory Committee guidelines shall be provided for each room/area of power station in addition to fixed fire protection system to extinguish fire in its early phase to prevent its spread.

(viii) Fire station and fire tenders along with trained staff shall be provided for the Station.

(ix) Passive fire protection measures such as fire barriers for cable galleries and shafts etc., fire retardant coatings, fire resistant penetration sealing for all openings in floors, ceilings, walls etc., fire proof doors etc. shall be provided to prevent spreading and for containment of fire.

(6) **Compressed air system.—**

(a) Compressed air system comprising of instrument air and service air shall be provided to cater to the requirement for operation of various pneumatically operated drives and general purpose cleaning and maintenance services:

Provided that air dryers shall be provided for instrument air to achieve desired dryness.

(b) At least one number air compressor shall be provided as standby.

(7) **Ventilation and air-conditioning system.—**

(a) Suitable ventilation and air-conditioning system shall be provided to achieve proper working environment in the Station.

(b) (i) Central control room, local control rooms and service building for Operation and Maintenance personnel shall be air conditioned:

Provided that the air- conditioned areas shall be maintained at about 25°C and 50 % relative humidity for comfort conditions.

(ii) Water chilling unit shall be of 2x100% or 3x50% capacity and condensing units shall be of 2x100% capacity:

Provided that the package type air-conditioners shall have 2x100% capacity or 3x50% capacity equipment:

Provided further that for window air conditioners and split air conditioners, if used for small control rooms, at least one unit shall be kept as standby.

(c) The type of ventilation systems to be provided, excluding for air conditioned areas shall be as under:—

(i) All floors of TG building, switchgear: Evaporating cooling system rooms and cable gallery

(ii) Other buildings: Mechanical ventilation system

(8) **Mill rejects system.—**The mill rejects system shall be provided to collect reject from coal mills in case of vertical mills:

Provided that the system shall be of mechanized type i.e. drag chain conveyor or pneumatically pressurized conveying system:

Provided further that the system shall consist of collection of rejects from each coal mill and transport to silos for final disposal.

(9) **Electric overhead travelling crane .—**

(a) The Electric Overhead Travelling cranes shall be provided for maintenance of Turbine Generator cycle equipment and Circulating Water pumps:

Provided that these shall comply with the requirements of latest versions of relevant Indian Standard:

Provided further that the crane capacity shall be taken as five percent more than the single heaviest equipment to be lifted by the crane.

(b) Two Electric Overhead Travelling cranes may be provided for maintenance of Turbine Generator cycle equipment in case more than two steam turbine generators are housed in the Turbine Generator hall.

(10) **Laboratories.—** The Station shall be provided with following laboratories namely:-

(a) Electrical laboratory with necessary equipment and instruments for testing and maintenance of electrical equipment;

(b) Control and Instrumentation laboratory with necessary equipment and instruments for testing, calibration and maintenance of control and instrumentation systems;

(c) Chemical laboratories with necessary equipment, instruments and reagents for chemical analysis in

Grant Thornton
An instinct for growth™

NTPC TANDA

OT Assessment Report

Cycle-2 & Revalidation _C1

Version Control					
Version	Date	Created by	Reviewed / Modified by	Approved by	Report Stage
1.0	16-12-2022	Akhil Kumar Agile	Rahul Sharma	Harish Sah	Stage-1
1.1	06-10-2023	Ujjwal Ranjan	Amit Kumar / Sonal Malhotra	Harish Sah	C2_Stage1 & Revalidation_C1

Report Distribution		
Name	Organization	Purpose
Suresh Kumar/ Manish Kumar Mishra/ Vivek Bhardwaj/ Abhishek Kumar Singh	NTPC	For intimation of vulnerabilities and their closure
Suneel Kumar Palavalasa/ Some Nath Kundu	NTPC	For information please

Contents

Report Guide

The following table depicts the flow of this report.

Section	Description
Introduction	This section basically sets the tone of the vulnerability assessment and OT assessment report and draws the boundaries of the report in terms of its objective, scope, project timeline, project team from both sides.
Executive Summary	This section is prepared for quick management reference. It contains summary of observations from our review of network security test.
Detailed Report	This section presents the detail of the observations/ gaps found in OT Assessment along with the following: • Risk rating • Description of observation • Recommendation to address the risk • Proof of Concept • Revalidation Status

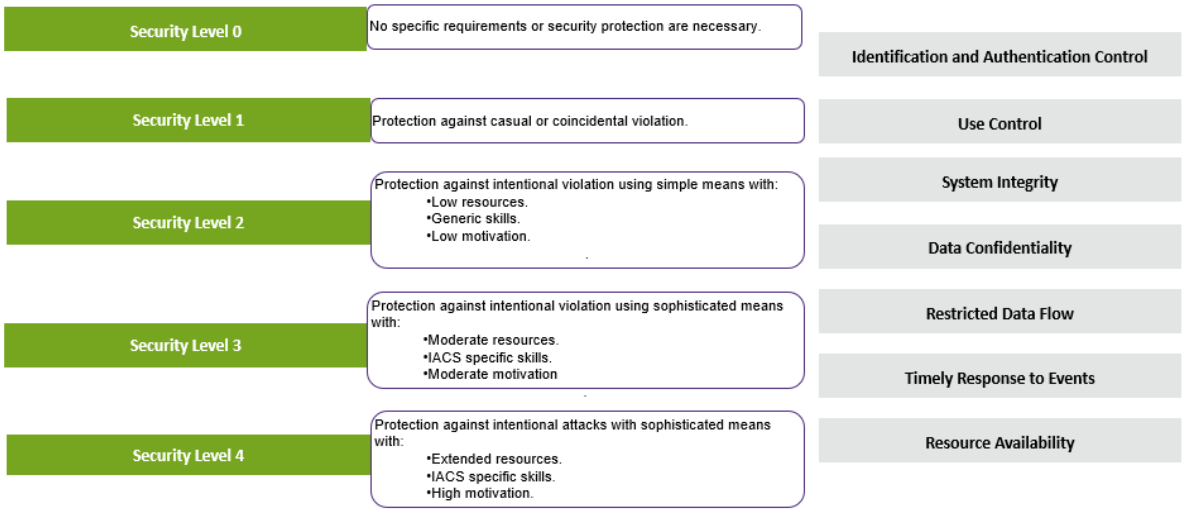
Introduction

Project Background

Grant Thornton Bharat LLP (GT) was engaged to conduct Network vulnerability assessment for **NTPC TANDA** OT assets. This network vulnerability assessment was conducted using the tools and techniques that a malicious attacker would use to try and compromise Security of OT Infrastructure with respect to **IEC62443 framework**.

IEC 62443 takes a risk-based approach to cyber security, which is based on the concept that it is neither efficient nor sustainable to try to protect all assets in equal measure. Instead, users must identify what is most valuable and requires the greatest protection and identify vulnerabilities.

Security Benchmarking using IEC 62443 Security Levels



The purpose of this assessment is to identify technical as well as logical vulnerabilities in the publicly exposed assets and provide recommendations for risk mitigation that may arise on successful exploitation of these vulnerabilities. The idea behind this testing is to discover whether an attacker may leverage flaws in the applications and supporting infrastructure to compromise the security at **NTPC TANDA**.

Project Timeline and Team

Cycle 1 - OT assessment timeline as follows:

Assessment Start Date	Assessment End Date
08-12-2022	14-12-2-22

Cycle 1 - Following team member was involved in this assessment:

GT Security Team	Contact Information
Akhil Kumar Agile	M: +91 8309008428 E: akhilkumar.agile@in.gt.com

Cycle -1 - Revalidation & Cycle-2 - OT assessment timeline as follows:

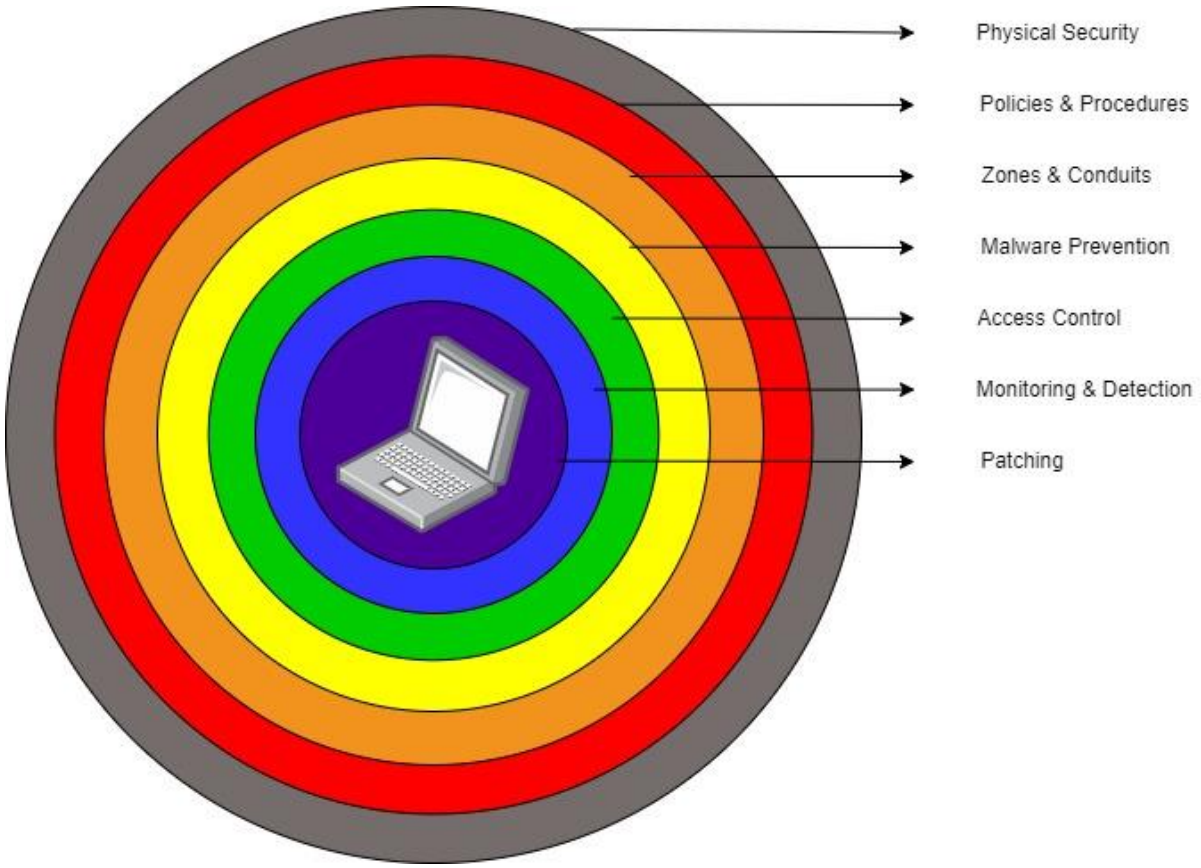
Unit Assessed	Start Date	End Date
Unit 1 – Unit 6	14-07-2023	21-07-2023

Cycle -1 - Revalidation & Cycle- 2 Following team member was involved in this assessment:

GT Security Team	Contact Information
Ujjwal Ranjan	M: +91 7739756835 E: Ujjwal.ranjan@in.gt.com

Executive Summary

In this report, we provide an overview of current visibility and insight into your OT environment from a risk point of view. We are providing the observation and recommendation based on the theories of defence in depth architecture which is explained in IEC 62443 for applying multiple countermeasures in a layered or stepwise manner.



This report provides detailed vulnerability and risk assessment conducted for **NTPC TANDA.** The Cycle 1 assessment was carried during Dec 2022 for which Revalidation of Cycle-1 & Assessment of Cycle-2 was carried during July'2023.

Cycle - 2:
C&I

1. Active assessment / Passive Assessment has not been carried out as all are in running condition
2. Physical assessment activity has been carried out.
3. Firewall rules and policies were reviewed.

Network Architecture

Existing network architecture reviewed and based on that proposed a new architecture.

Station LAN

1. Active assessment was carried out for stage 2 station LAN.

Electrical

1. Passive assessment was performed on SAS network.

2. Physical assessment was performed.

Note: Based on the assessment, risk mitigation and remediation are needed to reduce the risk of nation-level threat vector and improve the cyber posture.

C&I Department

Observations:

1. It has been observed that as of now there is no biometric lock in any programmer room of all units. Hence, it is recommended to have biometric lock to ensure physical Security.
2. It has been observed that site is managing the Asset list through excel based approach, but IPs of all devices is missing in that sheet. Hence, it is recommended to have up to date asset list with IP addresses or adopt some tool-based asset management technique which will increase the visibility of assets in your infrastructure.
3. It has also been observed that the no workstation & Servers have unique and strong password, also the password policy is not enforced in any system. Hence, it is recommended to have unique and strong password for all devices which must be updated in 90 to 180 days.
4. It has also been observed that Anti-Virus installed in all workstation & servers are outdated and there is no mechanism of its updating is available with site. So, it is recommended to adopt mechanism for AV patch update. Also make sure that the mechanism must be documented and in accordance with respective OEM.
5. As per the discussion with site Spoc regarding the scrap policy, it has been observed that all the workstation, server and field devices which are defected is declared as e-scrap and is directly sent to central store for scrapping. Hence, it is recommended to remove the hard disk for every device before scrapping it and that hard disk must be retained by the C&I Department.
6. It has been observed that almost all operator workstation is running on engineer account including UCR of all units and offsites. Hence, it is recommended to run all OWS on operator account with having very less or no privilege.
7. It has been observed all the group policies like account lockout, audit, advance audit, software restriction policies are not configured in any of the system installed. Hence, it is recommended to configure those policies.
8. It has been observed that many of the devices are running on obsolete OS i.e., Windows XP or Windows Server 2012 R2 which is going to obsolete in oct 2023. Hence, it is recommended to Upgrade the OS for all the outdated devices.
9. It has been observed that there is no role-based account has been created. There are the common users found with different privilege such as operator, engineer and administrator. When common user account used by different individual cannot create audit log for individual activity. Hence, it is recommended to configure role-based account.
10. It has also been observed that as of now the site have no patching mechanism and none of the devices is patched with latest OS updated. Hence, it is recommended to adopt some documented patching mechanism and perform this activity after a fixed interval of time. The time interval for patching will be decided by local cyber security response team and that also must be documented in same.

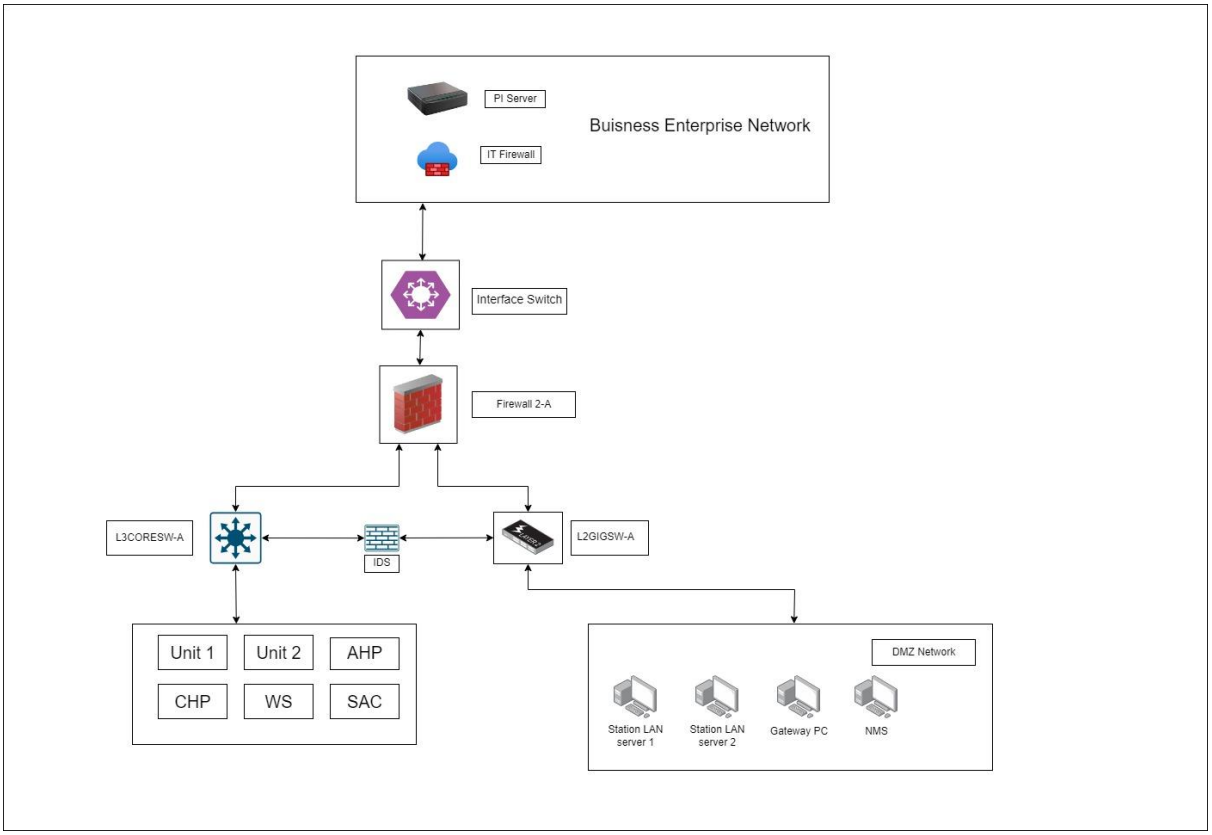
11. It has been observed that USB storage devices is enabled in few devices. It is recommended to disable the USB status in all workstations and servers and privilege to access the registry is only given to administrator.
12. It has been observed that OS firewall is disabled in all servers and workstation. It is recommended to enable the firewall in all devices.
13. It has been observed that several OS ports like port 80,135-139, 443, 445 etc. are found open and several services such as DHCP Client, DCOM+, etc. are running in all servers and workstation. These ports and services possess many vulnerabilities and provide the gateway for any kind of intrusion on the HMI. Hence, it is recommended to get a list of ports & services used by the application installed by OEM and close all the remaining unused ports and stop the services which are not required.

Note: All these observations belong to all stages and their offsites as well.

Network Architecture Review

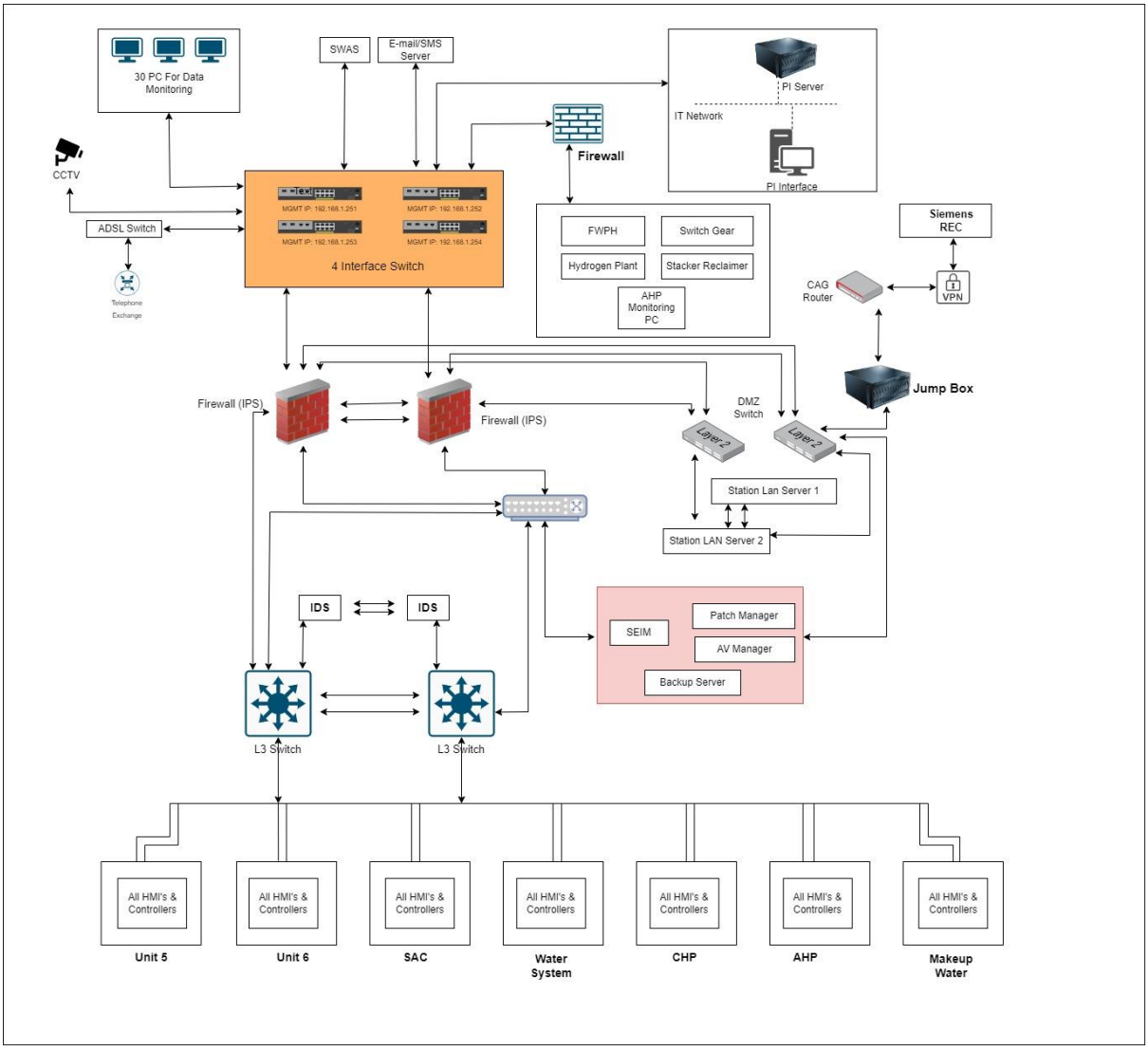
Existing Network Architecture

Below is the existing architecture of OT environment of NTPC Tanda.



Proposed Network Architecture

Below is proposed architecture which include security control implementation as ISA99/IEC62443 and CEA guidelines.



Recommendations:

Recommendations:

1. Integration of cyber stack with DCS which include below mentioned components:

    - **Centralized Patch Manager**: This Server ensure consistent and timely patching, reducing the risk of security breaches and improving overall system stability. This component follows server-client architecture where Patch Manager will act as a server and DCS workstations & Servers act as a client and validated OS patches are imported in Patch Manager via CD and Patch Manager automatically deploy patches in agents.

- **Centralized Antivirus Manager**: This component follows server-client architecture where Antivirus Manager will act as a server and DCS workstations act as a client and validated AV definitions are imported in AV Manager via CD and AV Manager automatically deploy definitions in agents.
- **Backup/Recovery server:** The role of this component is to take schedule backup of DCS critical assets and to recover the workstations if workstation got corrupted. This component also follows server-client based mechanism.
- **SEIM:** The role of this Server is to collect, analyse, and correlate security event logs from various sources within an OT network. It provides a centralized view of security events, enables threat detection, incident response, and compliance monitoring. This Server has features like log management, real-time monitoring, incident management, and reporting.

2. **Firewall:** It is recommended to place one firewall between 4 Interface Switches and Hydrogen Plant to eliminate any kind of unforeseen event to FWPH and Hydrogen Plant which is critical in nature for plant safety**.**

Jump Box: This device is used to provide controlled remote access. In existing scenario, there is no remote mechanism available with the site. By providing a jump box, only one remote session takes place at a time. All activity log gets generated, and this event gets recorded.

Firewall

Recommendations:

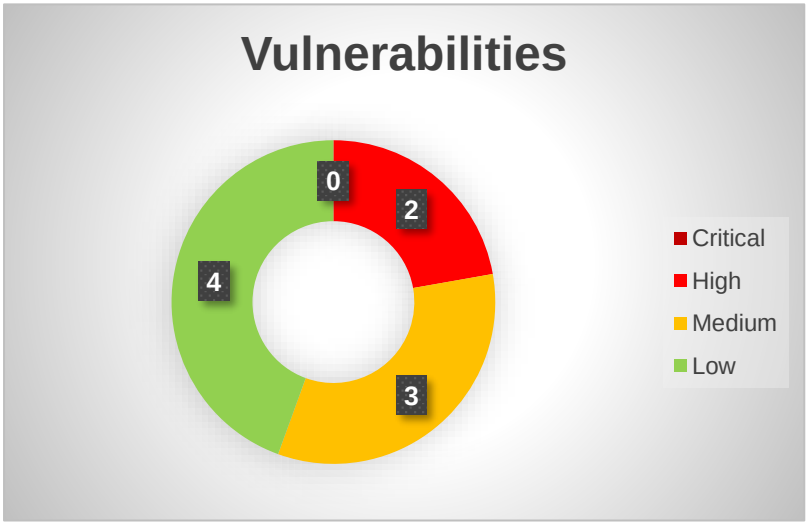
1. It is recommended to update the firewall to the latest firmware version.
2. Disable ping (ICMP) response on WAN port.
3. Disable UPnP (Universal plug-and-play).
4. Disable IDENT (i.e., port 113).
5. Disable remote management of the firewall.
6. The setting for a firewall policy should be as specific as possible. Do not allow ‘Any’ source or destination port and protocol also in any defined rule.
7. Periodic check for incoming/outgoing traffic security policy.
8. Allow only HTTPS access to the GUI and SSH access to the CLI.
9. Set up two-factor authentication for administrator.
10. Modify administrator account lockout duration and threshold values.
11. It is recommended that all management access from the internet is turned off.
12. Ensure that your SNMP setting are using SNMPv3 with encryption.
13. Default user account should be disabled and default password must be changed.

Vulnerability Summary

Domain	Critical	High	Medium	Low	Total
Vulnerability Assessment	0	2	3	4	9

Observation Summary

The chart given below represents the vulnerabilities found during network Vulnerability Assessment.



Vulnerability Assessment Test Observations

The below table illustrates the distribution of observations of Vulnerability Assessment based on the risk categorization i.e. Critical, High, Medium and Low

Vulnerabilities & Impact	Affected IP	Risk	Observations	Recommendations	Status
SSL Certificate Signed Using Weak Hashing Algorithm **Impact:** An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.	172.18.160.50	**High**	It has been observed that SSL certificate is signed using SHA-1 With RSA Encryption.	It is recommended to sign SSL certificate using strong encryption algorithm such as SHA-512. **References:** https://tools.ietf.org/html/rfc3279	**OPEN**
SSL Medium Strength Cipher Suites Supported (SWEET32) **Impact:** The remote host supports the use of SSL ciphers that offer medium strength encryption that it is considerably easier to circumvent medium strength encryption if the	172.18.160.50	**High**	It has been observed that SSL is using medium strength encryption such as DES-CBC3-SHA which can be easily compromised if the attacker is on the same physical network.	It is recommended to reconfigure the affected application, if possible, to avoid use of medium strength ciphers. **References:** https://www.openssl.org/blog/blog/2016/08/24/sweet32/	**OPEN**

attacker is on the same physical network.					
SSL RC4 Cipher Suites Supported (Bar Mitzvah) **Impact:** If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.	172.18.160.50	Medium	It has been observed that remote host is using weak cipher suite such as MD5 and SHA-1.	It is recommended to reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support. **References:** https://www.rc4nomore.com/ http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf	**OPEN**
TLS Version 1.1 Protocol Deprecated **Impact:** Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1. Hence an attacker can perform man-in-the-middle attack against the remote host.	172.18.160.50	Medium	It has been observed that remote host supports TLS version 1.1.	It is recommended to enable support for TLS 1.2 and/or 1.3 and disable support for TLS 1.1. **References:** https://datatracker.ietf.org/doc/html/rfc8996	**OPEN**
Unencrypted Telnet Server **Impact:** An attacker may eavesdrop on a Telnet session and obtain credentials or other sensitive information. Use of SSH is preferred	172.18.160.50	Medium	It is observed SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.	It is recommended to Disable the Telnet service and use SSH instead. **References:** How to Disable Telnet and Enable SSH on Cisco IOS Devices (networkstraining.com)	**OPEN**

nowadays as it protects credentials from eavesdropping and can tunnel additional data streams such as the X11 session.					
SSH Server CBC Mode Ciphers Enabled. **Impact:** The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.	172.18.160.50	**Low**	It was observed that the SSH server is configured to use Cipher Block Chaining.	It is recommended to contact the vendor or consult product documentation to disable CBC mode cipher encryption and enable CTR or GCM cipher mode encryption.	**OPEN**
SSH Weak Key Exchange Algorithms Enabled **Impact:** An attacker can easily exploit the remote SSH server that is configured to allow weak key exchange algorithms.	172.18.160.50	**Low**	It has been observed that remote host allow weak key exchange algorithms.	It is recommended to disable the weak key exchange algorithms. **References:** SSH Weak Key Exchange Algorithms Enabled - Virtue Security	**OPEN**
SSH Weak MAC Algorithms Enabled **Impact:** An attacker may try to exploit the host as the remote SSH server is configured to allow key exchange algorithms which are considered weak.	172.18.160.50	**Low**	It has been observed that the remote SSH server is configured to allow key exchange algorithms which are considered weak.	It is recommended to contact the vendor or consult product documentation to disable the weak algorithms. **References:** Disable SSH Weak MAC Algorithms in Linux - DbAppWeb.com	**OPEN**
SSL Certificate Chain Contains RSA Keys Less Than 2048 bits. **Impact:** According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014, must be at least 2048 bits. Some browser SSL	172.18.160.50	**Low**	It was observed that at least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits	It is recommended to replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.	**OPEN**

implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.					

Revalidation

C&I

1. Revalidation of Active assessment / Passive Assessment has not been carried out as all are in running condition
2. Revalidation of Physical assessment activity has been carried out.

Station LAN

1. Revalidation of Active assessment was carried out for stage 2 station LAN.

Electrical

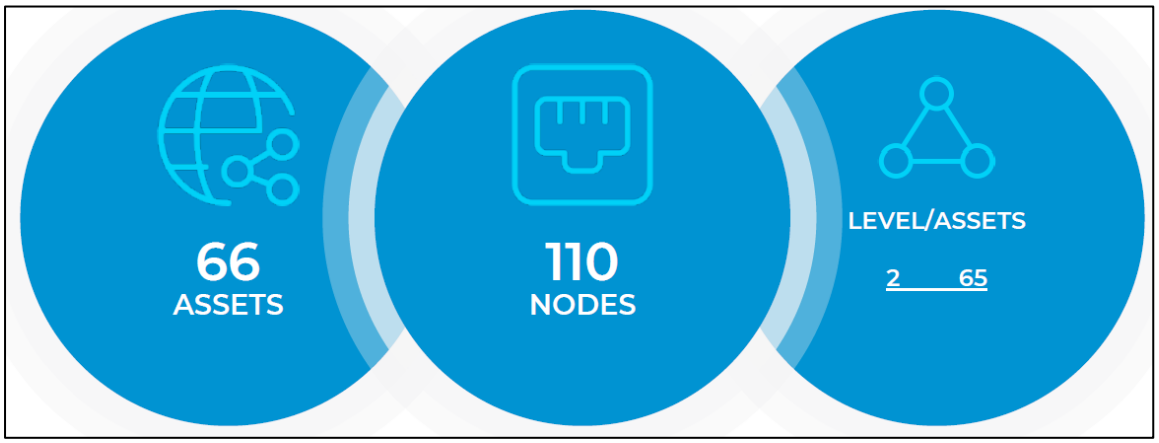
1. Revalidation of active assessment was not carried out as it is same.

Unit 1

Asset Classification

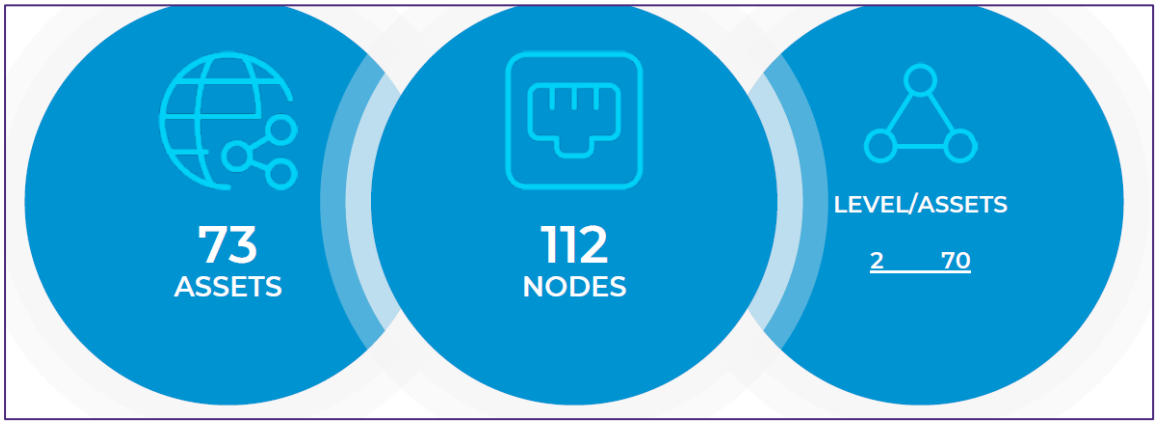
DCS 1 (BHEL Make)

The assessment was able to identify 66 all devices and discovered 52 vulnerabilities.
Based on the assessment, risk mitigation and remediation are needed to reduce the risk of nation-level threat vector and improve the cyber posture.



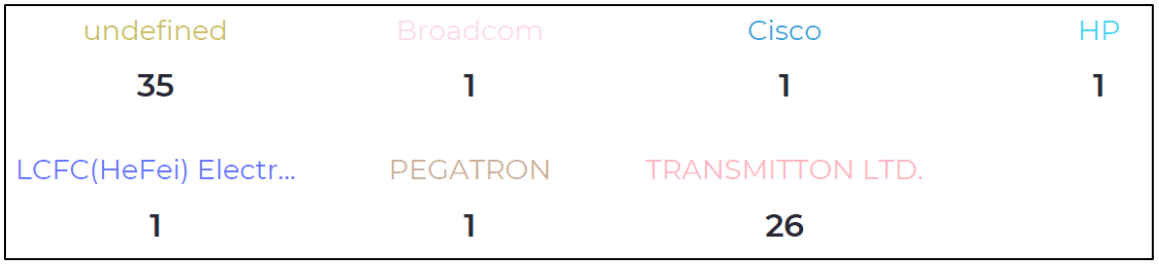
DCS 2(Emerson Make)

The assessment was able to identify 73 all devices and discovered 48 vulnerabilities.
Based on the assessment, risk mitigation and remediation are needed to reduce the risk of nation-level threat vector and improve the cyber posture.



Vendors

DCS 1



DCS 2

undefined	Cisco	Dell Inc.	Emerson Process
45	11	6	8
LCFC(HeFei) Electr...	VMware, Inc.		
2	1		

Asset Types

DCS 1

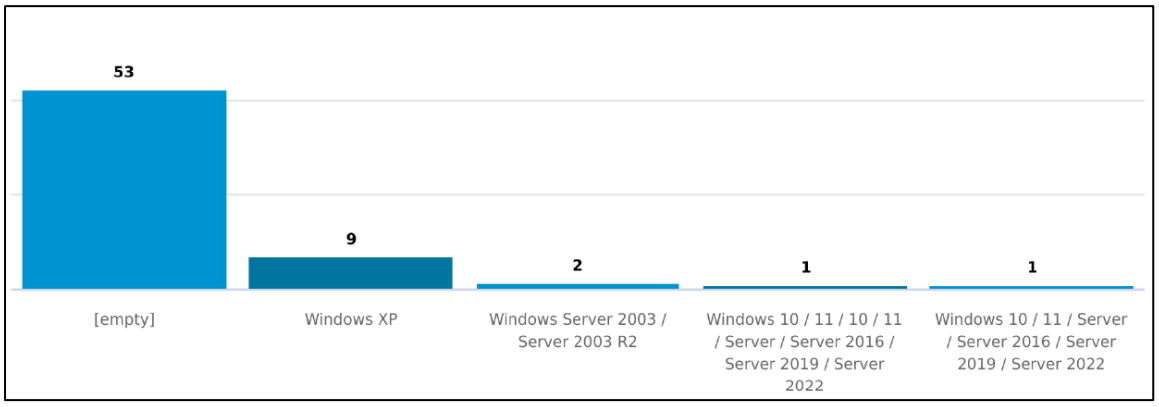
-	52	computer	13	switch	1

DCS 2

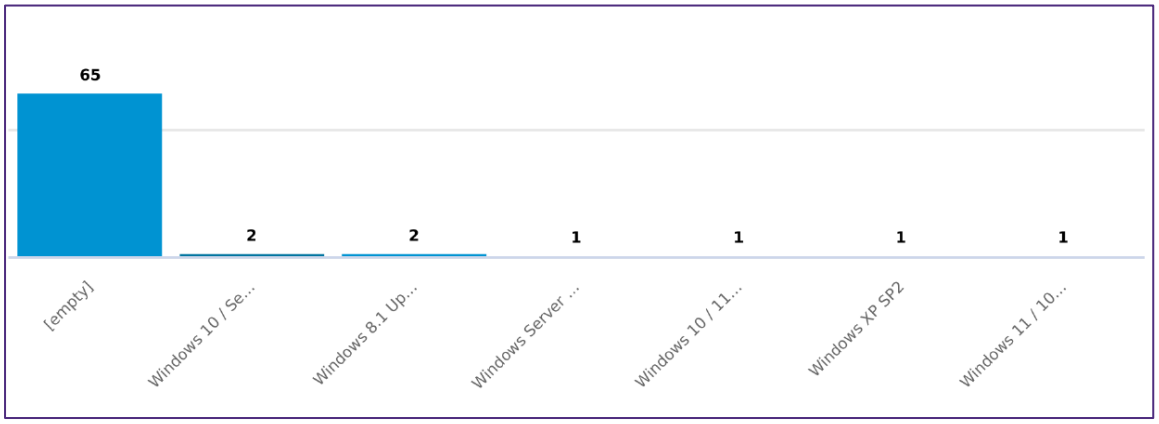
-	62	WAP	1	computer	7	router	2
switch	1						

Operating systems

DCS 1



DCS 2



Risk

Vulnerability Score

DCS 1

GT Risk Assessment Report provides a comprehensive risk analysis related to network behaviour and assets. Based on overall assessment for NTPC TANDA, all network risk score is 6.8 (Medium risk)

NAME	TYPE	OS/FIRMWARE	COUNT	SCORE DISTRIBUTION	SCORE GROUPS (Low, Medium, High)
ws-c2950c-24	switch	Firmware: 12.1(22)ea6	52		2 40 9
1OPSTN_5	computer	Windows XP	686		29 463 194
1ENGG	computer	Windows XP	686		29 463 194
1LVS_1	computer	Windows XP	686		29 463 194
1LVS_2	computer	Windows XP	686		29 463 194
1LVS_3	computer	Windows XP	686		29 463 194
1OPSTN_2	computer	Windows XP	686		29 463 194
1OPSTN_3	computer	Windows XP	686		29 463 194
9OPC	computer	Windows XP	686		29 463 194
1OPSTN_4	computer	Windows XP	686		29 463 194
WCCBLRLAP660	computer	Windows 10 / 11 / 10 / 11 / Server / Server 2016 / Server 2019 / Server 2022	8		1 7

Assets with confirmed CPEs	1
Assets with Firmware Discovered	110
Number of Hosts with Vulnerabilities	1
Number of Vulnerabilities	52
Vulnerability Average Score	6.8

DCS 2

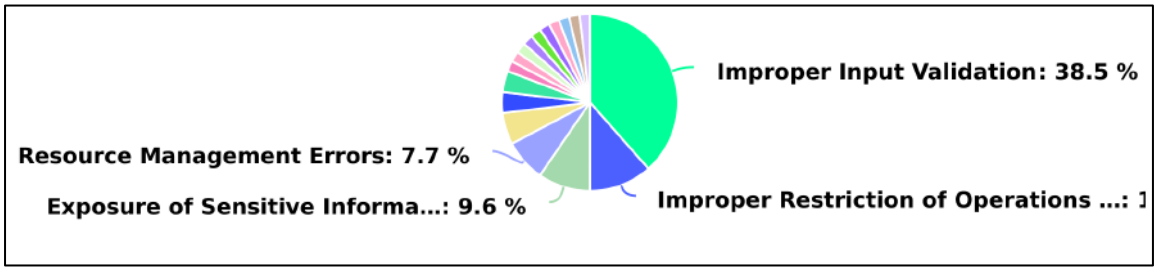
GT Risk Assessment Report provides a comprehensive risk analysis related to network behaviour and assets. Based on overall assessment for NTPC TANDA, all network risk score is 6.7 (Medium risk)

NAME	TYPE	OS/FIRMWARE	COUNT	SCORE DISTRIBUTION	SCORE GROUPS (Low, Medium, High)
ws-c2950-24	switch	Firmware: 12.1(22)ea5	48		2 37 8
drop200	computer	Windows Server 2012 R2 Update 1	2153		46 1 698 409
WCCBLRLAP660	WAP	Windows XP SP2	1027		21 498 508

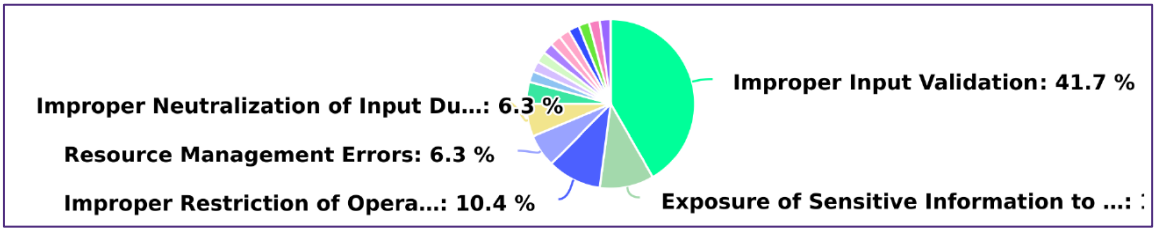
Assets with confirmed CPEs	1
Assets with Firmware Discovered	112
Number of Hosts with Vulnerabilities	1
Number of Vulnerabilities	48
Vulnerability Average Score	6.7

Vulnerabilities per type

DCS 1



DCS 2



Top 30 Vulnerabilities on Network Devices

Grant Thornton
An instinct for growth™

DCS 1

CVE	LABEL	CVE SCORE	CWE NAME	CVE CREATION TIME	TIME
CVE-2006-4950	00:16:9d:fd:da:cf	10.0	Improper Input Validation	2006-09-23 10:07:00	2022-12-13 14:28:28
CVE-2017-12240	00:16:9d:fd:da:cf	9.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-09-29 01:34:00	2022-12-13 14:28:28
CVE-2007-2586	00:16:9d:fd:da:cf	9.3	Incorrect Authorization	2007-05-10 00:19:00	2022-12-13 14:28:28
CVE-2007-5552	00:16:9d:fd:da:cf	9.3	Numeric Errors	2007-10-18 20:17:00	2022-12-13 14:28:28
CVE-2007-5381	00:16:9d:fd:da:cf	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer	2007-10-12 01:17:00	2022-12-13 14:28:28
CVE-2019-16009	00:16:9d:fd:da:cf	8.8	Cross-Site Request Forgery (CSRF)	2020-09-23 01:15:00	2022-12-13 14:28:28
CVE-2017-6743	00:16:9d:fd:da:cf	8.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-07-17 21:29:00	2022-12-13 14:28:28
CVE-2017-3864	00:16:9d:fd:da:cf	8.6	Improper Input Validation	2017-03-22 19:59:00	2022-12-13 14:28:28
CVE-2016-6380	00:16:9d:fd:da:cf	8.1	Improper Input Validation	2016-10-05 20:59:00	2022-12-13 14:28:28
CVE-2011-0946	00:16:9d:fd:da:cf	7.8	Improper Input Validation	2011-10-03 23:55:00	2022-12-13 14:28:28
CVE-2011-3279	00:16:9d:fd:da:cf	7.8	Improper Input Validation	2011-10-03 23:55:00	2022-12-13 14:28:28
CVE-2013-1142	00:16:9d:fd:da:cf	7.8	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	2013-03-28 23:55:00	2022-12-13 14:28:28
CVE-2009-2051	00:16:9d:fd:da:cf	7.8	Improper Input Validation	2009-08-27 17:00:00	2022-12-13 14:28:28
CVE-2021-34699	00:16:9d:fd:da:cf	7.7	Interpretation Conflict	2021-09-23 03:15:00	2022-12-13 14:28:28
CVE-2017-3857	00:16:9d:fd:da:cf	7.5	Uncontrolled Resource Consumption	2017-03-22 19:59:00	2022-12-13 14:28:28
CVE-2003-0647	00:16:9d:fd:da:cf	7.5	Improper Restriction of Operations within the Bounds of a Memory Buffer	2003-08-27 04:00:00	2022-12-13 14:28:28
CVE-2022-20726	00:16:9d:fd:da:cf	7.5	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2022-04-15 15:15:00	2022-12-13 14:28:28
CVE-2022-20724	00:16:9d:fd:da:cf	7.5	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	2022-04-15 15:15:00	2022-12-13 14:28:28
CVE-1999-0293	00:16:9d:fd:da:cf	7.5	Improper Input Validation	1998-01-01 05:00:00	2022-12-13 14:28:28
CVE-2019-12655	00:16:9d:fd:da:cf	7.5	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	2019-09-25 21:15:00	2022-12-13 14:28:28
CVE-2016-1409	00:16:9d:fd:da:cf	7.5	Improper Input Validation	2016-05-29 22:59:00	2022-12-13 14:28:28
CVE-2016-6384	00:16:9d:fd:da:cf	7.5	Improper Input Validation	2016-10-05 17:59:00	2022-12-13 14:28:28
CVE-2016-6393	00:16:9d:fd:da:cf	7.5	Resource Management Errors	2016-10-05 20:59:00	2022-12-13 14:28:28
CVE-2016-6415	00:16:9d:fd:da:cf	7.5	Exposure of Sensitive Information to an Unauthorized Actor	2016-09-19 01:59:00	2022-12-13 14:28:28
CVE-2019-1748	00:16:9d:fd:da:cf	7.4	Improper Certificate Validation	2019-03-28 00:29:00	2022-12-13 14:28:28
CVE-2008-1150	00:16:9d:fd:da:cf	7.1	Resource Management Errors	2008-03-27 17:44:00	2022-12-13 14:28:28
CVE-2007-5551	00:16:9d:fd:da:cf	7.1	Improper Restriction of Operations within the Bounds of a Memory Buffer	2007-10-18 20:17:00	2022-12-13 14:28:28
CVE-2008-1151	00:16:9d:fd:da:cf	7.1	Resource Management Errors	2008-03-27 17:44:00	2022-12-13 14:28:28
CVE-2008-4963	00:16:9d:fd:da:cf	7.1	Improper Input Validation	2008-11-06 15:55:00	2022-12-13 14:28:28
CVE-2008-4609	00:16:9d:fd:da:cf	7.1	Configuration	2008-10-20 17:59:00	2022-12-13 14:28:28

DCS 2

CVE	LABEL	CVE SCORE	CWE NAME	CVE CREATION TIME	TIME
CVE-2006-4950	00:1d:e5:ac:28:54	10.0	Improper Input Validation	2006-09-23 10:07:00	2022-12-15 21:59:08
CVE-2017-12240	00:1d:e5:ac:28:54	9.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-09-29 01:34:00	2022-12-15 21:59:08
CVE-2007-2586	00:1d:e5:ac:28:54	9.3	Incorrect Authorization	2007-05-10 00:19:00	2022-12-15 21:59:08
CVE-2007-5552	00:1d:e5:ac:28:54	9.3	Numeric Errors	2007-10-18 20:17:00	2022-12-15 21:59:08
CVE-2017-6743	00:1d:e5:ac:28:54	8.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-07-17 21:29:00	2022-12-15 21:59:08

CVE	LABEL	CVE SCORE	CWE NAME	CVE CREATION TIME	TIME
CVE-2019-16009	00:1d:e5:ac:28:54	8.8	Cross-Site Request Forgery (CSRF)	2020-09-23 01:15:00	2022-12-15 21:59:08
CVE-2017-3864	00:1d:e5:ac:28:54	8.6	Improper Input Validation	2017-03-22 19:59:00	2022-12-15 21:59:08
CVE-2016-6380	00:1d:e5:ac:28:54	8.1	Improper Input Validation	2016-10-05 20:59:00	2022-12-15 21:59:08
CVE-2011-3279	00:1d:e5:ac:28:54	7.8	Improper Input Validation	2011-10-03 23:55:00	2022-12-15 21:59:08
CVE-2009-2051	00:1d:e5:ac:28:54	7.8	Improper Input Validation	2009-08-27 17:00:00	2022-12-15 21:59:08
CVE-2011-0946	00:1d:e5:ac:28:54	7.8	Improper Input Validation	2011-10-03 23:55:00	2022-12-15 21:59:08
CVE-2013-1142	00:1d:e5:ac:28:54	7.8	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	2013-03-28 23:55:00	2022-12-15 21:59:08
CVE-2021-34699	00:1d:e5:ac:28:54	7.7	Interpretation Conflict	2021-09-23 03:15:00	2022-12-15 21:59:08
CVE-1999-0293	00:1d:e5:ac:28:54	7.5	Improper Input Validation	1998-01-01 05:00:00	2022-12-15 21:59:08
CVE-2017-3857	00:1d:e5:ac:28:54	7.5	Uncontrolled Resource Consumption	2017-03-22 19:59:00	2022-12-15 21:59:08
CVE-2016-1409	00:1d:e5:ac:28:54	7.5	Improper Input Validation	2016-05-29 22:59:00	2022-12-15 21:59:08
CVE-2022-20724	00:1d:e5:ac:28:54	7.5	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	2022-04-15 15:15:00	2022-12-15 21:59:08
CVE-2016-6415	00:1d:e5:ac:28:54	7.5	Exposure of Sensitive Information to an Unauthorized Actor	2016-09-19 01:59:00	2022-12-15 21:59:08
CVE-2016-6393	00:1d:e5:ac:28:54	7.5	Resource Management Errors	2016-10-05 20:59:00	2022-12-15 21:59:08
CVE-2016-6384	00:1d:e5:ac:28:54	7.5	Improper Input Validation	2016-10-05 17:59:00	2022-12-15 21:59:08
CVE-2019-12655	00:1d:e5:ac:28:54	7.5	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	2019-09-25 21:15:00	2022-12-15 21:59:08
CVE-2003-0647	00:1d:e5:ac:28:54	7.5	Improper Restriction of Operations within the Bounds of a Memory Buffer	2003-08-27 04:00:00	2022-12-15 21:59:08
CVE-2022-20726	00:1d:e5:ac:28:54	7.5	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2022-04-15 15:15:00	2022-12-15 21:59:08
CVE-2008-4609	00:1d:e5:ac:28:54	7.1	Configuration	2008-10-20 17:59:00	2022-12-15 21:59:08
CVE-2008-4963	00:1d:e5:ac:28:54	7.1	Improper Input Validation	2008-11-06 15:55:00	2022-12-15 21:59:08
CVE-2008-1151	00:1d:e5:ac:28:54	7.1	Resource Management Errors	2008-03-27 17:44:00	2022-12-15 21:59:08
CVE-2008-1150	00:1d:e5:ac:28:54	7.1	Resource Management Errors	2008-03-27 17:44:00	2022-12-15 21:59:08
CVE-2007-5551	00:1d:e5:ac:28:54	7.1	Improper Restriction of Operations within the Bounds of a Memory Buffer	2007-10-18 20:17:00	2022-12-15 21:59:08
CVE-2007-5548	00:1d:e5:ac:28:54	6.9	Improper Restriction of Operations within the Bounds of a Memory Buffer	2007-10-18 20:17:00	2022-12-15 21:59:08
CVE-2008-5230	00:1d:e5:ac:28:54	6.8	Cryptographic Issues	2008-11-25 23:30:00	2022-12-15 21:59:08

Vulnerability summary

DCS 1

Malware detected	0
Different Operating Systems	5
Different Types of Technologies	8
Attempted Links to Public Internet	0
Multi-homed Assets	0
Different Firmware Versions	2
Clients Accessing SMB Shares	0
Insecure Protocol Links in the Environment	1

DCS 2

Malware detected	0
Different Operating Systems	7
Different Types of Technologies	7
Attempted Links to Public Internet	0
Multi-homed Assets	23
Different Firmware Versions	2
Clients Accessing SMB Shares	7
Insecure Protocol Links in the Environment	106

Devices Vulnerability Summary

Domain	Critical	High	Medium	Low	Total
Vulnerability Assessment	8	4	6	1	19
Re-validation(closed)	0	0	0	0	0
Re-validation(open)	8	4	6	1	19

Observation Summary

The chart given below represents the vulnerabilities found during network vulnerability testing:

Fig:1

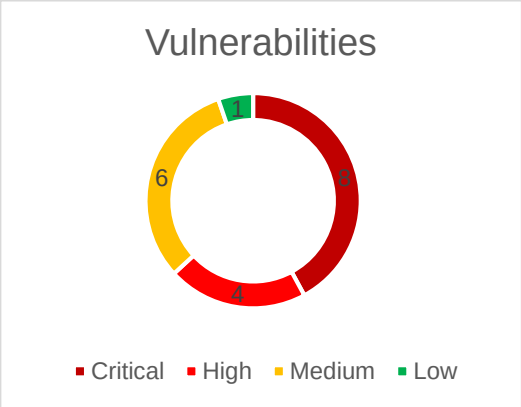


Fig:2

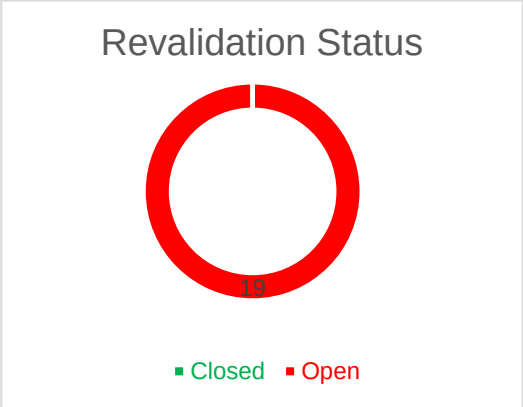


Figure 1: Vulnerability Assessment Test Observations

Illustrates the distribution of observations of Vulnerability testing based on the risk categorization i.e., Critical, High, Medium, and Low.

Figure 2: Vulnerability Assessment Test Observations- Revalidation

Illustrates the closure of Vulnerabilities based on the categorization i.e., Closed, Open.

Note:

Closed: Count considered having vulnerability in all the IP addresses as closed.

Open: Count considered having vulnerability in minimum one IP address as open/unreachable, it may have more different IP addresses which may have the same vulnerability as closed.

Vulnerability Assessment Test Observations

The below table illustrates the distribution of observations of Vulnerability testing based on the risk categorization i.e., Critical, High, Medium, and Low.

Vulnerabilities & Impact	Affected IP	Risk	Observations	Recommendations	Status	Revalidation status
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check) **Impact:**	172.16.160.16 172.17.160.16	**Critical**	It was observed that the remote host is affected by a remote code execution vulnerability.	It is recommended to implement patches for Windows XP, 2003, 2008, 7, and 2008 r2 released by Microsoft.	**Open**	**Open**

An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.						
Microsoft Windows Server 2003 Unsupported Installation Detection. **Impact:** Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.	172.16.160.14	**Critical**	It is observed that the remote operating system is no longer supported.	It is recommended to upgrade to a version of Windows that is currently supported.	**Open**	**Open**
Microsoft Windows XP Unsupported Installation Detection. **Impact:** Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.	172.16.160.10 172.16.160.12 172.16.160.18 172.16.160.20 172.16.160.22 172.16.160.4 172.16.160.6 172.16.160.60 172.16.160.8 172.17.160.12 172.17.160.18 172.17.160.20 172.17.160.22 172.17.160.4 172.17.160.6 172.17.160.60 172.17.160.8	**Critical**	It is observed that the remote operating system is no longer supported.	It is recommended to upgrade to a version of Windows that is currently supported.	**Open**	**Open**
MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check) **Impact:**	172.16.160.20 172.16.160.22 172.16.160.4 172.16.160.6 172.17.160.20 172.17.160.22 172.17.160.4 172.17.160.6	**Critical**	It is observed that an arbitrary code can be executed on the remote host due to a flaw in the SMB implementation.	It is recommended to upgrade to the patches provided by Microsoft for Windows 2000, XP, and 2003. Reference:	**Open**	**Open**

The remote version of Windows contains a flaw in the Server Message Block (SMB) implementation that may allow an attacker to execute arbitrary code on the remote host. An attacker does not need to be authenticated to exploit this flaw.				https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2005/ms05-027		
MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check) **Impact:** The remote host is vulnerable to a buffer overrun in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with 'SYSTEM' privileges.	172.16.160.20 172.16.160.22 172.16.160.4 172.16.160.6 172.17.160.20 172.17.160.22 172.17.160.4 172.17.160.6	**Critical**	It is observed that an arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.	It is recommended to upgrade to the patches provided by Microsoft for Windows 2000, XP, and 2003. References: https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2006/ms06-040	**Open**	**Open**
MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check) **Impact:** An unauthenticated, remote attacker can exploit this, via a specially crafted RPC request, to execute arbitrary code with 'System' privileges.	172.16.160.10 172.16.160.12 172.16.160.14 172.16.160.20 172.16.160.22 172.16.160.4 172.16.160.6 172.16.160.60 172.16.160.8 172.17.160.12 172.17.160.20 172.17.160.22 172.17.160.4 172.17.160.6 172.17.160.60 172.17.160.8	**Critical**	It is observed that the remote Windows host is affected by a remote code execution vulnerability.	It is recommended to upgrade to the patches provided by Microsoft for Windows 2000, XP, and 2003.	**Open**	**Open**

MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check) **Impact:** The remote host is affected by a memory corruption vulnerability in SMB that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host.	172.16.160.10 172.16.160.12 172.16.160.14 172.16.160.18 172.16.160.20 172.16.160.22 172.16.160.4 172.16.160.6 172.16.160.60 172.16.160.8 172.17.160.12 172.17.160.18 172.17.160.20 172.17.160.22 172.17.160.4 172.17.160.6 172.17.160.60 172.17.160.8	**Critical**	It is observed that it is possible to crash the remote host due to a flaw in SMB.	It is recommended to update set of patches for Windows 2000, XP, 2003, Vista and 2008 provided by Microsoft	**Open**	**Open**
Unsupported Windows OS (remote) **Impact:** The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.	172.16.160.10 172.16.160.12 172.16.160.14 172.16.160.18 172.16.160.20 172.16.160.22 172.16.160.4 172.16.160.6 172.16.160.60 172.16.160.8 172.17.160.12 172.17.160.18 172.17.160.20 172.17.160.22 172.17.160.4 172.17.160.6 172.17.160.60 172.17.160.8	**Critical**	It was observed that the remote version of Microsoft Windows is either missing a service pack or is no longer supported	It is recommended to upgrade to a supported service pack or operating system	**Open**	**Open**
MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check) **Impact:** The remote host is vulnerable to heap overflow in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with 'SYSTEM' privileges.	172.16.160.20 172.16.160.22 172.16.160.4 172.16.160.6 172.17.160.20 172.17.160.22 172.17.160.4 172.17.160.6	**High**	It was observed that an arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.	It is recommended to upgrade to the patches provided by Microsoft for Windows 2000, XP, and 2003.	**Open**	**Open**

In addition to this, the remote host is also affected by an information disclosure vulnerability in SMB that may allow an attacker to obtain portions of the memory of the remote host.						
MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) **Impact:** An arbitrary remote code vulnerability exists in the implementation of the Remote Desktop Protocol (RDP) on the remote Windows host. The vulnerability is due to the way that RDP accesses an object in memory that has been improperly initialized or has been deleted. If RDP has been enabled on the affected system, an unauthenticated, remote attacker could leverage this vulnerability to cause the system to execute arbitrary code by sending a sequence of specially crafted RDP packets to it.	172.16.160.16 172.17.160.16	**High**	It was observed that the remote Windows host could allow arbitrary code execution.	It is recommended to implement patches for Windows XP, 2003, 2008, 7, and 2008 r2 released by Microsoft.	**Open**	**Open**
MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY	172.16.160.10 172.16.160.12 172.16.160.14 172.16.160.18 172.16.160.20 172.16.160.22 172.16.160.4 172.16.160.6 172.16.160.60 172.16.160.8	**High**	It has been observed that device is not updated to the MS SMB security patch (MS17-010)	It is recommended to follow the below mentioned. Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT	**Open**	**Open**

) (WannaCry) (EternalRocks) (Petya) (uncredentialed check) **Impact:** An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148) - An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)	172.17.160.12 172.17.160.18 172.17.160.20 172.17.160.22 172.17.160.4 172.17.160.6 172.17.160.60 172.17.160.8			8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8. References: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010		
SMB NULL Session Authentication. **Impact:** The remote host is running and SMB protocol. It is possible to log into the browser or spoolss pipes using a NULL session (i.e., with no login or password). Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.	172.16.160.10 172.16.160.12 172.16.160.14 172.16.160.18 172.16.160.20 172.16.160.22 172.16.160.4 172.16.160.6 172.16.160.60 172.16.160.8 172.17.160.12 172.17.160.18 172.17.160.20 172.17.160.22 172.17.160.4 172.17.160.6 172.17.160.60 172.17.160.8	**High**	It is observed that it is possible to log into the remote host with a NULL session.	It is recommended to contact the product vendor for recommended solutions.	**Open**	**Open**

Microsoft Windows EFSRPC NTLM Reflection Elevation of Privilege (PetitPotam) (Remote). **Impact:** An unauthenticated, remote attacker can exploit this, by sending a specially-crafted EFSRPC request, to cause the affected host to connect to a malicious server. An attacker can then utilize an NTLM relay to impersonate the target host and authenticate against remote services.	172.16.160.14	Medium	It is observed that the remote host is affected by an NTLM reflection elevation of privilege vulnerability.	It is recommended to apply the updates supplied by the vendor. Optionally, refer to Microsoft's KB5005413 for mitigation guidance. RPC filters may also be implemented to block remote access to the interface UUIDs necessary for this exploit.	Open	Open
MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) **Impact:** Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.0. Hence an attacker can perform man-in-the-middle attack against the remote host.	172.16.160.14	Medium	It has been observed that the remote Windows host is affected by an elevation of privilege vulnerability.	It is recommended to implement the Microsoft released set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10. **References:** http://badlock.org/	Open	Open
Remote Desktop Protocol Server Man-in-the-Middle Weakness **Impact:** The MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.	172.16.160.16 172.17.160.16	Medium	It is observed the remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when	It is recommended to force the use of SSL as a transport layer for this service if supported, or/and. Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	Open	Open

			setting up encryption.	**References:** http://technet.microsoft.com/en-us/library/cc782610.aspx https://www.tenable.com/plugins/nessus/18405		
SMB Signing not required. **Impact:** An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.	172.16.160.10 172.16.160.12 172.16.160.14 172.16.160.18 172.16.160.20 172.16.160.22 172.16.160.4 172.16.160.6 172.16.160.60 172.16.160.8 172.17.160.12 172.17.160.18 172.17.160.20 172.17.160.22 172.17.160.4 172.17.160.6 172.17.160.60 172.17.160.8	**Medium**	It was observed that signing is not required on the remote SMB server.	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'.	**Open**	**Open**
Terminal Services Encryption Level is Medium or Low **Impact:** An attacker can eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.	172.16.160.16 172.17.160.16	**Medium**	It has been observed that the remote Terminal Services is t configured to use Medium cryptography.	It is recommended to Change RDP encryption level to High & FIPS Compliant **References:** https://techgenix.com/Windows_Terminal_Services/#:~:text=Medium%3A%20encrypts%20both%20the%20data%20sent%20from%20client,40%20bit%20key%2C%20depending%20on%20the%20client%20version.	**Open**	**Open**

Unencrypted Telnet Server **Impact:** Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server. SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.	172.16.200.201 172.16.200.202 172.16.200.203 172.16.200.204 172.16.200.205 172.17.200.201	Medium	It is observed that the remote Telnet server transmits traffic in cleartext.	It is recommended to disable the Telnet service and use SSH instead.	Open	Open
Terminal Services Encryption Level is not FIPS-140 Compliant **Impact:** The attacker observed the encryption setting used by the remote Terminal Services after the attacker easy to expose the all sensitive data	172.16.160.16 172.17.160.16	Low	It is observed the Client Compatible setting encrypts data sent between the client and the server at the maximum key strength supported by the client.	It is recommended to change RDP encryption level to: 4. FIPS Compliant **References:** https://www.tenable.com/plugins/nessus/30218	Open	Open

Asset Inventory detail

Inventory Overview

This section focuses on asset tracking, asset discovery and asset classification. These are the first steps for ensuring operational continuity, reliability and safety. They provide the user with a full context for security events and support routine procedures aimed at improving overall cyber hygiene. Creating an inventory of devices in the network, as well as understanding the relationships and connections between them, is a crucial component in network security.

Asset List DCS-1

Unit1_assets_DCS1.xlsx

Asset List DCS-2

Unit1_assets_1_DCS2.xlsx

Mapping of Vulnerabilities with Assets (DCS1)

Final Mapping of Assets:

Refer below excel file contains mapping of vulnerabilities & open ports with the assets, it provides the details of vulnerabilities observed in each asset.

U1_DCS1_Mapping of vulnerabilities wi

Mapping of Vulnerabilities with Assets (DCS2)

Final Mapping of Assets:

Refer below excel file contains mapping of vulnerabilities & open ports with the assets, it provides the details of vulnerabilities observed in each asset.

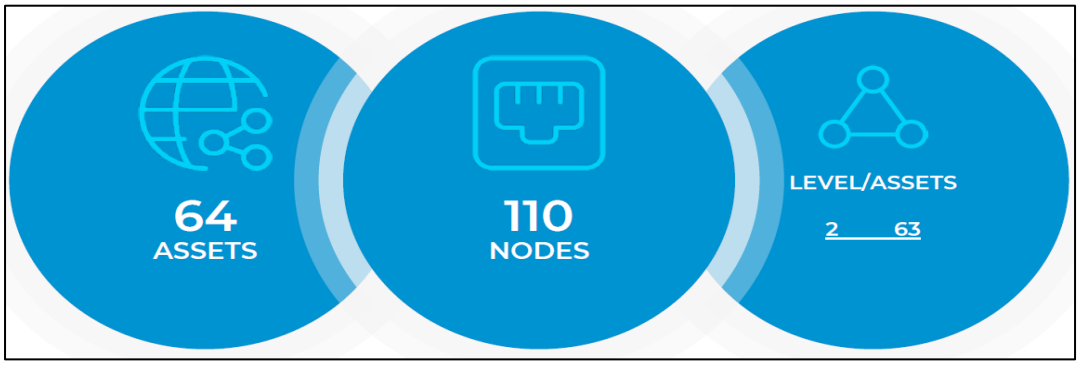
U1_DCS2_mapping of vulnerabilities wi

Unit 2

Asset Classification

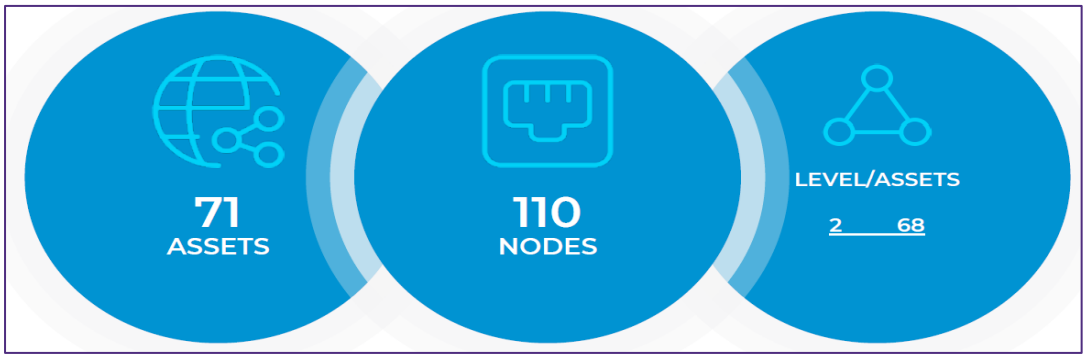
DCS 1 (BHEL Make)

The assessment was able to identify 64 all devices and discovered 52 vulnerabilities.
Based on the assessment, risk mitigation and remediation are needed to reduce the risk of nation-level threat vector and improve the cyber posture.



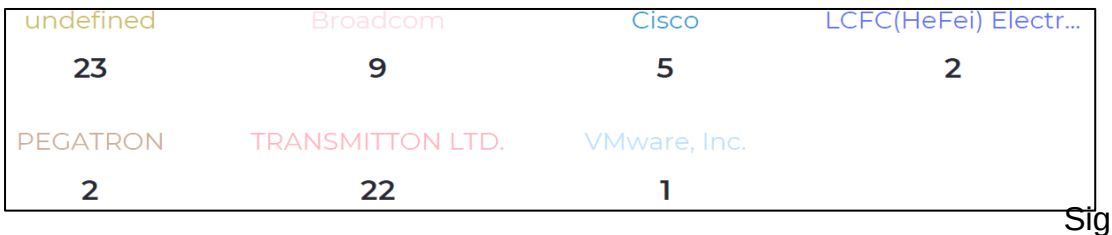
C&I – Unit -2 DCS 2 (Emerson Make)

The assessment was able to identify 71 all devices and discovered 47 vulnerabilities.
Based on the assessment, risk mitigation and remediation are needed to reduce the risk of nation-level threat vector and improve the cyber posture.



Vendors

C&I – Unit -2 DCS 1



C&I – Unit -2 DCS 2

undefined	Cisco	Dell Inc.	LCFC(HeFei) Electr...
40	7	6	2
MICRO INDUSTRIES	VMware, Inc.		
15	1		

Asset Types

C&I – Unit -2 DCS 1

-	50	WAP	1	computer	12	switch	1

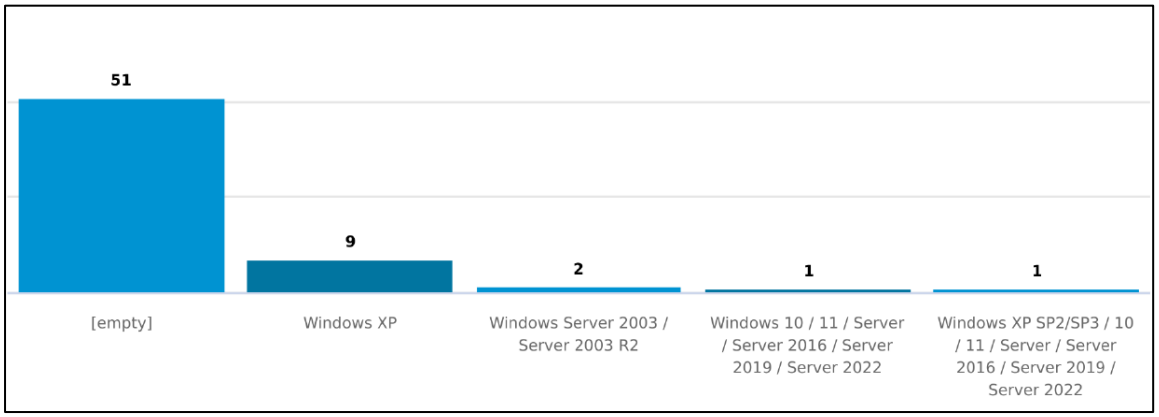
C&I – Unit -2 DCS 2

-	60	WAP	1	computer	7	router	2
switch	1						

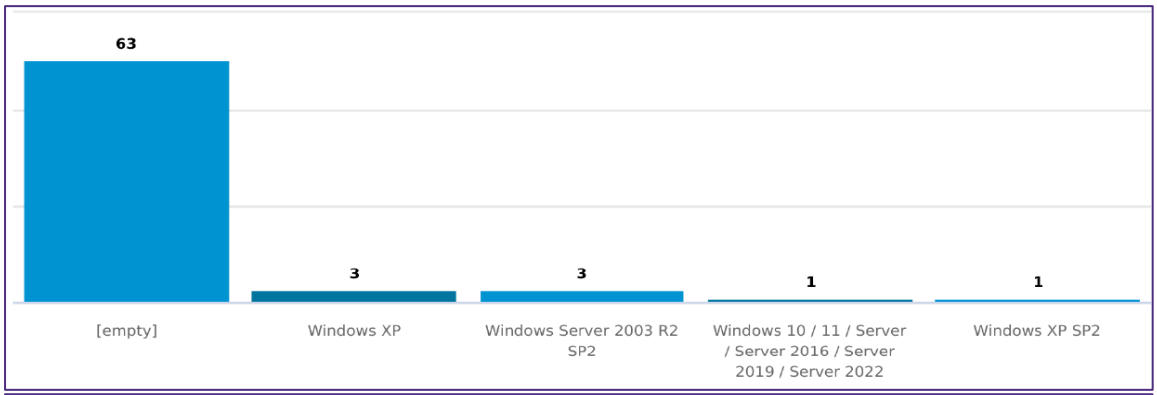
-	76	computer	12	router	23

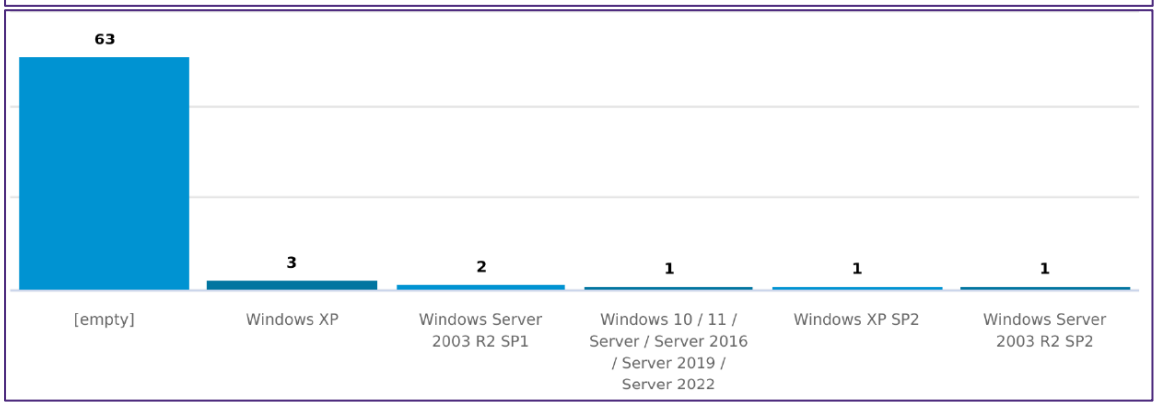
Operating systems

C&I – Unit -2 DCS 1



C&I – Unit -2 DCS 2





Risk

Vulnerability Score

DCS 1

GT Risk Assessment Report provides a comprehensive risk analysis related to network behaviour and assets. Based on overall assessment for **NTPC TANDA**, all network risk score is 6.8 (Medium risk)

NAME	TYPE	OS/FIRMWARE	COUNT	SCORE DISTRIBUTION	SCORE GROUPS (Low, Medium, High)
ws-c2950c-24	switch	Firmware: 12.1(22)ea6	52		2 40 9
2OPSTN_1	computer	Windows XP	686		29 463 194
2OPSTN_2	computer	Windows XP	686		29 463 194
2OPSTN_3	computer	Windows XP	686		29 463 194
2OPSTN_4	computer	Windows XP	686		29 463 194
2OPSTN_5	computer	Windows XP	686		29 463 194
2ENGG	computer	Windows XP	686		29 463 194
2LVS_1	computer	Windows XP	686		29 463 194
2LVS_2	computer	Windows XP	686		29 463 194
2LVS_3	computer	Windows XP	686		29 463 194
WCCBLRLAP660	WAP	Windows XP SP2/SP3 / 10 / 11 / Server / Server 2016 / Server 2019 / Server 2022	320		1 75 244

Assets with confirmed CPEs	1
Assets with Firmware Discovered	110
Number of Hosts with Vulnerabilities	1
Number of Vulnerabilities	52
Vulnerability Average Score	6.8

DCS 2

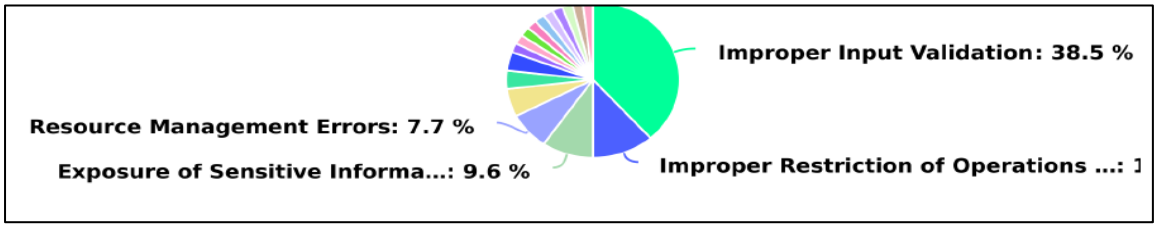
GT Risk Assessment Report provides a comprehensive risk analysis related to network behaviour and assets. Based on overall assessment for **NTPC TANDA**, all network risk score is 6.7(Medium Risk)

NAME	TYPE	OS/FIRMWARE	COUNT	SCORE DISTRIBUTION	SCORE GROUPS (Low, Medium, High)
u4-root-sw.cisco.com	switch	Firmware: 12.2(40)se	47		2 36 8
00:21:9b:87:f3:f8	computer	Windows XP	686		29 463 194
DROP210	computer	Windows XP	686		29 463 194
DROP211	computer	Windows XP	686		29 463 194
WCCBLRLAP660	WAP	Windows XP SP2	1027		21 498 508
DROP160	computer	Windows Server 2003 R2 SP2	341		2 240 99
DROP161	computer	Windows Server 2003 R2 SP2	341		2 240 99
DROP200	computer	Windows Server 2003 R2 SP2	341		2 240 99

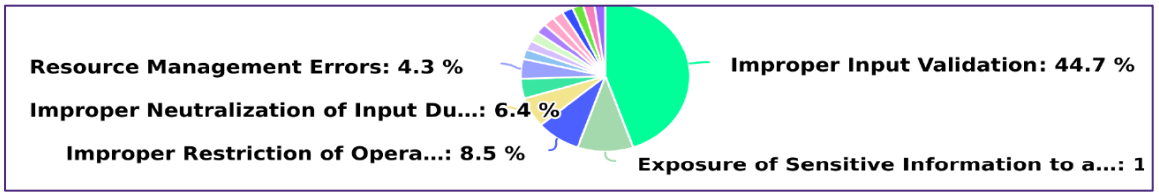
Assets with confirmed CPEs	1
Assets with Firmware Discovered	110
Number of Hosts with Vulnerabilities	1
Number of Vulnerabilities	47
Vulnerability Average Score	6.7

Vulnerabilities per type

DCS 1



DCS 2



Top 30 Vulnerabilities on Network Devices

DCS 1

CVE	LABEL	CVE SCORE	CWE NAME	CVE CREATION TIME	TIME
CVE-2006-4950	00:16:9d:ed:41:d1	10.0	Improper Input Validation	2006-09-23 10:07:00	2022-12-13 15:36:38
CVE-2017-12240	00:16:9d:ed:41:d1	9.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-09-29 01:34:00	2022-12-13 15:36:38
CVE-2007-2586	00:16:9d:ed:41:d1	9.3	Incorrect Authorization	2007-05-10 00:19:00	2022-12-13 15:36:38
CVE-2007-5381	00:16:9d:ed:41:d1	9.3	Improper Restriction of Operations within the Bounds of a Memory Buffer	2007-10-12 01:17:00	2022-12-13 15:36:38
CVE-2007-5552	00:16:9d:ed:41:d1	9.3	Numeric Errors	2007-10-18 20:17:00	2022-12-13 15:36:38
CVE-2017-6743	00:16:9d:ed:41:d1	8.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-07-17 21:29:00	2022-12-13 15:36:38
CVE-2019-16009	00:16:9d:ed:41:d1	8.8	Cross-Site Request Forgery (CSRF)	2020-09-23 01:15:00	2022-12-13 15:36:38
CVE-2017-3864	00:16:9d:ed:41:d1	8.6	Improper Input Validation	2017-03-22 19:59:00	2022-12-13 15:36:38
CVE-2016-6380	00:16:9d:ed:41:d1	8.1	Improper Input Validation	2016-10-05 20:59:00	2022-12-13 15:36:38
CVE-2013-1142	00:16:9d:ed:41:d1	7.8	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	2013-03-28 23:55:00	2022-12-13 15:36:38
CVE-2009-2051	00:16:9d:ed:41:d1	7.8	Improper Input Validation	2009-08-27 17:00:00	2022-12-13 15:36:38
CVE-2011-0946	00:16:9d:ed:41:d1	7.8	Improper Input Validation	2011-10-03 23:55:00	2022-12-13 15:36:38
CVE-2011-3279	00:16:9d:ed:41:d1	7.8	Improper Input Validation	2011-10-03 23:55:00	2022-12-13 15:36:38
CVE-2021-34699	00:16:9d:ed:41:d1	7.7	Interpretation Conflict	2021-09-23 03:15:00	2022-12-13 15:36:38
CVE-2017-3857	00:16:9d:ed:41:d1	7.5	Uncontrolled Resource Consumption	2017-03-22 19:59:00	2022-12-13 15:36:38
CVE-2022-20726	00:16:9d:ed:41:d1	7.5	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2022-04-15 15:15:00	2022-12-13 15:36:38
CVE-2019-12655	00:16:9d:ed:41:d1	7.5	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	2019-09-25 21:15:00	2022-12-13 15:36:38
CVE-1999-0293	00:16:9d:ed:41:d1	7.5	Improper Input Validation	1998-01-01 05:00:00	2022-12-13 15:36:38
CVE-2016-6415	00:16:9d:ed:41:d1	7.5	Exposure of Sensitive Information to an Unauthorized Actor	2016-09-19 01:59:00	2022-12-13 15:36:38
CVE-2016-6393	00:16:9d:ed:41:d1	7.5	Resource Management Errors	2016-10-05 20:59:00	2022-12-13 15:36:38
CVE-2016-6384	00:16:9d:ed:41:d1	7.5	Improper Input Validation	2016-10-05 17:59:00	2022-12-13 15:36:38
CVE-2022-20724	00:16:9d:ed:41:d1	7.5	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	2022-04-15 15:15:00	2022-12-13 15:36:38
CVE-2016-1409	00:16:9d:ed:41:d1	7.5	Improper Input Validation	2016-05-29 22:59:00	2022-12-13 15:36:38
CVE-2003-0647	00:16:9d:ed:41:d1	7.5	Improper Restriction of Operations within the Bounds of a Memory Buffer	2003-08-27 04:00:00	2022-12-13 15:36:38
CVE-2019-1748	00:16:9d:ed:41:d1	7.4	Improper Certificate Validation	2019-03-28 00:29:00	2022-12-13 15:36:38
CVE-2008-1151	00:16:9d:ed:41:d1	7.1	Resource Management Errors	2008-03-27 17:44:00	2022-12-13 15:36:38
CVE-2007-5551	00:16:9d:ed:41:d1	7.1	Improper Restriction of Operations within the Bounds of a Memory Buffer	2007-10-18 20:17:00	2022-12-13 15:36:38
CVE-2008-4963	00:16:9d:ed:41:d1	7.1	Improper Input Validation	2008-11-06 15:55:00	2022-12-13 15:36:38
CVE-2008-4609	00:16:9d:ed:41:d1	7.1	Configuration	2008-10-20 17:59:00	2022-12-13 15:36:38
CVE-2008-1150	00:16:9d:ed:41:d1	7.1	Resource Management Errors	2008-03-27 17:44:00	2022-12-13 15:36:38

C&I – Unit -2 DCS 2

CVE	LABEL	CVE SCORE	CWE NAME	CVE CREATION TIME	TIME
CVE-2006-4950	u4-root-sw.cisco.com	10.0	Improper Input Validation	2006-09-23 10:07:00	2022-12-15 22:20:27
CVE-2017-12240	u4-root-sw.cisco.com	9.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-09-29 01:34:00	2022-12-15 22:20:27
CVE-2007-2586	u4-root-sw.cisco.com	9.3	Incorrect Authorization	2007-05-10 00:19:00	2022-12-15 22:20:27
CVE-2007-5552	u4-root-sw.cisco.com	9.3	Numeric Errors	2007-10-18 20:17:00	2022-12-15 22:20:27
CVE-2017-6743	u4-root-sw.cisco.com	8.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-07-17 21:29:00	2022-12-15 22:20:27
CVE-2019-16009	u4-root-sw.cisco.com	8.8	Cross-Site Request Forgery (CSRF)	2020-09-23 01:15:00	2022-12-15 22:20:27
CVE-2017-3864	u4-root-sw.cisco.com	8.6	Improper Input Validation	2017-03-22 19:59:00	2022-12-15 22:20:27
CVE-2016-6380	u4-root-sw.cisco.com	8.1	Improper Input Validation	2016-10-05 20:59:00	2022-12-15 22:20:27
CVE-2009-2051	u4-root-sw.cisco.com	7.8	Improper Input Validation	2009-08-27 17:00:00	2022-12-15 22:20:27
CVE-2011-0946	u4-root-sw.cisco.com	7.8	Improper Input Validation	2011-10-03 23:55:00	2022-12-15 22:20:27
CVE-2011-3279	u4-root-sw.cisco.com	7.8	Improper Input Validation	2011-10-03 23:55:00	2022-12-15 22:20:27
CVE-2013-1142	u4-root-sw.cisco.com	7.8	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	2013-03-28 23:55:00	2022-12-15 22:20:27
CVE-2021-34699	u4-root-sw.cisco.com	7.7	Interpretation Conflict	2021-09-23 03:15:00	2022-12-15 22:20:27
CVE-1999-0293	u4-root-sw.cisco.com	7.5	Improper Input Validation	1998-01-01 05:00:00	2022-12-15 22:20:27
CVE-2022-20726	u4-root-sw.cisco.com	7.5	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2022-04-15 15:15:00	2022-12-15 22:20:27
CVE-2022-20724	u4-root-sw.cisco.com	7.5	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	2022-04-15 15:15:00	2022-12-15 22:20:27
CVE-2019-12655	u4-root-sw.cisco.com	7.5	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	2019-09-25 21:15:00	2022-12-15 22:20:27
CVE-2017-3857	u4-root-sw.cisco.com	7.5	Uncontrolled Resource Consumption	2017-03-22 19:59:00	2022-12-15 22:20:27
CVE-2016-6415	u4-root-sw.cisco.com	7.5	Exposure of Sensitive Information to an Unauthorized Actor	2016-09-19 01:59:00	2022-12-15 22:20:27
CVE-2016-6393	u4-root-sw.cisco.com	7.5	Resource Management Errors	2016-10-05 20:59:00	2022-12-15 22:20:27
CVE-2016-6385	u4-root-sw.cisco.com	7.5	Resource Management Errors	2016-10-05 20:59:00	2022-12-15 22:20:27
CVE-2016-6384	u4-root-sw.cisco.com	7.5	Improper Input Validation	2016-10-05 17:59:00	2022-12-15 22:20:27
CVE-2016-1409	u4-root-sw.cisco.com	7.5	Improper Input Validation	2016-05-29 22:59:00	2022-12-15 22:20:27
CVE-2008-4609	u4-root-sw.cisco.com	7.1	Configuration	2008-10-20 17:59:00	2022-12-15 22:20:27
CVE-2008-4963	u4-root-sw.cisco.com	7.1	Improper Input Validation	2008-11-06 15:55:00	2022-12-15 22:20:27
CVE-2007-5551	u4-root-sw.cisco.com	7.1	Improper Restriction of Operations within the Bounds of a Memory Buffer	2007-10-18 20:17:00	2022-12-15 22:20:27
CVE-2007-5548	u4-root-sw.cisco.com	6.9	Improper Restriction of Operations within the Bounds of a Memory Buffer	2007-10-18 20:17:00	2022-12-15 22:20:27
CVE-2008-5230	u4-root-sw.cisco.com	6.8	Cryptographic Issues	2008-11-25 23:30:00	2022-12-15 22:20:27
CVE-2013-6686	u4-root-sw.cisco.com	6.8	Improper Input Validation	2013-11-18 03:55:00	2022-12-15 22:20:27
CVE-2020-3204	u4-root-sw.cisco.com	6.7	Improper Input Validation	2020-06-03 18:15:00	2022-12-15 22:20:27

Vulnerability summary

DCS 1

Malware detected	0
Different Operating Systems	5
Different Types of Technologies	6
Attempted Links to Public Internet	0
Multi-homed Assets	0
Different Firmware Versions	2
Clients Accessing SMB Shares	0
Insecure Protocol Links in the Environment	12

DCS 2

Malware detected	0
Different Operating Systems	5
Different Types of Technologies	5
Attempted Links to Public Internet	0
Multi-homed Assets	38
Different Firmware Versions	2
Clients Accessing SMB Shares	6
Insecure Protocol Links in the Environment	136

Clients accessing SMB Shares

FROM	TO	PROTOCOL	TX PACKETS	TX BYTES
192.168.9.149	192.168.8.201	smb		
192.168.9.149	192.168.8.160	smb		
192.168.9.149	192.168.8.211	smb		
192.168.9.149	192.168.8.200	smb		
192.168.9.149	192.168.8.161	smb		
192.168.9.149	192.168.8.210	smb		

Devices Vulnerability Summary

Domain	Critical	High	Medium	Low	Total
Vulnerability Assessment	10	5	12	3	30
Re-validation(closed)	0	0	0	0	0
Re-validation(open)	10	5	12	3	30

Observation Summary

The chart given below represents the vulnerabilities found during network vulnerability testing:

Fig:1

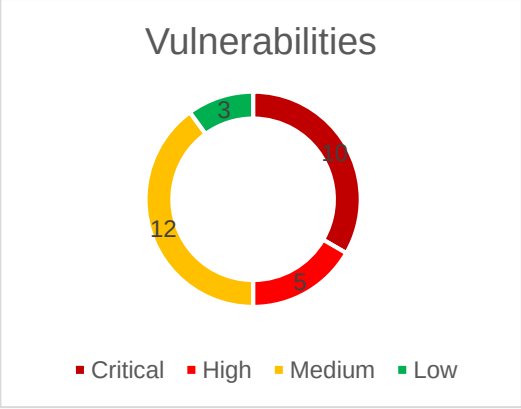


Fig:2

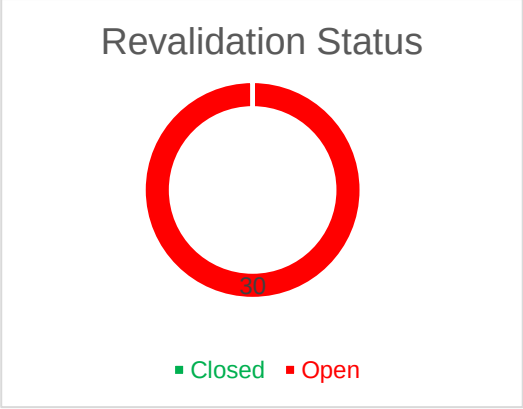


Figure 1: Vulnerability Assessment Test Observations

Illustrates the distribution of observations of Vulnerability testing based on the risk categorization i.e., Critical, High, Medium, and Low.

Figure 2: Vulnerability Assessment Test Observations- Revalidation

Illustrates the closure of Vulnerabilities based on the categorization i.e., Closed, Open.

Note:

Closed: Count considered having vulnerability in all the IP addresses as closed.

Open: Count considered having vulnerability in minimum one IP address as open/unreachable, it may have more different IP addresses which may have the same vulnerability as closed.

Grant Thornton
An instinct for growth™

Vulnerability Assessment Test Observations

The below table illustrates the distribution of observations of Vulnerability testing based on the risk categorization i.e., Critical, High, Medium, and Low.

Vulnerabilities & Impact	Affected IP	Risk	Observations	Recommendations	Status	Revalidation status
Microsoft IIS 6.0 Unsupported Version Detection **Impact:** Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.	192.168.8.160 192.168.8.161	**Critical**	It was observed that an unsupported version of Microsoft IIS is running on the remote Windows host.	It is recommended to upgrade to a version of Microsoft IIS that is currently supported.	**Open**	**Open**
Microsoft Windows Server 2003 Unsupported Installation Detection. **Impact:** Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.	172.16.160.36 172.16.160.38 172.17.160.36 192.168.8.160 192.168.8.161 192.168.8.200	**Critical**	It is observed that the remote operating system is no longer supported.	It is recommended to upgrade to a version of Windows that is currently supported.	**Open**	**Open**
Microsoft Windows XP Unsupported Installation Detection. **Impact:** Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or	172.16.160.24 172.16.160.26 172.16.160.28 172.16.160.30 172.16.160.32 172.16.160.34 172.16.160.40 172.16.160.42 172.16.160.44 172.17.160.24 172.17.160.26 172.17.160.28 172.17.160.30 172.17.160.32 172.17.160.40 172.17.160.42	**Critical**	It is observed that the remote operating system is no longer supported.	It is recommended to upgrade to a version of Windows that is currently supported.	**Open**	**Open**

acknowledge reports of vulnerabilities.	172.17.160.44 192.168.8.201 192.168.8.210 192.168.8.211					
MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check) **Impact:** The remote version of Windows contains a flaw in the Server Message Block (SMB) implementation that may allow an attacker to execute arbitrary code on the remote host. An attacker does not need to be authenticated to exploit this flaw.	172.16.160.24 172.16.160.26 172.16.160.30 172.16.160.40 172.16.160.44 172.17.160.24 172.17.160.26 172.17.160.30 172.17.160.40 172.17.160.44 192.168.8.201	**Critical**	It is observed that an arbitrary code can be executed on the remote host due to a flaw in the SMB implementation.	It is recommended to upgrade to the patches provided by Microsoft for Windows 2000, XP, and 2003. **Reference:** https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2005/ms05-027	**Open**	**Open**
MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check) **Impact:** The remote host is vulnerable to a buffer overrun in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with 'SYSTEM' privileges.	172.16.160.24 172.16.160.26 172.16.160.30 172.16.160.40 172.16.160.44 172.17.160.24 172.17.160.26 172.17.160.30 172.17.160.40 172.17.160.44 192.168.8.201	**Critical**	It is observed that an arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.	It is recommended to upgrade to the patches provided by Microsoft for Windows 2000, XP, and 2003. References: https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2006/ms06-040	**Open**	**Open**
MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING)	172.16.160.24 172.16.160.26 172.16.160.30 172.16.160.34 172.16.160.36 172.16.160.38 172.16.160.40 172.16.160.42	**Critical**	It is observed that the remote Windows host is affected by a remote code execution vulnerability.	It is recommended to upgrade to the patches provided by Microsoft for Windows 2000, XP, and 2003.	**Open**	**Open**

(uncredentialed check) **Impact:** An unauthenticated, remote attacker can exploit this, via a specially crafted RPC request, to execute arbitrary code with 'System' privileges.	172.16.160.44 172.17.160.24 172.17.160.26 172.17.160.30 172.17.160.36 172.17.160.40 172.17.160.42 172.17.160.44 192.168.8.161 192.168.8.200 192.168.8.201					
MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check) **Impact:** The remote host is affected by a memory corruption vulnerability in SMB that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host**.**	172.16.160.24 172.16.160.26 172.16.160.28 172.16.160.30 172.16.160.34 172.16.160.36 172.16.160.38 172.16.160.40 172.16.160.42 172.16.160.44 172.17.160.24 172.17.160.26 172.17.160.28 172.17.160.30 172.17.160.36 172.17.160.40 172.17.160.42 172.17.160.44 192.168.8.160 192.168.8.161 192.168.8.200 192.168.8.201 192.168.8.210 192.168.8.211	**Critical**	It is observed that it is possible to crash the remote host due to a flaw in SMB.	It is recommended to update set of patches for Windows 2000, XP, 2003, Vista and 2008 provided by Microsoft	**Open**	**Open**
SSL Version 2 and 3 Protocol Detection. **Impact:** The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes.	192.168.8.160 192.168.8.200	**Critical**	It is observed that the remote service encrypts traffic using a protocol with known weaknesses.	It is recommended to consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.	**Open**	**Open**

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.						
Unsupported Web Server Detection **Impact:** According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.	192.168.8.160 192.168.8.161	**Critical**	It was observed that the remote web server is obsolete / unsupported.	It is recommended to remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server.	**Open**	**Open**
Unsupported Windows OS (remote) **Impact:** The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.	172.16.160.24 172.16.160.26 172.16.160.28 172.16.160.30 172.16.160.32 172.16.160.34 172.16.160.36 172.16.160.38 172.16.160.40 172.16.160.42 172.16.160.44 172.17.160.24 172.17.160.26 172.17.160.28 172.17.160.30 172.17.160.32 172.17.160.36 172.17.160.40 172.17.160.42 172.17.160.44 192.168.8.160 192.168.8.161 192.168.8.200 192.168.8.201 192.168.8.210 192.168.8.211	**Critical**	It was observed that the remote version of Microsoft Windows is either missing a service pack or is no longer supported	It is recommended to upgrade to a supported service pack or operating system	**Open**	**Open**

MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check) **Impact:** The remote host is vulnerable to heap overflow in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with 'SYSTEM' privileges. In addition to this, the remote host is also affected by an information disclosure vulnerability in SMB that may allow an attacker to obtain portions of the memory of the remote host.	172.16.160.24 172.16.160.26 172.16.160.30 172.16.160.32 172.16.160.40 172.16.160.44 172.17.160.24 172.17.160.26 172.17.160.30 172.17.160.32 172.17.160.40 172.17.160.44 192.168.8.201	**High**	It was observed that an arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.	It is recommended to upgrade to the patches provided by Microsoft for Windows 2000, XP, and 2003.	**Open**	**Open**
MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check) **Impact:** An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)	172.16.160.24 172.16.160.26 172.16.160.28 172.16.160.30 172.16.160.32 172.16.160.34 172.16.160.36 172.16.160.38 172.16.160.40 172.16.160.42 172.16.160.44 172.17.160.24 172.17.160.26 172.17.160.28 172.17.160.30 172.17.160.32 172.17.160.36 172.17.160.40 172.17.160.42 172.17.160.44 192.168.8.160 192.168.8.161 192.168.8.200 192.168.8.201 192.168.8.210 192.168.8.211	**High**	It has been observed that device is not updated to the MS SMB security patch (MS17-010)	It is recommended to follow the below mentioned. Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8. **References:** https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010	**Open**	**Open**

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)						
SMB NULL Session Authentication. **Impact:** The remote host is running and SMB protocol. It is possible to log into the browser or spoolss pipes using a NULL session (i.e., with no login or password). Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.	172.16.160.24 172.16.160.26 172.16.160.28 172.16.160.30 172.16.160.34 172.16.160.36 172.16.160.38 172.16.160.40 172.16.160.42 172.16.160.44 172.17.160.24 172.17.160.26 172.17.160.28 172.17.160.30 172.17.160.36 172.17.160.40 172.17.160.42 172.17.160.44 192.168.8.160 192.168.8.161 192.168.8.200 192.168.8.201 192.168.8.210 192.168.8.211	**High**	It is observed that it is possible to log into the remote host with a NULL session.	It is recommended to contact the product vendor for recommended solutions.	**Open**	**Open**
SSL Certificate Signed Using Weak Hashing Algorithm **Impact:** These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.	192.168.8.160 192.168.8.200	**High**	It was observed that the remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1).	It is recommended to have the SSL certificate reissued.	**Open**	**Open**

SSL Medium Strength Cipher Suites Supported (SWEET32) **Impact:** The remote host supports the use of SSL ciphers that offer medium strength encryption that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.	192.168.8.160 192.168.8.200	**High**	It has been observed that SSL is using medium strength encryption which can be easily compromised if the attacker is on the same physical network.	It is recommended to reconfigure the affected application if possible to avoid use of medium strength ciphers. **References:** [SOLVED] how to disable ssl medium strength cipher suites supported (sweet32) in GPO - Microsoft Remote Desktop Services (spiceworks.com)	**Open**	**Open**
Microsoft Windows EFSRPC NTLM Reflection Elevation of Privilege (PetitPotam) (Remote). **Impact:** An unauthenticated, remote attacker can exploit this, by sending a specially-crafted EFSRPC request, to cause the affected host to connect to a malicious server. An attacker can then utilize an NTLM relay to impersonate the target host and authenticate against remote services.	172.16.160.36 172.16.160.38 172.17.160.36 192.168.8.160 192.168.8.161 192.168.8.200	**Medium**	It is observed that the remote host is affected by an NTLM reflection elevation of privilege vulnerability.	It is recommended to apply the updates supplied by the vendor. Optionally, refer to Microsoft's KB5005413 for mitigation guidance. RPC filters may also be implemented to block remote access to the interface UUIDs necessary for this exploit.	**Open**	**Open**
Microsoft Windows SMB LsaQueryInformation Policy Function SID Enumeration Without Credentials **Impact:** By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier), without credentials.	192.168.8.200	**Medium**	It is observed that it is possible to obtain the host SID for the remote host, without credentials.	It is recommended to prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value. **References:** https://learn.microsoft.com/en-us/previous-versions/tn-	**Open**	**Open**

The host SID can then be used to get the list of local users.				archive/bb418944(v=technet.10)?redirectedfrom=MSDN		
MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) **Impact:** Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.0. Hence an attacker can perform man-in-the-middle attack against the remote host.	172.16.160.36 172.16.160.38 172.17.160.36 192.168.8.160 192.168.8.161 192.168.8.200	Medium	It has been observed that the remote Windows host is affected by an elevation of privilege vulnerability.	It is recommended to implement the Microsoft released set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10. **References:** http://badlock.org/	Open	Open
SMB Signing not required. **Impact:** An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.	172.16.160.24 172.16.160.26 172.16.160.28 172.16.160.30 172.16.160.32 172.16.160.34 172.16.160.36 172.16.160.38 172.16.160.40 172.16.160.42 172.16.160.44 172.17.160.24 172.17.160.26 172.17.160.28 172.17.160.30 172.17.160.32 172.17.160.36 172.17.160.40 172.17.160.42 172.17.160.44 192.168.8.160 192.168.8.161 192.168.8.201 192.168.8.210 192.168.8.211	Medium	It was observed that signing is not required on the remote SMB server.	It is recommended to enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'.	Open	Open

SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection **Impact:** An unauthenticated, remote attacker may be able to leverage this issue to inject an arbitrary amount of plaintext into the beginning of the application protocol stream, which could facilitate man-in-the-middle attacks if the service assumes that the sessions before and after renegotiation are from the same 'client' and merges them at the application layer.	192.168.8.160 192.168.8.200	Medium	It is observed that the remote service allows insecure renegotiation of TLS / SSL connections.	It is recommended to contact the vendor for specific patch information	Open	Open
SSL Certificate Expiry **Impact:** Websites with expired certificates are prone to attacks by hackers or attackers.	192.168.8.160 192.168.8.200	Medium	It is observed to when using an expired SSL certificate, there is a continuous risk to the encryption and mutual authentication of website.	It is recommended to Purchase or generate a new SSL certificate to replace the existing one. **References:** https://www.tenable.com/plugins/nessus/15901 https://nvd.nist.gov/vuln/detail/CVE-2015-3886	Open	Open
SSL RC4 Cipher Suites Supported (Bar Mitzvah) **Impact:** If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the	192.168.8.160 192.168.8.200	Medium	It has been observed that remote host is using weak cipher suite.	It is recommended to reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support. **References:**	Open	Open

attacker may be able to derive the plaintext.				SSL RC4 Cipher Suites Supported (Bar Mitzvah) (microsoft.com)		
SSL Weak Cipher Suites Supported **Impact:** The attackers can spoof the identity of the victim. Unlike CA-issued certificates, self-signed certificates cannot be revoked. The inability to quickly find and revoke private key associated with a self-signed certificate creates serious risk.	192.168.8.160 192.168.8.200	Medium	It is observed this is considerably easier to exploit if the attacker is on the same physical network.	It is recommended to Reconfigure the affected application, if possible to avoid the use of weak ciphers. **References:** How to Disable Weak SSL Protocols and Ciphers in IIS | Wayne Zimmerman's Blog	Open	Open
SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK) **Impact:** The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time. A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.	192.168.8.160 192.168.8.200	Medium	It is observed that the remote host supports a set of weak ciphers.	It is recommended to reconfigure the service to remove support for EXPORT_RSA cipher suites.	Open	Open
SSLv3 Padding Oracle on Downgraded Legacy Encryption	192.168.8.160 192.168.8.200	Medium	It has been observed that the remote host is vulnerable to	It is recommended to disable SSLv3. Services that must support SSLv3 should enable the	Open	Open

Vulnerability (POODLE) **Impact:** An attacker can perform a man-in-the-middle (MitM) information disclosure known as POODLE. MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.			padding oracle attack.	TLS Fallback SCSV mechanism until SSLv3 can be disabled. **References:** How to fix POODLE vulnerability (SSL v3) in Windows - Windows VPS Hosting Blog - AccuWeb Hosting		
TLS Version 1.0 Protocol Detection **Impact:** An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS). Websites using TLS 1.0 will be considered non-compliant by PCI after 30 June 2018.	192.168.8.160 192.168.8.200	**Medium**	It is observed to TLS 1.2 is more secure, an attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities.	It is recommended to Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0. **References:** https://datatracker.ietf.org/doc/html/rfc8996	**Open**	**Open**
Unencrypted Telnet Server **Impact:** An attacker may eavesdrop on a Telnet session and obtain credentials or other sensitive information. Use of SSH is preferred nowadays as it protects credentials from eavesdropping and can tunnel additional data streams such as the X11 session.	172.16.200.212 172.16.200.213 172.16.200.214 172.16.200.216 172.17.200.212 172.17.200.213 172.17.200.214 172.17.200.215 172.17.200.216	**Medium**	It is observed SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.	It is recommended to Disable the Telnet service and use SSH instead. **References:** How to Disable Telnet and Enable SSH on Cisco IOS Devices (networkstraining.com)	**Open**	**Open**

SSL Certificate Chain Contains RSA Keys Less Than 2048 bits. **Impact:** According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits. Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.	192.168.8.160 192.168.8.200	**Low**	It was observed that at least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits	It is recommended to replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.	**Open**	**Open**
SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) **Impact:** Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.	192.168.8.160 192.168.8.200	**Low**	It was observed that the remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.	It is recommended to reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.	**Open**	**Open**

SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam) **Impact:** The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time. A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.	192.168.8.160 192.168.8.200	Low	It is observed that the remote host supports a set of weak ciphers.	It is recommended to reconfigure the service to remove support for EXPORT_DHE cipher suites.	Open	Open

Asset Inventory detail

Inventory Overview

This section focuses on asset tracking, asset discovery and asset classification. These are the first steps for ensuring operational continuity, reliability and safety. They provide the user with a full context for security events and support routine procedures aimed at improving overall cyber hygiene. Creating an inventory of devices in the network, as well as understanding the relationships and connections between them, is a crucial component in network security.

Asset List DCS-1

Unit2_assets_DCS1.xlsx

Asset List DCS-2

Unit2_assets_1_DCS2.xlsx

Mapping of Vulnerabilities with Assets (DCS1)

Final Mapping of C&I Unit-2 Dept Assets:

Refer below excel file contains mapping of vulnerabilities & open ports with the assets, it provides the details of vulnerabilities observed in each asset.

U2_DCS1_Mapping of vulnerabilities wi

Mapping of Vulnerabilities with Assets (DCS2)

Final Mapping of C&I Unit-2 Dept Assets:

Refer below excel file contains mapping of vulnerabilities & open ports with the assets, it provides the details of vulnerabilities observed in each asset.

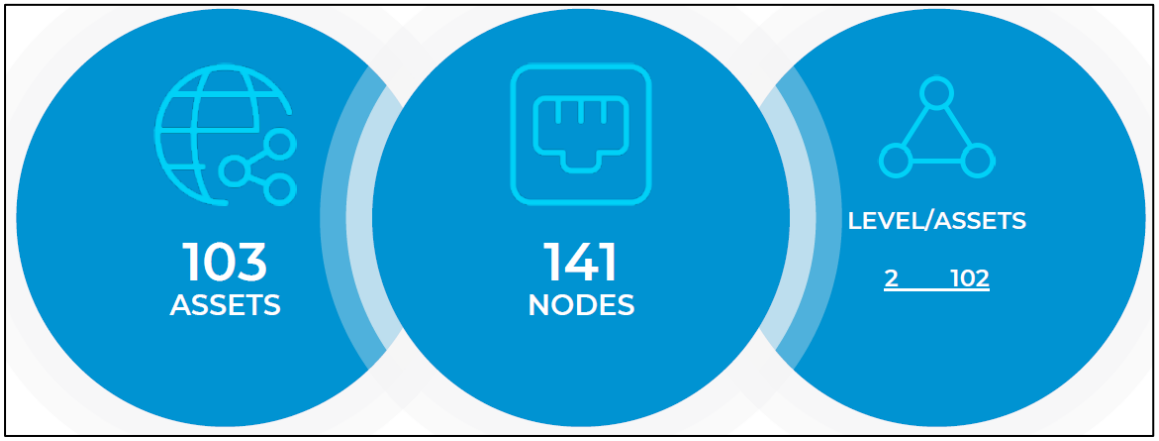
U2_DCS2_Mapping of vulnerabilities wi

Unit 3

Asset Classification

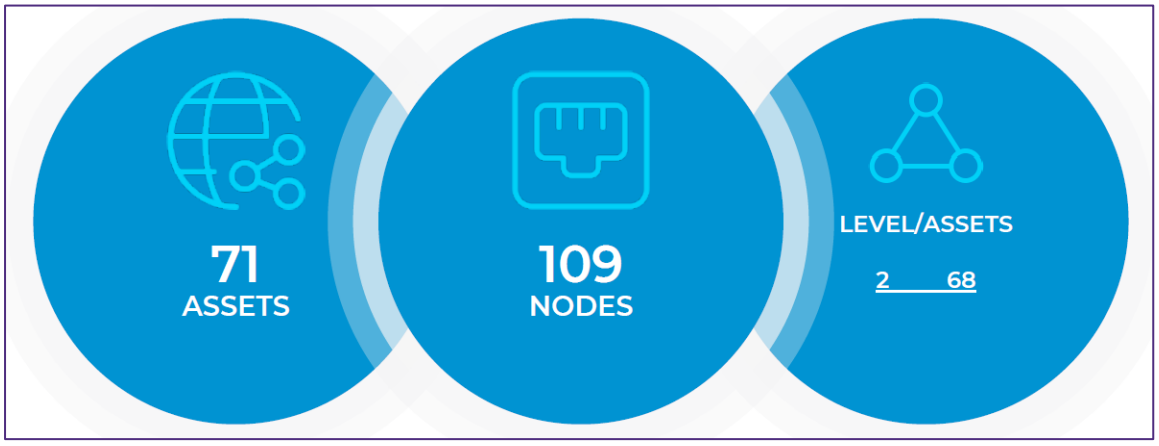
DCS 1(BHEL Make)

The assessment was able to identify 103 all devices and discovered 48 vulnerabilities.
Based on the assessment, risk mitigation and remediation are needed to reduce the risk of nation-level threat vector and improve the cyber posture.



DCS 2 (Emerson Make)

The assessment was able to identify 71 all devices and discovered 48 vulnerabilities.
Based on the assessment, risk mitigation and remediation are needed to reduce the risk of nation-level threat vector and improve the cyber posture.



Vendors

DCS 1

undefined	Broadcom	Cisco	HP
59	5	3	3
LCFC(HeFei) Electr...	PEGATRON	-	TRANSMITTON LTD.
2	1	5	24
VMware, Inc.			
1			

DCS 2

undefined	Cisco	Dell Inc.	LCFC(HeFei) Electr...
40	6	6	2
MICRO INDUSTRIES			
17			

undefined	Broadcom	Cisco	Hirschmann
101	6	3	3
Intel Corporate	LCFC(HeFei) Electr...	TRANSMITTON LTD.	VMware, Inc.
26	2	1	1

Asset Types

DCS 1

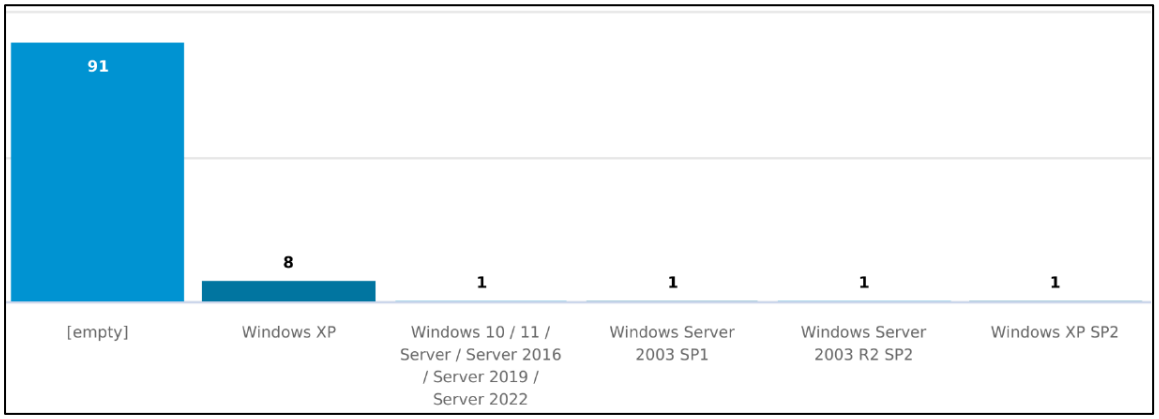
-	90	computer	12	switch	1

DCS 2

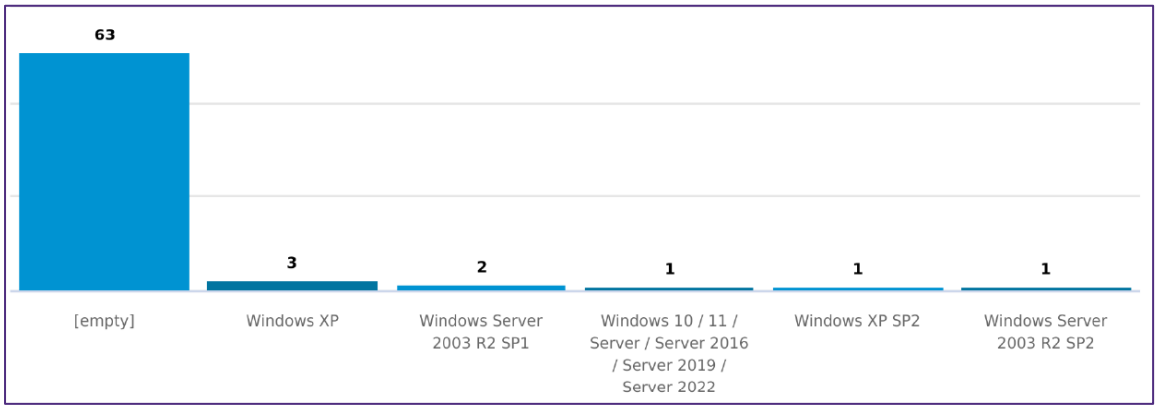
-	60	computer	8	router	2	switch	1

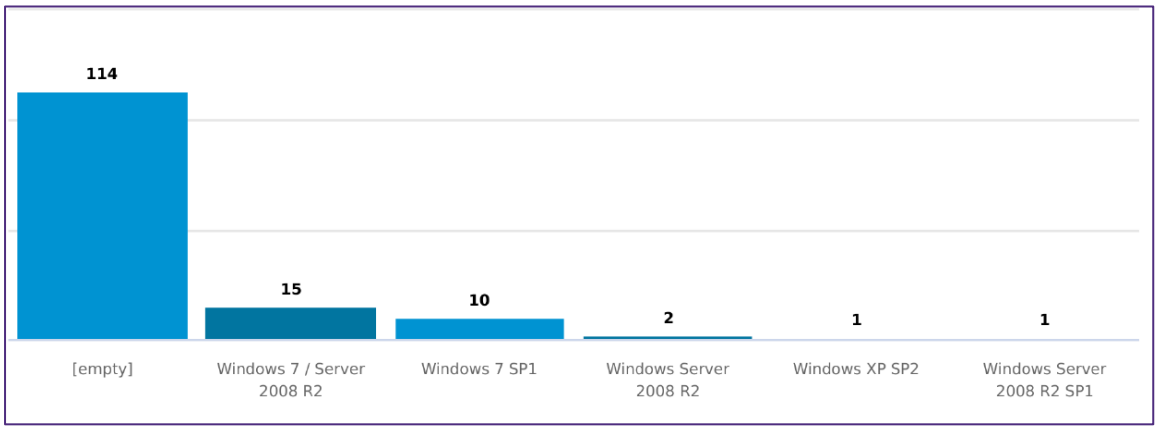
Operating systems

DCS 1



DCS 2





Risk

Vulnerability Score

DCS 1

GT Risk Assessment Report provides a comprehensive risk analysis related to network behaviour and assets. Based on overall assessment for **NTPC TANDA**, all network risk score is 6.7(Medium Risk)

NAME	TYPE	OS/FIRMWARE	COUNT	SCORE DISTRIBUTION	SCORE GROUPS (Low, Medium, High)
ws-c2950c-24	switch	Firmware: 12.1(22)ea9	48		2 37 8
OWS1	computer	Windows XP	686		29 463 194
4OPSTN_2	computer	Windows XP	686		29 463 194
4OPSTN_3	computer	Windows XP	686		29 463 194
4ENGG	computer	Windows XP	686		29 463 194
4LVS_1	computer	Windows XP	686		29 463 194
3EWS	computer	Windows XP	686		29 463 194
OWS2	computer	Windows XP	686		29 463 194
3STORIAN	computer	Windows XP	686		29 463 194
WCCBLRLAP660	computer	Windows XP SP2	1027		21 498 508
4STORIAN_2	computer	Windows Server 2003 R2 SP2	341		2 240 99
4STORIAN_1	computer	Windows Server 2003 SP1	52		1 35 16

Assets with confirmed CPEs	1
Assets with Firmware Discovered	141
Number of Hosts with Vulnerabilities	1
Number of Vulnerabilities	48
Vulnerability Average Score	6.7

DCS 2

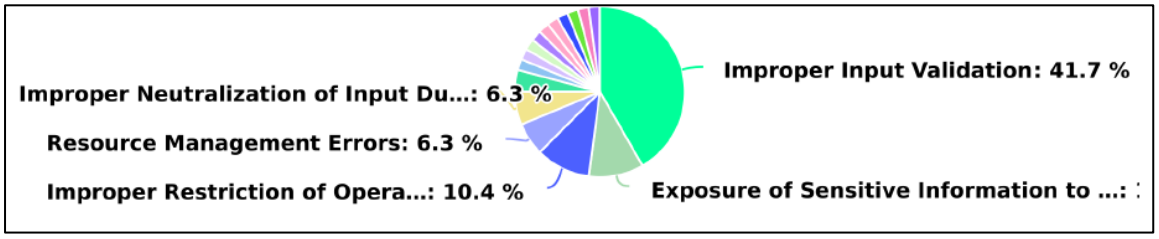
GT Risk Assessment Report provides a comprehensive risk analysis related to network behaviour and assets. Based on overall assessment for **NTPC TANDA**, all network risk score is 6.7(Medium risk)

NAME	TYPE	OS/FIRMWARE	COUNT	SCORE DISTRIBUTION	SCORE GROUPS (Low, Medium, High)
ws-c2950-24	switch	Firmware: 12.1(22)ea5	48		2 37 8
DROP201	computer	Windows XP	686		29 463 194
DROP210	computer	Windows XP	686		29 463 194
DROP211	computer	Windows XP	686		29 463 194
WCCBLRLAP660	computer	Windows XP SP2	1027		21 498 508
DROP160	computer	Windows Server 2003 R2 SP1	43		2 26 15
DROP161	computer	Windows Server 2003 R2 SP1	43		2 26 15
DROP200	computer	Windows Server 2003 R2 SP2	341		2 240 99

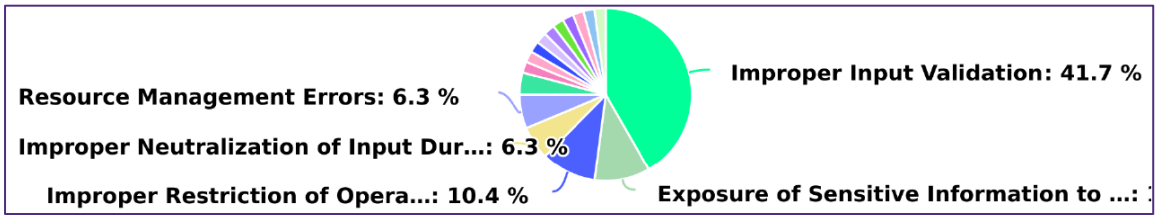
Assets with confirmed CPEs	1
Assets with Firmware Discovered	109
Number of Hosts with Vulnerabilities	1
Number of Vulnerabilities	48
Vulnerability Average Score	6.7

Vulnerabilities per type

C&I – Unit -3 DCS 1



C&I – Unit -3 DCS 2



Grant Thornton
An instinct for growth™

Top 30 Vulnerabilities on Network Devices

C&I – Unit -3 DCS 1

CVE	LABEL	CVE SCORE	CWE NAME	CVE CREATION TIME	TIME
CVE-2006-4950	00:1c:0f:75:c8:4d	10.0	Improper Input Validation	2006-09-23 10:07:00	2022-12-15 10:22:00
CVE-2017-12240	00:1c:0f:75:c8:4d	9.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-09-29 01:34:00	2022-12-15 10:22:00
CVE-2007-2586	00:1c:0f:75:c8:4d	9.3	Incorrect Authorization	2007-05-10 00:19:00	2022-12-15 10:22:00
CVE-2007-5552	00:1c:0f:75:c8:4d	9.3	Numeric Errors	2007-10-18 20:17:00	2022-12-15 10:22:00
CVE-2017-6743	00:1c:0f:75:c8:4d	8.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-07-17 21:29:00	2022-12-15 10:22:00
CVE-2019-16009	00:1c:0f:75:c8:4d	8.8	Cross-Site Request Forgery (CSRF)	2020-09-23 01:15:00	2022-12-15 10:22:00
CVE-2017-3864	00:1c:0f:75:c8:4d	8.6	Improper Input Validation	2017-03-22 19:59:00	2022-12-15 10:22:00
CVE-2016-6380	00:1c:0f:75:c8:4d	8.1	Improper Input Validation	2016-10-05 20:59:00	2022-12-15 10:22:00
CVE-2011-3279	00:1c:0f:75:c8:4d	7.8	Improper Input Validation	2011-10-03 23:55:00	2022-12-15 10:22:00
CVE-2009-2051	00:1c:0f:75:c8:4d	7.8	Improper Input Validation	2009-08-27 17:00:00	2022-12-15 10:22:00
CVE-2011-0946	00:1c:0f:75:c8:4d	7.8	Improper Input Validation	2011-10-03 23:55:00	2022-12-15 10:22:00
CVE-2013-1142	00:1c:0f:75:c8:4d	7.8	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	2013-03-28 23:55:00	2022-12-15 10:22:00
CVE-2021-34699	00:1c:0f:75:c8:4d	7.7	Interpretation Conflict	2021-09-23 03:15:00	2022-12-15 10:22:00
CVE-1999-0293	00:1c:0f:75:c8:4d	7.5	Improper Input Validation	1998-01-01 05:00:00	2022-12-15 10:22:00
CVE-2017-3857	00:1c:0f:75:c8:4d	7.5	Uncontrolled Resource Consumption	2017-03-22 19:59:00	2022-12-15 10:22:00
CVE-2016-1409	00:1c:0f:75:c8:4d	7.5	Improper Input Validation	2016-05-29 22:59:00	2022-12-15 10:22:00
CVE-2022-20724	00:1c:0f:75:c8:4d	7.5	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	2022-04-15 15:15:00	2022-12-15 10:22:00
CVE-2016-6415	00:1c:0f:75:c8:4d	7.5	Exposure of Sensitive Information to an Unauthorized Actor	2016-09-19 01:59:00	2022-12-15 10:22:00
CVE-2016-6393	00:1c:0f:75:c8:4d	7.5	Resource Management Errors	2016-10-05 20:59:00	2022-12-15 10:22:00
CVE-2016-6384	00:1c:0f:75:c8:4d	7.5	Improper Input Validation	2016-10-05 17:59:00	2022-12-15 10:22:00
CVE-2019-12655	00:1c:0f:75:c8:4d	7.5	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	2019-09-25 21:15:00	2022-12-15 10:22:00
CVE-2003-0647	00:1c:0f:75:c8:4d	7.5	Improper Restriction of Operations within the Bounds of a Memory Buffer	2003-08-27 04:00:00	2022-12-15 10:22:00
CVE-2022-20726	00:1c:0f:75:c8:4d	7.5	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2022-04-15 15:15:00	2022-12-15 10:22:00
CVE-2008-4609	00:1c:0f:75:c8:4d	7.1	Configuration	2008-10-20 17:59:00	2022-12-15 10:22:00
CVE-2008-4963	00:1c:0f:75:c8:4d	7.1	Improper Input Validation	2008-11-06 15:55:00	2022-12-15 10:22:00
CVE-2008-1151	00:1c:0f:75:c8:4d	7.1	Resource Management Errors	2008-03-27 17:44:00	2022-12-15 10:22:00
CVE-2008-1150	00:1c:0f:75:c8:4d	7.1	Resource Management Errors	2008-03-27 17:44:00	2022-12-15 10:22:00
CVE-2007-5551	00:1c:0f:75:c8:4d	7.1	Improper Restriction of Operations within the Bounds of a Memory Buffer	2007-10-18 20:17:00	2022-12-15 10:22:00
CVE-2007-5548	00:1c:0f:75:c8:4d	6.9	Improper Restriction of Operations within the Bounds of a Memory Buffer	2007-10-18 20:17:00	2022-12-15 10:22:00
CVE-2008-5230	00:1c:0f:75:c8:4d	6.8	Cryptographic Issues	2008-11-25 23:30:00	2022-12-15 10:22:00

Grant Thornton
An instinct for growth™

C&I – Unit -3 DCS 2

CVE	LABEL	CVE SCORE	CWE NAME	CVE CREATION TIME	TIME
CVE-2006-4950	00:1c:b1:b2:53:94	10.0	Improper Input Validation	2006-09-23 10:07:00	2022-12-15 22:34:31
CVE-2017-12240	00:1c:b1:b2:53:94	9.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-09-29 01:34:00	2022-12-15 22:34:31
CVE-2007-2586	00:1c:b1:b2:53:94	9.3	Incorrect Authorization	2007-05-10 00:19:00	2022-12-15 22:34:31
CVE-2007-5552	00:1c:b1:b2:53:94	9.3	Numeric Errors	2007-10-18 20:17:00	2022-12-15 22:34:31
CVE-2017-6743	00:1c:b1:b2:53:94	8.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-07-17 21:29:00	2022-12-15 22:34:31
CVE-2019-16009	00:1c:b1:b2:53:94	8.8	Cross-Site Request Forgery (CSRF)	2020-09-23 01:15:00	2022-12-15 22:34:31
CVE-2017-3864	00:1c:b1:b2:53:94	8.6	Improper Input Validation	2017-03-22 19:59:00	2022-12-15 22:34:31
CVE-2016-6380	00:1c:b1:b2:53:94	8.1	Improper Input Validation	2016-10-05 20:59:00	2022-12-15 22:34:31
CVE-2011-3279	00:1c:b1:b2:53:94	7.8	Improper Input Validation	2011-10-03 23:55:00	2022-12-15 22:34:31
CVE-2009-2051	00:1c:b1:b2:53:94	7.8	Improper Input Validation	2009-08-27 17:00:00	2022-12-15 22:34:31
CVE-2011-0946	00:1c:b1:b2:53:94	7.8	Improper Input Validation	2011-10-03 23:55:00	2022-12-15 22:34:31
CVE-2013-1142	00:1c:b1:b2:53:94	7.8	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	2013-03-28 23:55:00	2022-12-15 22:34:31
CVE-2021-34699	00:1c:b1:b2:53:94	7.7	Interpretation Conflict	2021-09-23 03:15:00	2022-12-15 22:34:31
CVE-1999-0293	00:1c:b1:b2:53:94	7.5	Improper Input Validation	1998-01-01 05:00:00	2022-12-15 22:34:31
CVE-2017-3857	00:1c:b1:b2:53:94	7.5	Uncontrolled Resource Consumption	2017-03-22 19:59:00	2022-12-15 22:34:31
CVE-2016-1409	00:1c:b1:b2:53:94	7.5	Improper Input Validation	2016-05-29 22:59:00	2022-12-15 22:34:31
CVE-2022-20724	00:1c:b1:b2:53:94	7.5	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	2022-04-15 15:15:00	2022-12-15 22:34:31
CVE-2016-6415	00:1c:b1:b2:53:94	7.5	Exposure of Sensitive Information to an Unauthorized Actor	2016-09-19 01:59:00	2022-12-15 22:34:31
CVE-2016-6393	00:1c:b1:b2:53:94	7.5	Resource Management Errors	2016-10-05 20:59:00	2022-12-15 22:34:31
CVE-2016-6384	00:1c:b1:b2:53:94	7.5	Improper Input Validation	2016-10-05 17:59:00	2022-12-15 22:34:31
CVE-2019-12655	00:1c:b1:b2:53:94	7.5	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	2019-09-25 21:15:00	2022-12-15 22:34:31
CVE-2003-0647	00:1c:b1:b2:53:94	7.5	Improper Restriction of Operations within the Bounds of a Memory Buffer	2003-08-27 04:00:00	2022-12-15 22:34:31
CVE-2022-20726	00:1c:b1:b2:53:94	7.5	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2022-04-15 15:15:00	2022-12-15 22:34:31
CVE-2008-4609	00:1c:b1:b2:53:94	7.1	Configuration	2008-10-20 17:59:00	2022-12-15 22:34:31
CVE-2008-4963	00:1c:b1:b2:53:94	7.1	Improper Input Validation	2008-11-06 15:55:00	2022-12-15 22:34:31
CVE-2008-1151	00:1c:b1:b2:53:94	7.1	Resource Management Errors	2008-03-27 17:44:00	2022-12-15 22:34:31
CVE-2008-1150	00:1c:b1:b2:53:94	7.1	Resource Management Errors	2008-03-27 17:44:00	2022-12-15 22:34:31
CVE-2007-5551	00:1c:b1:b2:53:94	7.1	Improper Restriction of Operations within the Bounds of a Memory Buffer	2007-10-18 20:17:00	2022-12-15 22:34:31
CVE-2007-5548	00:1c:b1:b2:53:94	6.9	Improper Restriction of Operations within the Bounds of a Memory Buffer	2007-10-18 20:17:00	2022-12-15 22:34:31
CVE-2008-5230	00:1c:b1:b2:53:94	6.8	Cryptographic Issues	2008-11-25 23:30:00	2022-12-15 22:34:31

Vulnerability summary

C&I – Unit -3 DCS 1

Malware detected	0
Different Operating Systems	6
Different Types of Technologies	8
Attempted Links to Public Internet	0
Multi-homed Assets	0
Different Firmware Versions	2
Clients Accessing SMB Shares	19
Insecure Protocol Links in the Environment	103

Clients accessing SMB Shares

FROM	TO	PROTOCOL	TX PACKETS	TX BYTES
172.16.160.56	172.16.160.8	smb		
172.16.200.149	172.16.160.86	smb		
172.16.200.149	172.16.160.8	smb		
172.16.200.149	172.16.160.54	smb		
172.16.200.149	172.16.160.84	smb		
172.16.200.149	172.16.160.80	smb		
172.16.200.149	172.16.160.78	smb		
172.16.200.149	172.16.3.37	smb		
172.16.200.149	172.16.160.4	smb		
172.16.200.149	172.16.160.56	smb		
172.16.200.149	172.16.3.35	smb		
172.16.200.149	172.16.160.58	smb		
172.16.200.149	172.16.3.36	smb		
172.16.200.149	172.16.3.34	smb		
172.16.200.149	172.16.160.50	smb		
172.16.200.149	172.16.160.46	smb		
172.16.200.149	172.16.3.32	smb		
172.16.200.149	172.16.160.52	smb		
172.16.200.149	172.16.160.48	smb		

C&I – Unit -3 DCS 2

Malware detected	0
Different Operating Systems	6
Different Types of Technologies	5
Attempted Links to Public Internet	0
Multi-homed Assets	38
Different Firmware Versions	2
Clients Accessing SMB Shares	6
Insecure Protocol Links in the Environment	140

Clients accessing SMB Shares

FROM	TO	PROTOCOL	TX PACKETS	TX BYTES
192.168.3.149	192.168.2.211	smb		
192.168.3.149	192.168.2.210	smb		
192.168.3.149	192.168.2.160	smb		
192.168.3.149	192.168.2.161	smb		
192.168.3.149	192.168.2.201	smb		
192.168.3.149	192.168.2.200	smb		

Devices Vulnerability Summary

Unit 3

Domain	Critical	High	Medium	Low	Total
Vulnerability Assessment	12	7	18	4	41
Re-validation(closed)	0	0	0	0	0
Re-validation(open)	12	7	18	4	41

Observation Summary

The chart given below represents the vulnerabilities found during network vulnerability testing:

Fig:1

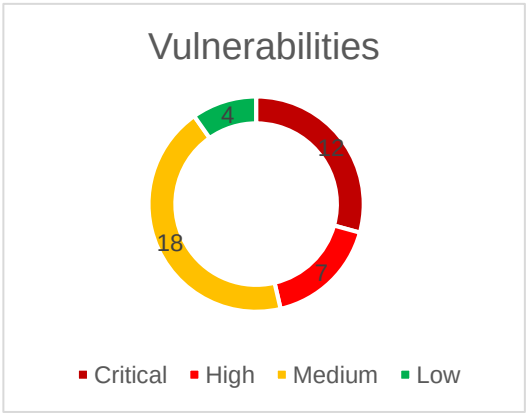


Figure 1: Vulnerability Assessment Test Observations

Illustrates the distribution of observations of Vulnerability testing based on the risk categorization i.e., Critical, High, Medium, and Low.

Fig:2

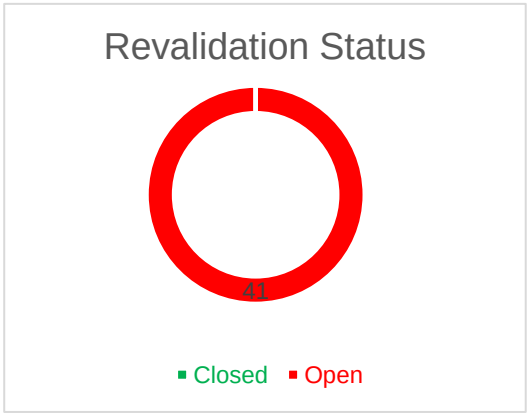


Figure 2: Vulnerability Assessment Test Observations- Revalidation

Illustrates the closure of Vulnerabilities based on the categorization i.e., Closed, Open.

Note:

Closed: Count considered having vulnerability in all the IP addresses as closed.

Open: Count considered having vulnerability in minimum one IP address as open/unreachable, it may have more different IP addresses which may have the same vulnerability as closed.

Vulnerability Assessment Test Observations

The below table illustrates the distribution of observations of Vulnerability testing based on the risk categorization i.e., Critical, High, Medium, and Low.

Vulnerabilities & Impact	Affected IP	Risk	Observations	Recommendations	Status	Revalidation status
Conficker Worm Detection (uncredentialed check) **Impact:** This worm has several capabilities which allow an attacker to execute arbitrary code on the remote operating system. The remote host might also be attempting to propagate the worm to third party hosts**.**	172.17.160.78 172.17.160.8 172.17.160.86	**Critical**	It was observed that the remote host seems to be infected by a variant of the Conficker worm.	It is recommended to update your Antivirus and perform a full scan of the remote operating system.	**Open**	**Open**
Microsoft IIS 6.0 Unsupported Version Detection **Impact:** Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.	192.168.2.160 192.168.2.161	**Critical**	It was observed that an unsupported version of Microsoft IIS is running on the remote Windows host.	It is recommended to upgrade to a version of Microsoft IIS that is currently supported.	**Open**	**Open**
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check) **Impact:** An unauthenticated, remote attacker can exploit this, via a series of specially crafted	192.168.2.160 192.168.2.161 192.168.2.200	**Critical**	It was observed that the remote host is affected by a remote code execution vulnerability.	It is recommended to implement patches for Windows XP, 2003, 2008, 7, and 2008 r2 released by Microsoft.	**Open**	**Open**

requests, to execute arbitrary code.						
Microsoft Windows Server 2003 Unsupported Installation Detection. **Impact:** Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.	192.168.2.160 192.168.2.161 192.168.2.200	**Critical**	It is observed that the remote operating system is no longer supported.	It is recommended to upgrade to a version of Windows that is currently supported.	**Open**	**Open**
Microsoft Windows XP Unsupported Installation Detection. **Impact:** Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.	172.16.160.4 172.17.160.4 172.17.160.78 172.17.160.8 172.17.160.86 192.168.2.201 192.168.2.210 192.168.2.211	**Critical**	It is observed that the remote operating system is no longer supported.	It is recommended to upgrade to a version of Windows that is currently supported.	**Open**	**Open**
MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check) **Impact:** The remote version of Windows contains a flaw in the Server Message Block (SMB) implementation that may allow an attacker to execute arbitrary code on the remote	172.16.160.4 172.17.160.4 192.168.2.201	**Critical**	It is observed that an arbitrary code can be executed on the remote host due to a flaw in the SMB implementation.	It is recommended to upgrade to the patches provided by Microsoft for Windows 2000, XP, and 2003. **Reference:** https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2005/ms05-027	**Open**	**Open**

host. An attacker does not need to be authenticated to exploit this flaw.						
MS05-046: Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution (899589) (uncredentialed check) **Impact:** An attacker may exploit this flaw by connecting to the NetWare RPC service (possibly over IP) and triggering the overflow by sending a malformed RPC request.	192.168.2.201	**Critical**	It is observed that a flaw in the client service for NetWare may allow an attacker to execute arbitrary code on the remote host.	It is recommended to upgrade to the patches provided by Microsoft for Windows 2000, XP, and 2003.	**Open**	**Open**
MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check) **Impact:** An unauthenticated, remote attacker can exploit this, via a specially crafted RPC request, to execute arbitrary code with 'System' privileges.	172.16.160.4 172.17.160.4 192.168.2.160 192.168.2.161 192.168.2.200 192.168.2.201 192.168.2.210 192.168.2.211	**Critical**	It is observed that the remote Windows host is affected by a remote code execution vulnerability.	It is recommended to upgrade to the patches provided by Microsoft for Windows 2000, XP, and 2003.	**Open**	**Open**
MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check) **Impact:**	172.16.160.4 172.17.160.4 172.17.160.78 172.17.160.8 172.17.160.86 192.168.2.160 192.168.2.161 192.168.2.200 192.168.2.201 192.168.2.210	**Critical**	It is observed that it is possible to crash the remote host due to a flaw in SMB.	It is recommended to update set of patches for Windows 2000, XP, 2003, Vista and 2008 provided by Microsoft	**Open**	**Open**

The remote host is affected by a memory corruption vulnerability in SMB that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host**.**	192.168.2.211					
SSL Version 2 and 3 Protocol Detection. **Impact:** The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.	172.17.160.80 172.17.160.84 192.168.2.200	**Critical**	It is observed that the remote service encrypts traffic using a protocol with known weaknesses.	It is recommended to consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.	**Open**	**Open**
Unsupported Web Server Detection **Impact:** According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.	192.168.2.160 192.168.2.161	**Critical**	It was observed that the remote web server is obsolete / unsupported.	It is recommended to remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server.	**Open**	**Open**

Unsupported Windows OS (remote) **Impact:** The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.	172.16.160.4 172.17.160.4 172.17.160.78 172.17.160.8 172.17.160.86 192.168.2.160 192.168.2.161 192.168.2.200 192.168.2.201 192.168.2.210 192.168.2.211	**Critical**	It was observed that the remote version of Microsoft Windows is either missing a service pack or is no longer supported	It is recommended to upgrade to a supported service pack or operating system	**Open**	**Open**
MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check) **Impact:** The remote host is vulnerable to heap overflow in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with 'SYSTEM' privileges. In addition to this, the remote host is also affected by an information disclosure vulnerability in SMB that may allow an attacker to obtain portions of the memory of the remote host.	172.16.160.4 172.17.160.4 192.168.2.201	**High**	It was observed that an arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.	It is recommended to upgrade to the patches provided by Microsoft for Windows 2000, XP, and 2003.	**Open**	**Open**
MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) **Impact:** An arbitrary remote code vulnerability exists in the implementation of the	192.168.2.160 192.168.2.161 192.168.2.200	**High**	It was observed that the remote Windows host could allow arbitrary code execution.	It is recommended to implement patches for Windows XP, 2003, 2008, 7, and 2008 r2 released by Microsoft.	**Open**	**Open**

Remote Desktop Protocol (RDP) on the remote Windows host. The vulnerability is due to the way that RDP accesses an object in memory that has been improperly initialized or has been deleted. If RDP has been enabled on the affected system, an unauthenticated, remote attacker could leverage this vulnerability to cause the system to execute arbitrary code by sending a sequence of specially crafted RDP packets to it.						
MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check) **Impact:** An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148) - An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to	172.16.160.4 172.17.160.4 172.17.160.78 172.17.160.8 172.17.160.86 192.168.2.160 192.168.2.161 192.168.2.200 192.168.2.201 192.168.2.210 192.168.2.211	**High**	It has been observed that device is not updated to the MS SMB security patch (MS17-010)	It is recommended to follow the below mentioned. Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8. REFERENCE: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010	**Open**	**Open**

improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)						
Network Time Protocol Daemon (ntpd) monlist Command Enabled DoS. **Impact:** The version of ntpd running on the remote host is vulnerable to a DoS attack if the 'monlist' command is enabled. The 'monlist' command returns a list of recent hosts that have connected to the service. However, it is affected by a denial-of-service vulnerability in ntp_request.c that allows an unauthenticated, remote attacker to saturate network traffic to a specific IP address by using forged REQ_MON_GETLIST or REQ_MON_GETLIST_1 requests. Furthermore, an attacker can exploit this issue to conduct reconnaissance or distributed denial of service (DDoS) attacks.	172.17.160.84 192.168.2.201	**High**	It was observed that the remote network time server can be affected by a denial-of-service vulnerability.	It is recommended to upgrade to NTP version 4.2.7-p26 or later. Alternatively, add 'disable monitor' to the ntp.conf configuration file and restart the service. Otherwise, limit access to the affected service to trusted hosts, or contact the vendor for a fix.	**Open**	**Open**
SMB NULL Session Authentication. **Impact:** The remote host is running and SMB protocol. It is possible to log into the browser or spoolss pipes using a NULL session (i.e.,	172.16.160.4 172.17.160.4 172.17.160.78 172.17.160.8 172.17.160.86 192.168.2.160 192.168.2.161 192.168.2.200 192.168.2.201 192.168.2.210 192.168.2.211	**High**	It is observed that it is possible to log into the remote host with a NULL session.	It is recommended to contact the product vendor for recommended solutions.	**Open**	**Open**

with no login or password). Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.						
SSL Certificate Signed Using Weak Hashing Algorithm **Impact:** These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.	172.17.160.80 172.17.160.84 192.168.2.200	**High**	It was observed that the remote service uses an SSL certificate chain that has been signed using a cryptographicall y weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1).	It is recommended to have the SSL certificate reissued.	**Open**	**Open**
SSL Medium Strength Cipher Suites Supported (SWEET32) **Impact:** The remote host supports the use of SSL ciphers that offer medium strength encryption that it is considerably easier to circumvent medium strength. encryption if the attacker is on the same physical network.	172.17.160.80 172.17.160.84 192.168.2.200	**High**	It has been observed that SSL is using medium strength encryption which can be easily compromised if the attacker is on the same physical network.	It is recommended to reconfigure the affected application, if possible, to avoid use of medium strength ciphers. **References:** [SOLVED] how to disable ssl medium strength cipher suites supported (sweet32) in GPO - Microsoft Remote Desktop Services (spiceworks.com)	**Open**	**Open**
IP Forwarding Enabled. **Impact:** The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass	192.168.3.5 192.168.3.6	**Medium**	It has been observed that IP forwarding is enabled on remote hosts	It is recommended to follow the given steps below: On Linux, you can disable IP forwarding by doing:	**Open**	**Open**

some firewalls / routers / NAC filtering.				echo 0 > /proc/sys/net/ipv4/ip_forward On Windows, set the key 'IPEnableRouter' to 0 under HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters On Mac OS X, you can disable IP forwarding by executing the command : sysctl -w net.inet.ip.forwarding=0 References: https://linuxconfig.org/how-to-turn-on-off-ip-forwarding-in-linux https://docs.oracle.com/cd/E19957-01/805-2901-12/6j2p9gi08/index.html		
Microsoft Windows EFSRPC NTLM Reflection Elevation of Privilege (PetitPotam) (Remote). **Impact:** An unauthenticated, remote attacker can exploit this, by sending a specially crafted EFSRPC request, to cause the affected host to connect to a malicious server. An attacker can then utilize an NTLM relay to impersonate the target host and authenticate	192.168.2.160 192.168.2.161 192.168.2.200	Medium	It is observed that the remote host is affected by an NTLM reflection elevation of privilege vulnerability.	It is recommended to apply the updates supplied by the vendor. Optionally, refer to Microsoft's KB5005413 for mitigation guidance. RPC filters may also be implemented to block remote access to the interface UUIDs necessary for this exploit.	Open	Open

against remote services.						
Microsoft Windows SMB LsaQueryInformation Policy Function SID Enumeration Without Credentials **Impact:** By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier), without credentials. The host SID can then be used to get the list of local users.	192.168.2.200	**Medium**	It is observed that it is possible to obtain the host SID for the remote host, without credentials.	It is recommended to prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value. **References:** https://learn.microsoft.com/en-us/previous-versions/tn-archive/bb418944(v=technet.10)?redirectedfrom=MSDN	**Open**	**Open**
MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) **Impact:** Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.0. Hence an attacker can perform man-in-the-middle attack against the remote host.	192.168.2.160 192.168.2.161 192.168.2.200	**Medium**	It has been observed that the remote Windows host is affected by an elevation of privilege vulnerability.	It is recommended to implement the Microsoft released set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10. **References:** http://badlock.org/	**Open**	**Open**
Network Time Protocol (NTP) Mode 6 Scanner **Impact:** An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause	172.17.160.84 192.168.2.201 192.168.3.1 192.168.3.2 192.168.3.5 192.168.3.6	**Medium**	It has been observed that a remote NTP server responds to mode 6 queries.	It is recommended to restrict NTP mode 6 queries. References: https://www.ibm.com/support/pages/ibm-aix-disable-ntp-mode-6-and-7-queries	**Open**	**Open**

a reflected denial of service condition.				https://community.cisco.com/t5/other-data-center-subjects/how-to-restrict-ntp-mode-6-queries/td-p/3335720		
NTP ntpd Mode 7 Error Response Packet Loop Remote DoS **Impact:** The version of ntpd running on the remote host has a denial-of-service vulnerability. It responds to mode 7 error packets with its own mode 7 error packets. A remote attacker could exploit this by sending a mode 7 error response with a spoofed IP header, setting the source and destination IP addresses to the IP address of the target. This would cause ntpd to respond to itself endlessly, consuming excessive amounts of CPU, resulting in a denial of service.	172.17.160.84 192.168.2.201	Medium	It is observed that the remote network time service has a denial-of-service vulnerability.	It is recommended to upgrade to NTP 4.2.4p8 / 4.2.6 or later.	Open	Open
Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness **Impact:** The MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.	192.168.2.160 192.168.2.161 192.168.2.200	Medium	It is observed the remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption.	It is recommended to force the use of SSL as a transport layer for this service if supported, or/and. Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available. **References:** http://technet.microsoft.com/en-us/library/cc782610.aspx	Open	Open

				https://www.tenable.com/plugins/nessus/18405		
SMB Signing not required **Impact:** Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.	172.16.160.4 172.17.160.4 172.17.160.78 172.17.160.8 172.17.160.86 192.168.2.160 192.168.2.161 192.168.2.201 192.168.2.210 192.168.2.211	Medium	It has been observed that remote host does not require SMB Signing.	It is recommended to enable signing is on the remote SMB server. **References:** How to resolve SMB Signing not required Vulnerability - GISPP	Open	Open
SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection **Impact:** An unauthenticated, remote attacker may be able to leverage this issue to inject an arbitrary amount of plaintext into the beginning of the application protocol stream, which could facilitate man-in-the-middle attacks if the service assumes that the sessions before and after renegotiation are from the same 'client' and merges them at the application layer.	172.17.160.80 172.17.160.84 192.168.2.200	Medium	It is observed that the remote service allows insecure renegotiation of TLS / SSL connections.	It is recommended to contact the vendor for specific patch information	Open	Open
SSL Certificate Expiry **Impact:** Websites with expired certificates are prone to attacks by hackers or attackers.	172.17.160.80 172.17.160.84 192.168.2.200	Medium	It is observed to when using an expired SSL certificate, there is a continuous risk to the encryption and mutual	It is recommended to Purchase or generate a new SSL certificate to replace the existing one. **References:** https://www.tenable.com/plugins/nessus/15901	Open	Open

			authentication of website.	https://nvd.nist.gov/vuln/detail/CVE-2015-3886		
SSL Certificate with Wrong Hostname **Impact:** The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.	172.17.160.80 172.17.160.84	**Medium**	It has been observed that the SSL certificate for this service is for a different host.	Purchase or generate a proper SSL certificate for this service.	**Open**	**Open**
SSL RC4 Cipher Suites Supported (Bar Mitzvah) **Impact:** If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e. tens of millions) ciphertexts, the attacker may be able to derive the plaintext.	172.17.160.80 172.17.160.84 192.168.2.200	**Medium**	It has been observed that remote host is using weak cipher suite.	It is recommended to reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support. **References:** SSL RC4 Cipher Suites Supported (Bar Mitzvah) (microsoft.com)	**Open**	**Open**
SSL Weak Cipher Suites Supported **Impact:** The attackers can spoof the identity of the victim. Unlike CA-issued certificates, self-signed certificates cannot be revoked. The inability to quickly find and revoke private key associated with a self-signed certificate creates serious risk.	172.17.160.80 172.17.160.84 192.168.2.200	**Medium**	It is observed this is considerably easier to exploit if the attacker is on the same physical network.	It is recommended to Reconfigure the affected application, if possible to avoid the use of weak ciphers. **References:** How to Disable Weak SSL Protocols and Ciphers in IIS | Wayne Zimmerman's Blog	**Open**	**Open**

SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK) **Impact:** The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time. A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.	172.17.160.80 172.17.160.84 192.168.2.200	Medium	It is observed that the remote host supports a set of weak ciphers.	It is recommended to reconfigure the service to remove support for EXPORT_RSA cipher suites.	Open	Open
SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability (POODLE) **Impact:** An attacker can perform a man-in-the-middle (MitM) information disclosure known as POODLE. MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.	172.17.160.80 172.17.160.84 192.168.2.200	Medium	It has been observed that the remote host is vulnerable to padding oracle attack.	It is recommended to disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled. **References:** How to fix POODLE vulnerability (SSL v3) in Windows - Windows VPS Hosting Blog - AccuWeb Hosting	Open	Open
Terminal Services Encryption Level is Medium or Low **Impact:** An attacker can eavesdrop on the communications more	192.168.2.160 192.168.2.161 192.168.2.200	Medium	It has been observed that the remote Terminal Services is t configured to	It is recommended to Change RDP encryption level to High & FIPS Compliant **References:**	Open	Open

easily and obtain screenshots and/or keystrokes.			use Medium cryptography.	https://techgenix.com/Windows_Terminal_Services/#:~:text=Medium%3A%20encrypts%20both%20the%20data%20sent%20from%20client,40%20bit%20key%2C%20depending%20on%20the%20client%20version.		
TLS Version 1.0 Protocol Detection **Impact:** An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS). Websites using TLS 1.0 will be considered non-compliant by PCI after 30 June 2018.	172.17.160.80 172.17.160.84 192.168.2.200	**Medium**	It is observed to TLS 1.2 is more secure, an attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities.	It is recommended to Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0. **References:** https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/insecure-transportation-security-protocol-supported-tls-10/	**Open**	**Open**
Unencrypted Telnet Server **Impact:** Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server. SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional	172.16.200.163 172.17.200.163 192.168.3.1 192.168.3.2 192.168.3.5 192.168.3.6 192.168.3.9	**Medium**	It is observed that the remote Telnet server transmits traffic in cleartext.	It is recommended to disable the Telnet service and use SSH instead.	**Open**	**Open**

data streams such as an X11 session.						
Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak) **Impact:** this information disclosure vulnerability may allow an attacker to collect sensitive information from the affected host provided he is on the same physical subnet as that host.	172.16.3.32 172.16.3.33 172.16.3.34 172.16.3.35 172.16.3.36 172.16.3.37 172.17.3.32 172.17.3.33 172.17.3.34 172.17.3.35 172.17.3.36 172.17.3.37	**Low**	It is observed that the remote host appears to leak memory in network packets.	It is recommended to contact the network device driver's vendor for a fix.	**Open**	**Open**
SSL Certificate Chain Contains RSA Keys Less Than 2048 bits. **Impact:** According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits. Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.	192.168.2.200	**Low**	It was observed that at least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits	It is recommended to replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.	**Open**	**Open**
SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) **Impact:** Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources).	172.17.160.80 172.17.160.84 192.168.2.200	**Low**	It was observed that the remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.	It is recommended to reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.	**Open**	**Open**

This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.						
SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam) **Impact:** The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time. A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.	172.17.160.80 172.17.160.84 192.168.2.200	**Low**	It is observed that the remote host supports a set of weak ciphers.	It is recommended to reconfigure the service to remove support for EXPORT_DHE cipher suites.	**Open**	**Open**

Asset Inventory detail

Inventory Overview

This section focuses on asset tracking, asset discovery and asset classification. These are the first steps for ensuring operational continuity, reliability and safety. They provide the user with a full context for security events and support routine procedures aimed at improving overall cyber hygiene. Creating an inventory of devices in the network, as well as understanding the relationships and connections between them, is a crucial component in network security.

Asset List DCS-1

Unit3_assets_DCS1.xlsx

Asset List DCS-2

Unit3_assets_1_DCS 2.xlsx

Mapping of Vulnerabilities with Assets (DCS1)

Final Mapping of C&I Unit-3 Dept Assets:

Refer below excel file contains mapping of vulnerabilities & open ports with the assets, it provides the details of vulnerabilities observed in each asset.

U3_DCS1_Mapping of vulnerabilities wi

Mapping of Vulnerabilities with Assets (DCS2)

Final Mapping of C&I Unit-3 Dept Assets:

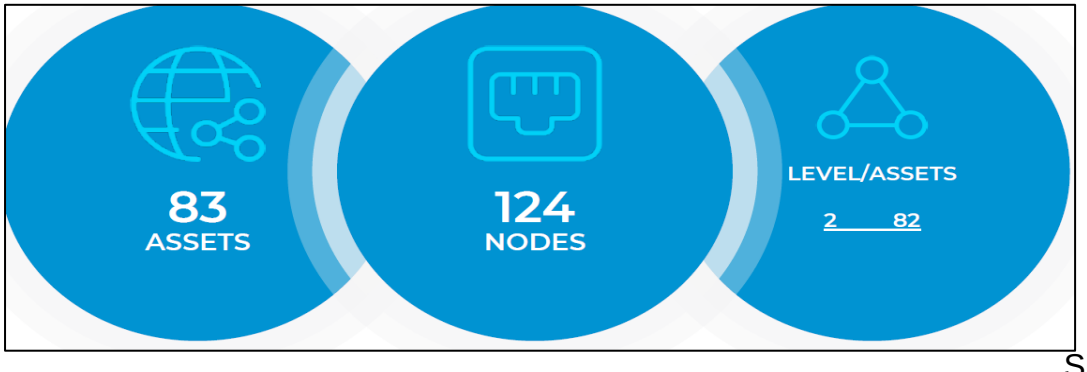
Refer below excel file contains mapping of vulnerabilities & open ports with the assets , it provides the details of vulnerabilities observed in each asset.

U3_DCS2_Mapping of vulnerabilities wi

Unit 4

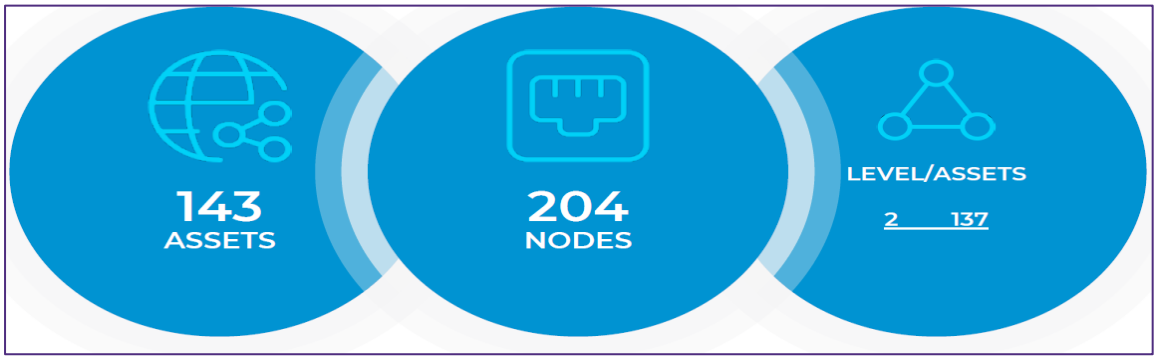
Asset Classification

DCS 1 (BHEL Make)
The assessment was able to identify 83 all devices and discovered 48 vulnerabilities.
Based on the assessment, risk mitigation and remediation are needed to reduce the risk of nation-level threat vector and improve the cyber posture.



C&I – Unit -4 DCS 2 (Emerson Make)

The assessment was able to identify 143 all devices and discovered 96 vulnerabilities.
Based on the assessment, risk mitigation and remediation are needed to reduce the risk of nation-level threat vector and improve the cyber posture.



Vendors

C&I – Unit -4 DCS 1

undefined	Broadcom	Cisco	HP
44	5	3	3
LCFC(HeFei) Electr...	PEGATRON	-	TRANSMITTON LTD.
3	1	5	19

C&I – Unit -4 DCS 2

undefined	Cisco	Dell Inc.	LCFC(HeFei) Electr...
83	16	10	2
MICRO INDUSTRIES			
32			

Asset Types

C&I – Unit -4 DCS 1

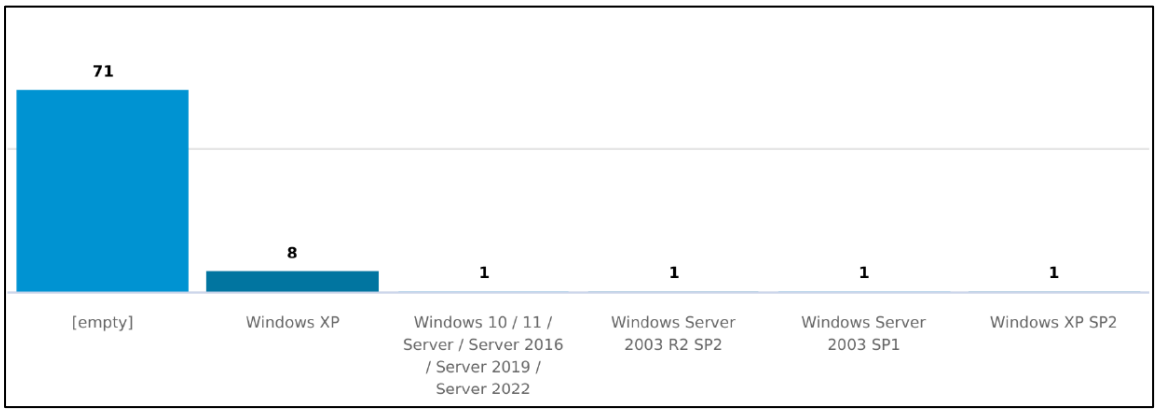
-	70	computer	12	switch	1

C&I – Unit -4 DCS 2

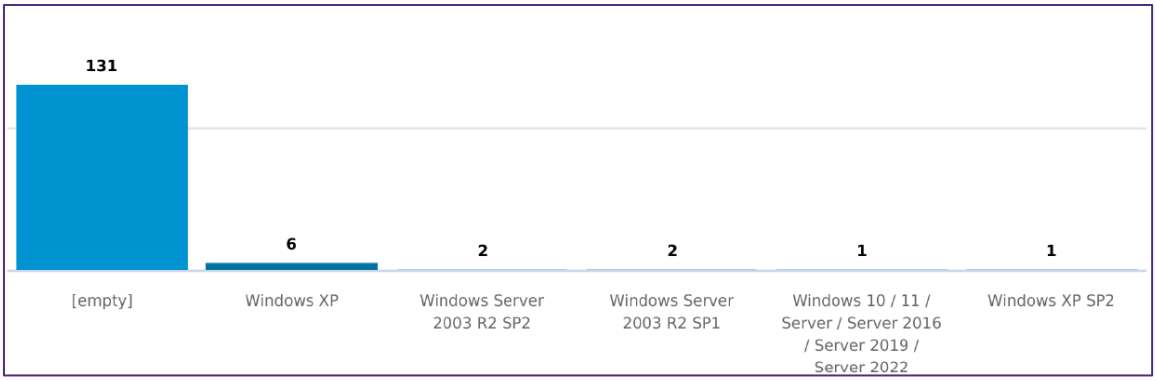
-	125	computer	12	router	4	switch	2

Operating systems

C&I – Unit -4 DCS 1



C&I – Unit -4 DCS 2

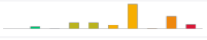


Risk

Vulnerability Score

C&I – Unit -4 DCS 1

GT Risk Assessment Report provides a comprehensive risk analysis related to network behaviour and assets. Based on overall assessment for **NTPC TANDA**, all network risk score is 6.7(Medium risk)

NAME	TYPE	OS/FIRMWARE	COUNT	SCORE DISTRIBUTION	SCORE GROUPS (Low, Medium, High)
ws-c2950c-24	switch	Firmware: 12.1(22)ea8a	48		2 37 8
OWS1	computer	Windows XP	686		29 463 194
4OPSTN_2	computer	Windows XP	686		29 463 194
4OPSTN_3	computer	Windows XP	686		29 463 194
4ENGG	computer	Windows XP	686		29 463 194
4LVS_1	computer	Windows XP	686		29 463 194
3EWS	computer	Windows XP	686		29 463 194
OWS2	computer	Windows XP	686		29 463 194
3STORIAN	computer	Windows XP	686		29 463 194
WCCBLRLAP660	computer	Windows XP SP2	1027		21 498 508
4STORIAN_2	computer	Windows Server 2003 R2 SP2	341		2 240 99
4STORIAN_1	computer	Windows Server 2003 SP1	52		1 35 16

Assets with confirmed CPEs	1
Assets with Firmware Discovered	124
Number of Hosts with Vulnerabilities	1
Number of Vulnerabilities	48
Vulnerability Average Score	6.7

C&I – Unit -4 DCS 2

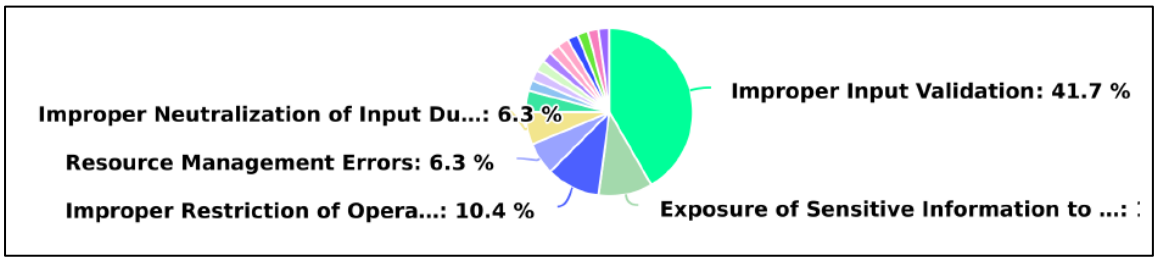
GT Risk Assessment Report provides a comprehensive risk analysis related to network behaviour and assets. Based on overall assessment for **NTPC TANDA**, all network risk score is 6.7(Medium risk)

NAME	TYPE	OS/FIRMWARE	COUNT	SCORE DISTRIBUTION	SCORE GROUPS (Low, Medium, High)
ws-c2950-24	switch	Firmware: 12.1(22)ea5	48		2 37 8
ws-c2950-24	switch	Firmware: 12.1(22)ea5	48		2 37 8
DROP201	computer	Windows XP	686		29 463 194
DROP210	computer	Windows XP	686		29 463 194
DROP211	computer	Windows XP	686		29 463 194
WCCBLRLAP660	computer	Windows XP SP2	2054		42 996 1 016
00:1e:4f:de:51:06	computer	Windows XP	686		29 463 194
DROP210	computer	Windows XP	686		29 463 194
DROP211	computer	Windows XP	686		29 463 194
DROP160	computer	Windows Server 2003 R2 SP1	43		2 26 15
DROP161	computer	Windows Server 2003 R2 SP1	384		4 266 114
DROP200	computer	Windows Server 2003 R2 SP2	682		4 480 198
DROP160	computer	Windows Server 2003 R2 SP2	341		2 240 99

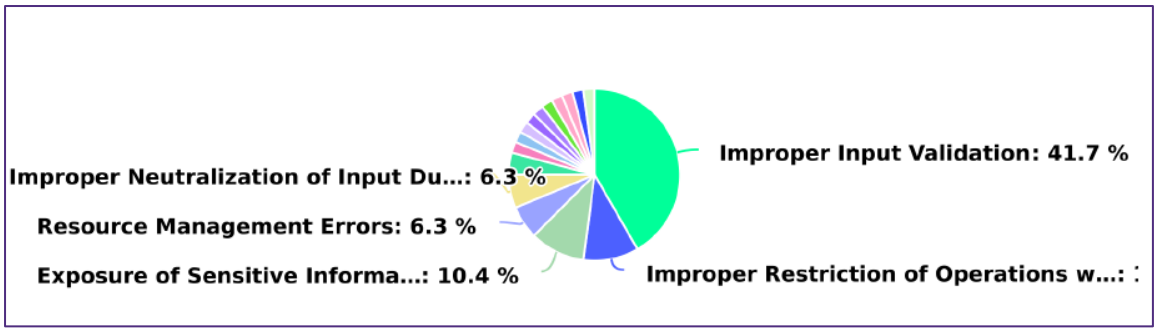
Assets with confirmed CPEs	2
Assets with Firmware Discovered	204
Number of Hosts with Vulnerabilities	2
Number of Vulnerabilities	96
Vulnerability Average Score	6.7

Vulnerabilities per type

C&I – Unit -4 DCS 1



C&I – Unit -4 DCS 2



Top 30 Vulnerabilities on Network Devices

C&I – Unit -4 DCS 1

CVE	LABEL	CVE SCORE	CWE NAME	CVE CREATION TIME	TIME
CVE-2006-4950	00:19:aa:f2:a5:4e	10.0	Improper Input Validation	2006-09-23 10:07:00	2022-12-15 11:42:09
CVE-2017-12240	00:19:aa:f2:a5:4e	9.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-09-29 01:34:00	2022-12-15 11:42:09
CVE-2007-2586	00:19:aa:f2:a5:4e	9.3	Incorrect Authorization	2007-05-10 00:19:00	2022-12-15 11:42:09
CVE-2007-5552	00:19:aa:f2:a5:4e	9.3	Numeric Errors	2007-10-18 20:17:00	2022-12-15 11:42:09
CVE-2017-6743	00:19:aa:f2:a5:4e	8.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-07-17 21:29:00	2022-12-15 11:42:09
CVE-2019-16009	00:19:aa:f2:a5:4e	8.8	Cross-Site Request Forgery (CSRF)	2020-09-23 01:15:00	2022-12-15 11:42:09
CVE-2017-3864	00:19:aa:f2:a5:4e	8.6	Improper Input Validation	2017-03-22 19:59:00	2022-12-15 11:42:09
CVE-2016-6380	00:19:aa:f2:a5:4e	8.1	Improper Input Validation	2016-10-05 20:59:00	2022-12-15 11:42:09
CVE-2011-3279	00:19:aa:f2:a5:4e	7.8	Improper Input Validation	2011-10-05 23:55:00	2022-12-15 11:42:09
CVE-2009-2051	00:19:aa:f2:a5:4e	7.8	Improper Input Validation	2009-08-27 17:00:00	2022-12-15 11:42:09
CVE-2011-0946	00:19:aa:f2:a5:4e	7.8	Improper Input Validation	2011-10-03 23:55:00	2022-12-15 11:42:09
CVE-2013-1142	00:19:aa:f2:a5:4e	7.8	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	2013-03-28 23:55:00	2022-12-15 11:42:09
CVE-2021-34699	00:19:aa:f2:a5:4e	7.7	Interpretation Conflict	2021-09-23 03:15:00	2022-12-15 11:42:09
CVE-1999-0293	00:19:aa:f2:a5:4e	7.5	Improper Input Validation	1998-01-01 05:00:00	2022-12-15 11:42:09
CVE-2017-3857	00:19:aa:f2:a5:4e	7.5	Uncontrolled Resource Consumption	2017-03-22 19:59:00	2022-12-15 11:42:09
CVE-2016-1409	00:19:aa:f2:a5:4e	7.5	Improper Input Validation	2016-05-29 22:59:00	2022-12-15 11:42:09
CVE-2022-20724	00:19:aa:f2:a5:4e	7.5	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	2022-04-15 15:15:00	2022-12-15 11:42:09
CVE-2016-6415	00:19:aa:f2:a5:4e	7.5	Exposure of Sensitive Information to an Unauthorized Actor	2016-09-19 01:59:00	2022-12-15 11:42:09
CVE-2016-6393	00:19:aa:f2:a5:4e	7.5	Resource Management Errors	2016-10-05 20:59:00	2022-12-15 11:42:09
CVE-2016-6384	00:19:aa:f2:a5:4e	7.5	Improper Input Validation	2016-10-05 17:59:00	2022-12-15 11:42:09
CVE-2019-12655	00:19:aa:f2:a5:4e	7.5	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	2019-09-25 21:15:00	2022-12-15 11:42:09
CVE-2003-0647	00:19:aa:f2:a5:4e	7.5	Improper Restriction of Operations within the Bounds of a Memory Buffer	2003-08-27 04:00:00	2022-12-15 11:42:09
CVE-2022-20726	00:19:aa:f2:a5:4e	7.5	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2022-04-15 15:15:00	2022-12-15 11:42:09
CVE-2008-4609	00:19:aa:f2:a5:4e	7.1	Configuration	2008-10-20 17:59:00	2022-12-15 11:42:09
CVE-2008-4963	00:19:aa:f2:a5:4e	7.1	Improper Input Validation	2008-11-06 15:55:00	2022-12-15 11:42:09
CVE-2008-1151	00:19:aa:f2:a5:4e	7.1	Resource Management Errors	2008-03-27 17:44:00	2022-12-15 11:42:09
CVE-2008-1150	00:19:aa:f2:a5:4e	7.1	Resource Management Errors	2008-03-27 17:44:00	2022-12-15 11:42:09
CVE-2007-5551	00:19:aa:f2:a5:4e	7.1	Improper Restriction of Operations within the Bounds of a Memory Buffer	2007-10-18 20:17:00	2022-12-15 11:42:09
CVE-2007-5548	00:19:aa:f2:a5:4e	6.9	Improper Restriction of Operations within the Bounds of a Memory Buffer	2007-10-18 20:17:00	2022-12-15 11:42:09
CVE-2008-5230	00:19:aa:f2:a5:4e	6.8	Cryptographic Issues	2008-11-25 23:30:00	2022-12-15 11:42:09

C&I – Unit -4 DCS 2

CVE	LABEL	CVE SCORE	CWE NAME	CVE CREATION TIME	TIME
CVE-2006-4950	00:1c:b1:b2:53:94	10.0	Improper Input Validation	2006-09-23 10:07:00	2022-12-15 22:34:31
CVE-2006-4950	00:1c:f9:fd:73:08	10.0	Improper Input Validation	2006-09-23 10:07:00	2022-12-15 22:50:46
CVE-2017-12240	00:1c:b1:b2:53:94	9.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-09-29 01:34:00	2022-12-15 22:34:31
CVE-2017-12240	00:1c:f9:fd:73:08	9.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-09-29 01:34:00	2022-12-15 22:50:46
CVE-2007-2586	00:1c:b1:b2:53:94	9.3	Incorrect Authorization	2007-05-10 00:19:00	2022-12-15 22:34:31
CVE-2007-2586	00:1c:f9:fd:73:08	9.3	Incorrect Authorization	2007-05-10 00:19:00	2022-12-15 22:50:46
CVE-2007-5552	00:1c:b1:b2:53:94	9.3	Numeric Errors	2007-10-18 20:17:00	2022-12-15 22:34:31
CVE-2007-5552	00:1c:f9:fd:73:08	9.3	Numeric Errors	2007-10-18 20:17:00	2022-12-15 22:50:46
CVE-2019-16009	00:1c:b1:b2:53:94	8.8	Cross-Site Request Forgery (CSRF)	2020-09-23 01:15:00	2022-12-15 22:34:31
CVE-2017-6743	00:1c:f9:fd:73:08	8.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-07-17 21:29:00	2022-12-15 22:50:46
CVE-2019-16009	00:1c:f9:fd:73:08	8.8	Cross-Site Request Forgery (CSRF)	2020-09-23 01:15:00	2022-12-15 22:50:46
CVE-2017-6743	00:1c:b1:b2:53:94	8.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-07-17 21:29:00	2022-12-15 22:34:31
CVE-2017-3864	00:1c:b1:b2:53:94	8.6	Improper Input Validation	2017-03-22 19:59:00	2022-12-15 22:34:31
CVE-2017-3864	00:1c:f9:fd:73:08	8.6	Improper Input Validation	2017-03-22 19:59:00	2022-12-15 22:50:46
CVE-2016-6380	00:1c:b1:b2:53:94	8.1	Improper Input Validation	2016-10-05 20:59:00	2022-12-15 22:34:31
CVE-2016-6380	00:1c:f9:fd:73:08	8.1	Improper Input Validation	2016-10-05 20:59:00	2022-12-15 22:50:46
CVE-2009-2051	00:1c:b1:b2:53:94	7.8	Improper Input Validation	2009-08-27 17:00:00	2022-12-15 22:34:31
CVE-2011-0946	00:1c:b1:b2:53:94	7.8	Improper Input Validation	2011-10-03 23:55:00	2022-12-15 22:34:31
CVE-2011-3279	00:1c:b1:b2:53:94	7.8	Improper Input Validation	2011-10-03 23:55:00	2022-12-15 22:34:31
CVE-2013-1142	00:1c:b1:b2:53:94	7.8	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	2013-03-28 23:55:00	2022-12-15 22:34:31
CVE-2011-0946	00:1c:f9:fd:73:08	7.8	Improper Input Validation	2011-10-03 23:55:00	2022-12-15 22:50:46
CVE-2011-3279	00:1c:f9:fd:73:08	7.8	Improper Input Validation	2011-10-03 23:55:00	2022-12-15 22:50:46
CVE-2009-2051	00:1c:f9:fd:73:08	7.8	Improper Input Validation	2009-08-27 17:00:00	2022-12-15 22:50:46
CVE-2013-1142	00:1c:f9:fd:73:08	7.8	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	2013-03-28 23:55:00	2022-12-15 22:50:46
CVE-2021-34699	00:1c:b1:b2:53:94	7.7	Interpretation Conflict	2021-09-23 03:15:00	2022-12-15 22:34:31
CVE-2021-34699	00:1c:f9:fd:73:08	7.7	Interpretation Conflict	2021-09-23 03:15:00	2022-12-15 22:50:46
CVE-2017-3857	00:1c:b1:b2:53:94	7.5	Uncontrolled Resource Consumption	2017-03-22 19:59:00	2022-12-15 22:34:31
CVE-2019-12655	00:1c:f9:fd:73:08	7.5	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	2019-09-25 21:15:00	2022-12-15 22:50:46
CVE-2022-20724	00:1c:b1:b2:53:94	7.5	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	2022-04-15 15:15:00	2022-12-15 22:34:31
CVE-1999-0293	00:1c:b1:b2:53:94	7.5	Improper Input Validation	1998-01-01 05:00:00	2022-12-15 22:34:31

Vulnerability summary

C&I – Unit -4 DCS 1

Malware detected	0
Different Operating Systems	6
Different Types of Technologies	8
Attempted Links to Public Internet	0
Multi-homed Assets	0
Different Firmware Versions	2
Clients Accessing SMB Shares	10
Insecure Protocol Links in the Environment	57

Clients accessing SMB Shares

FROM	TO	PROTOCOL	TX PACKETS	TX BYTES
172.16.200.149	172.16.160.80	smb		
172.16.200.149	172.16.160.46	smb		
172.16.200.149	172.16.160.54	smb		
172.16.200.149	172.16.160.78	smb		
172.16.200.149	172.16.160.50	smb		
172.16.200.149	172.16.160.84	smb		
172.16.200.149	172.16.160.56	smb		
172.16.200.149	172.16.160.58	smb		
172.16.200.149	172.16.160.52	smb		
172.16.200.149	172.16.160.48	smb		

C&I – Unit -4 DCS 2

Malware detected	0
Different Operating Systems	6
Different Types of Technologies	5
Attempted Links to Public Internet	0
Multi-homed Assets	82
Different Firmware Versions	2
Clients Accessing SMB Shares	12
Insecure Protocol Links in the Environment	295

Clients accessing SMB Shares

FROM	TO	PROTOCOL	TX PACKETS	TX BYTES
192.168.7.149	192.168.6.211	smb		
192.168.7.149	192.168.6.210	smb		
192.168.7.149	192.168.6.201	smb		
192.168.7.149	192.168.6.160	smb		
192.168.7.149	192.168.6.161	smb		
192.168.7.149	192.168.6.200	smb		
192.168.3.149	192.168.2.211	smb		
192.168.3.149	192.168.2.210	smb		
192.168.3.149	192.168.2.160	smb		
192.168.3.149	192.168.2.161	smb		
192.168.3.149	192.168.2.201	smb		
192.168.3.149	192.168.2.200	smb		

Devices Vulnerability Summary

Domain	Critical	High	Medium	Low	Total
Vulnerability Assessment	13	7	19	4	33
Re-validation(closed)	0	0	0	0	0
Re-validation(open)	13	7	19	4	33

Observation Summary

The chart given below represents the vulnerabilities found during network vulnerability testing:

Fig:1

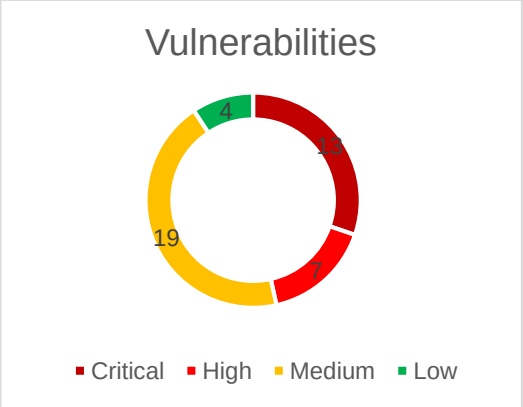


Figure 1: Vulnerability Assessment Test Observations

Illustrates the distribution of observations of Vulnerability testing based on the risk categorization i.e., Critical, High, Medium, and Low.

Fig:2

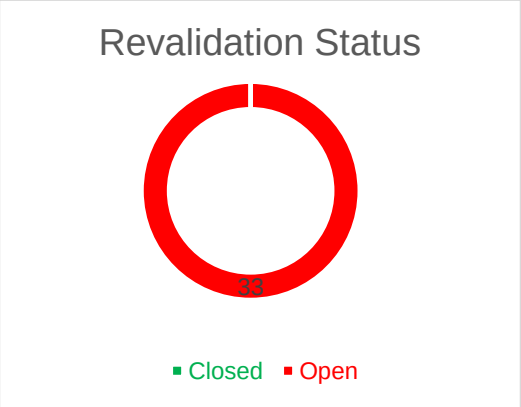


Figure 2: Vulnerability Assessment Test Observations- Revalidation

Illustrates the closure of Vulnerabilities based on the categorization i.e., Closed, Open.

Note:

Closed: Count considered having vulnerability in all the IP addresses as closed.

Open: Count considered having vulnerability in minimum one IP address as open/unreachable, it may have more different IP addresses which may have the same vulnerability as closed.

Grant Thornton
An instinct for growth™

Vulnerability Assessment Test Observations

The below table illustrates the distribution of observations of Vulnerability testing based on the risk categorization i.e., Critical, High, Medium, and Low.

Vulnerabilities & Impact	Affected IP	Risk	Observations	Recommendations	Status	Revalidation status
Conficker Worm Detection (uncredentialed check) **Impact:** This worm has several capabilities which allow an attacker to execute arbitrary code on the remote operating system. The remote host might also be attempting to propagate the worm to third party hosts.	172.16.160.50 172.16.160.54 172.16.160.56 172.16.160.58 172.16.160.78 172.17.160.50 172.17.160.54 172.17.160.56 172.17.160.58	Critical	It was observed that the remote host seems to be infected by a variant of the Conficker worm.	It is recommended to update your Antivirus and perform a full scan of the remote operating system.	Open	Open
HP System Management Homepage Multiple Vulnerabilities (HPSBMU03593) **Impact:** An unauthenticated, remote attacker can exploit this, via a saturation of partial HTTP requests, to cause a daemon outage. (CVE-2007-6750) An unauthenticated, remote attacker can exploit this, via a specially crafted tag, to inject arbitrary script code or HTML into the user's browser session. (CVE-2011-4969) A remote attacker can exploit this to cause the signature verification routine to crash, resulting in a denial of service condition. (CVE-2015-3194)	172.16.160.56 172.17.160.56	Critical	It is observed that the remote web server is affected by multiple vulnerabilities.	It is recommended to upgrade to HP System Management Homepage version 7.5.5 or later.	Open	Open

A remote attacker can exploit this to cause a memory leak by triggering a decoding failure in a PKCS#7 or CMS application, resulting in a denial of service. (CVE-2015-3195) An unauthenticated, remote attacker can exploit this, using a malicious SMB server and crafted length and offset values, to disclose sensitive memory information or to cause a denial-of-service condition. (CVE-2015-3237) A remote attacker can exploit this to corrupt memory, resulting in a denial-of-service condition or the execution of arbitrary code. (CVE-2016-0705)						
Microsoft IIS 6.0 Unsupported Version Detection **Impact:** Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.	192.168.6.160 192.168.6.161	**Critical**	It was observed that an unsupported version of Microsoft IIS is running on the remote Windows host.	It is recommended to upgrade to a version of Microsoft IIS that is currently supported.	**Open**	**Open**
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check) **Impact:** An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.	192.168.6.160 192.168.6.161	**Critical**	It was observed that the remote host is affected by a remote code execution vulnerability.	It is recommended to implement patches for Windows XP, 2003, 2008, 7, and 2008 r2 released by Microsoft.	**Open**	**Open**

Microsoft Windows Server 2003 Unsupported Installation Detection. **Impact:** Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.	172.16.160.54 172.16.160.56 172.17.160.54 172.17.160.56 192.168.6.160 192.168.6.161 192.168.6.200	**Critical**	It is observed that the remote operating system is no longer supported.	It is recommended to upgrade to a version of Windows that is currently supported.	**Open**	**Open**
Microsoft Windows XP Unsupported Installation Detection. **Impact:** Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.	172.16.160.48 172.16.160.50 172.16.160.52 172.16.160.58 172.16.160.78 172.17.160.48 172.17.160.50 172.17.160.52 172.17.160.58 192.168.6.201 192.168.6.210 192.168.6.211	**Critical**	It is observed that the remote operating system is no longer supported.	It is recommended to upgrade to a version of Windows that is currently supported.	**Open**	**Open**
MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check) **Impact:** The remote version of Windows contains a flaw in the Server Message Block (SMB) implementation that may allow an attacker to execute arbitrary code on the remote host. An attacker does not need to be	172.16.160.58 172.17.160.58 192.168.6.201	**Critical**	It is observed that an arbitrary code can be executed on the remote host due to a flaw in the SMB implementation.	It is recommended to upgrade to the patches provided by Microsoft for Windows 2000, XP, and 2003. Reference: https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2005/ms05-027	**Open**	**Open**

authenticated to exploit this flaw.						
MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check) **Impact:** The remote host is vulnerable to a buffer overrun in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with 'SYSTEM' privileges.	172.16.160.54 172.16.160.58 172.17.160.54 172.17.160.58 192.168.6.201	**Critical**	It is observed that an arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.	It is recommended to upgrade to the patches provided by Microsoft for Windows 2000, XP, and 2003. **References:** https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2006/ms06-040	**Open**	**Open**
MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check) **Impact:** An unauthenticated, remote attacker can exploit this, via a specially crafted RPC request, to execute arbitrary code with 'System' privileges.	192.168.6.160 192.168.6.161 192.168.6.201 192.168.6.210 192.168.6.211	**Critical**	It is observed that the remote Windows host is affected by a remote code execution vulnerability.	It is recommended to upgrade to the patches provided by Microsoft for Windows 2000, XP, and 2003.	**Open**	**Open**
MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check) **Impact:** The remote host is affected by a memory	172.16.160.48 172.16.160.50 172.16.160.52 172.16.160.54 172.16.160.56 172.16.160.58 172.16.160.78 172.17.160.48 172.17.160.50 172.17.160.52 172.17.160.54	**Critical**	It is observed that it is possible to crash the remote host due to a flaw in SMB.	It is recommended to update set of patches for Windows 2000, XP, 2003, Vista and 2008 provided by Microsoft	**Open**	**Open**

corruption vulnerability in SMB that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host.	172.17.160.56 172.17.160.58 192.168.6.160 192.168.6.161 192.168.6.200 192.168.6.201 192.168.6.210 192.168.6.211					
SSL Version 2 and 3 Protocol Detection. **Impact:** The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.	172.16.160.56 172.16.160.80 172.16.160.84 172.17.160.56 192.168.6.160 192.168.6.161 192.168.6.200	**Critical**	It is observed that the remote service encrypts traffic using a protocol with known weaknesses.	It is recommended to consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.	**Open**	**Open**
Unsupported Web Server Detection **Impact:** According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.	192.168.6.160 192.168.6.161	**Critical**	It was observed that the remote web server is obsolete / unsupported.	It is recommended to remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server.	**Open**	**Open**

Unsupported Windows OS (remote) **Impact:** The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.	172.16.160.48 172.16.160.50 172.16.160.52 172.16.160.54 172.16.160.56 172.16.160.58 172.16.160.78 172.17.160.48 172.17.160.50 172.17.160.52 172.17.160.54 172.17.160.56 172.17.160.58 192.168.6.160 192.168.6.161 192.168.6.200 192.168.6.201 192.168.6.210 192.168.6.211	**Critical**	It was observed that the remote version of Microsoft Windows is either missing a service pack or is no longer supported	It is recommended to upgrade to a supported service pack or operating system	**Open**	**Open**
MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check) **Impact:** The remote host is vulnerable to heap overflow in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with 'SYSTEM' privileges. In addition to this, the remote host is also affected by an information disclosure vulnerability in SMB that may allow an attacker to obtain portions of the memory of the remote host.	172.16.160.54 172.16.160.58 172.17.160.54 172.17.160.58 192.168.6.201	**High**	It was observed that an arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.	It is recommended to upgrade to the patches provided by Microsoft for Windows 2000, XP, and 2003.	**Open**	**Open**
MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	192.168.6.160 192.168.6.161	**High**	It was observed that the remote Windows host could allow arbitrary code execution.	It is recommended to implement patches for Windows XP, 2003, 2008, 7, and 2008 r2 released by Microsoft.	**Open**	**Open**

Impact: An arbitrary remote code vulnerability exists in the implementation of the Remote Desktop Protocol (RDP) on the remote Windows host. The vulnerability is due to the way that RDP accesses an object in memory that has been improperly initialized or has been deleted. If RDP has been enabled on the affected system, an unauthenticated, remote attacker could leverage this vulnerability to cause the system to execute arbitrary code by sending a sequence of specially crafted RDP packets to it.						
MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check) **Impact:** An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)	172.16.160.48 172.16.160.50 172.16.160.52 172.16.160.54 172.16.160.56 172.16.160.58 172.16.160.78 172.17.160.48 172.17.160.50 172.17.160.52 172.17.160.54 172.17.160.56 172.17.160.58 192.168.6.160 192.168.6.161 192.168.6.200 192.168.6.201 192.168.6.210 192.168.6.211	**High**	It has been observed that device is not updated to the MS SMB security patch (MS17-010)	It is recommended to follow the below mentioned. Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8. REFERENCE: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010	**Open**	**Open**

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)						
Network Time Protocol Daemon (ntpd) monlist Command Enabled DoS. **Impact:** The version of ntpd running on the remote host is vulnerable to a DoS attack if the 'monlist' command is enabled. The 'monlist' command returns a list of recent hosts that have connected to the service. However, it is affected by a denial-of-service vulnerability in ntp_request.c that allows an unauthenticated, remote attacker to saturate network traffic to a specific IP address by using forged REQ_MON_GETLIST or REQ_MON_GETLIST _1 requests. Furthermore, an attacker can exploit this issue to conduct reconnaissance or distributed denial of service (DDoS) attacks.	172.16.160.84	**High**	It was observed that the remote network time server can be affected by a denial-of-service vulnerability.	It is recommended to upgrade to NTP version 4.2.7-p26 or later. Alternatively, add 'disable monitor' to the ntp.conf configuration file and restart the service. Otherwise, limit access to the affected service to trusted hosts, or contact the vendor for a fix.	**Open**	**Open**
SMB NULL Session Authentication. **Impact:** The remote host is running and SMB protocol. It is possible to log into the browser	172.16.160.48 172.16.160.50 172.16.160.52 172.16.160.54 172.16.160.56 172.16.160.58 172.16.160.78	**High**	It is observed that it is possible to log into the remote host with a NULL session.	It is recommended to contact the product vendor for recommended solutions.	**Open**	**Open**

or spoolss pipes using a NULL session (i.e., with no login or password). Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.	172.17.160.48 172.17.160.50 172.17.160.52 172.17.160.54 172.17.160.56 172.17.160.58 192.168.6.160 192.168.6.161 192.168.6.200 192.168.6.201 192.168.6.210 192.168.6.211					
SSL Certificate Signed Using Weak Hashing Algorithm **Impact:** These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.	172.16.160.80 172.16.160.84 192.168.6.160 192.168.6.161 192.168.6.200	**High**	It was observed that the remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1).	It is recommended to have the SSL certificate reissued.	**Open**	**Open**
SSL Medium Strength Cipher Suites Supported (SWEET32) **Impact:** The remote host supports the use of SSL ciphers that offer medium strength encryption that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.	172.16.160.56 172.16.160.80 172.16.160.84 172.17.160.56 192.168.6.160 192.168.6.161 192.168.6.200	**High**	It has been observed that SSL is using medium strength encryption which can be easily compromised if the attacker is on the same physical network.	It is recommended to reconfigure the affected application, if possible, to avoid use of medium strength ciphers. **References:** [SOLVED] how to disable ssl medium strength cipher suites supported (sweet32) in GPO - Microsoft Remote Desktop Services (spiceworks.com)	**Open**	**Open**
IP Forwarding Enabled. **Impact:** The remote host has IP forwarding enabled. An attacker can exploit this to route packets	192.168.7.5 192.168.7.6	**Medium**	It has been observed that IP forwarding is enabled on remote hosts	It is recommended to follow the given steps below: On Linux, you can disable IP forwarding by doing :	**Open**	**Open**

through the host and potentially bypass some firewalls / routers / NAC filtering.				echo 0 > /proc/sys/net/ipv4/ip_forward On Windows, set the key 'IPEnableRouter' to 0 under HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters On Mac OS X, you can disable IP forwarding by executing the command : sysctl -w net.inet.ip.forwarding=0 References: https://linuxconfig.org/how-to-turn-on-off-ip-forwarding-in-linux https://docs.oracle.com/cd/E19957-01/805-2901-12/6j2p9gi08/index.html		
Microsoft Windows EFSRPC NTLM Reflection Elevation of Privilege (PetitPotam) (Remote). **Impact:** An unauthenticated, remote attacker can exploit this, by sending a specially crafted EFSRPC request, to cause the affected host to connect to a malicious server. An attacker can then	172.16.160.54 172.16.160.56 172.17.160.54 172.17.160.56 192.168.6.160 192.168.6.161 192.168.6.200	Medium	It is observed that the remote host is affected by an NTLM reflection elevation of privilege vulnerability.	It is recommended to apply the updates supplied by the vendor. Optionally, refer to Microsoft's KB5005413 for mitigation guidance. RPC filters may also be implemented to block remote access to the interface UUIDs necessary for this exploit.	Open	Open

utilize an NTLM relay to impersonate the target host and authenticate against remote services.						
Microsoft Windows SMB LsaQueryInformation Policy Function SID Enumeration Without Credentials **Impact:** By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier), without credentials. The host SID can then be used to get the list of local users.	192.168.6.200	**Medium**	It is observed that it is possible to obtain the host SID for the remote host, without credentials.	It is recommended to prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value. **References:** https://learn.microsoft.com/en-us/previous-versions/tn-archive/bb418944(v=technet.10)?redirectedfrom=MSDN	**Open**	**Open**
MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) **Impact:** Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.0. Hence an attacker can perform man-in-the-middle attack against the remote host.	172.16.160.54 172.16.160.56 172.17.160.54 172.17.160.56 192.168.6.160 192.168.6.161 192.168.6.200	**Medium**	It has been observed that the remote Windows host is affected by an elevation of privilege vulnerability.	It is recommended to implement the Microsoft released set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10. **References:** http://badlock.org/	**Open**	**Open**
Network Time Protocol (NTP) Mode 6 Scanner **Impact:** An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause	172.16.160.84 192.168.7.1 192.168.7.17 192.168.7.18 192.168.7.19 192.168.7.2 192.168.7.20 192.168.7.5 192.168.7.6	**Medium**	It has been observed that a remote NTP server responds to mode 6 queries.	It is recommended to restrict NTP mode 6 queries. References: https://www.ibm.com/support/pages/ibm-aix-disable-ntp-	**Open**	**Open**

a reflected denial of service condition.				mode-6-and-7-queries https://community.cisco.com/t5/other-data-center-subjects/how-to-restrict-ntp-mode-6-queries/td-p/3335720		
NTP ntpd Mode 7 Error Response Packet Loop Remote DoS **Impact:** The version of ntpd running on the remote host has a denial-of-service vulnerability. It responds to mode 7 error packets with its own mode 7 error packets. A remote attacker could exploit this by sending a mode 7 error response with a spoofed IP header, setting the source and destination IP addresses to the IP address of the target. This would cause ntpd to respond to itself endlessly, consuming excessive amounts of CPU, resulting in a denial of service.	172.16.160.84	**Medium**	It is observed that the remote network time service has a denial-of-service vulnerability.	It is recommended to upgrade to NTP 4.2.4p8 / 4.2.6 or later.	**Open**	**Open**
OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue **Impact:** an attacker that sees (i.e., by sniffing) the start of an SSL connection can	172.16.160.56 172.17.160.56	**Medium**	It is observed that the remote host allows resuming SSL sessions with a weaker cipher than the one originally negotiated.	It is recommended to upgrade to OpenSSL 0.9.8q / 1.0.0.c or later, or contact your vendor for a patch.	**Open**	**Open**

manipulate the OpenSSL session cache to cause subsequent resumptions of that session to use a weaker cipher chosen by the attacker.						
Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness **Impact:** The MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.	192.168.6.160 192.168.6.161	Medium	It is observed the remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption.	It is recommended to force the use of SSL as a transport layer for this service if supported, or/and. Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available. **References:** http://technet.microsoft.com/en-us/library/cc782610.aspx https://www.tenable.com/plugins/nessus/18405	Open	Open
SMB Signing not required. **Impact:** Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.	172.16.160.48 172.16.160.50 172.16.160.52 172.16.160.54 172.16.160.56 172.16.160.58 172.16.160.78 172.17.160.48 172.17.160.50 172.17.160.52 172.17.160.54 172.17.160.56 172.17.160.58 192.168.6.160 192.168.6.161 192.168.6.201 192.168.6.210 192.168.6.211	Medium	It has been observed that remote host does not require SMB Signing.	It is recommended to enable signing is on the remote SMB server. **References:** How to resolve SMB Signing not required Vulnerability - GISPP	Open	Open

SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection **Impact:** An unauthenticated, remote attacker may be able to leverage this issue to inject an arbitrary amount of plaintext into the beginning of the application protocol stream, which could facilitate man-in-the-middle attacks if the service assumes that the sessions before and after renegotiation are from the same 'client' and merges them at the application layer.	172.16.160.56 172.16.160.80 172.16.160.84 172.17.160.56 192.168.6.160 192.168.6.161 192.168.6.200	Medium	It is observed that the remote service allows insecure renegotiation of TLS / SSL connections.	It is recommended to contact the vendor for specific patch information	Open	Open
SSL Certificate with Wrong Hostname **Impact:** The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.	172.16.160.80 172.16.160.84	Medium	It has been observed that the SSL certificate for this service is for a different host.	Purchase or generate a proper SSL certificate for this service.	Open	Open
SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) **Impact:** This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously	172.16.160.56 172.17.160.56	Medium	It has been observed that the remote host may be affected by a vulnerability that allows a remote attacker to potentially decrypt captured TLS traffic.	It is recommended to Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections. **References:** https://drownattack.com/drown-attack-paper.pdf	Open	Open

captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key.						
SSL RC4 Cipher Suites Supported (Bar Mitzvah) **Impact:** If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.	172.16.160.56 172.16.160.80 172.16.160.84 172.17.160.56 192.168.6.160 192.168.6.161 192.168.6.200	**Medium**	It has been observed that remote host is using weak cipher suite such as MD5 and SHA-1.	It is recommended to reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support. **References:** https://www.rc4nomore.com/ http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf	**Open**	**Open**
SSL Weak Cipher Suites Supported. **Impact:** This is considerably easier to exploit if the attacker is on the same physical network.	172.16.160.80 172.16.160.84 192.168.6.160 192.168.6.161 192.168.6.200	**Medium**	It was observed that the remote host supports the use of SSL ciphers that offer weak encryption.	It is recommended to reconfigure the affected application, if possible, to avoid the use of weak ciphers.	**Open**	**Open**
SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK) **Impact:** The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time.	172.16.160.80 172.16.160.84 192.168.6.160 192.168.6.161 192.168.6.200	**Medium**	It is observed that the remote host supports a set of weak ciphers.	It is recommended to reconfigure the service to remove support for EXPORT_RSA cipher suites.	**Open**	**Open**

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g., CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.						
SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability (POODLE) **Impact:** MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.	172.16.160.56 172.16.160.80 172.16.160.84 172.17.160.56 192.168.6.160 192.168.6.161 192.168.6.200	Medium	It was observed that the remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE.	It is recommended to disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.	Open	Open
Terminal Services Encryption Level is Medium or Low **Impact:** An attacker can eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.	192.168.6.160 192.168.6.161	Medium	It has been observed that the remote Terminal Services is t configured to use Medium cryptography.	It is recommended to Change RDP encryption level to High & FIPS Compliant **References:** https://techgenix.com/Windows_Terminal_Services/#:~:text=Medium%3A%20encrypts%20both%20the%20data%20sent%20from%20client,40%20bit%20key%2C%20depending%20on%20the%20client%20version.	Open	Open
TLS Version 1.0 Protocol Detection **Impact:** An attacker can cause connection failures and	172.16.160.56 172.16.160.80 172.16.160.84 172.17.160.56 192.168.6.160 192.168.6.161 192.168.6.200	Medium	It is observed to TLS 1.2 is more secure, an attacker can cause connection failures and they	It is recommended to Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.	Open	Open

they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS). Websites using TLS 1.0 will be considered non-compliant by PCI after 30 June 2018.			can trigger the use of TLS 1.0 to exploit vulnerabilities.	**References:** https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/insecure-transportation-security-protocol-supported-tls-10/		
Unencrypted Telnet Server **Impact:** Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server. SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.	172.16.200.225 172.17.200.225 192.168.7.1 192.168.7.10 192.168.7.17 192.168.7.18 192.168.7.19 192.168.7.2 192.168.7.20 192.168.7.5 192.168.7.9	Medium	It is observed that the remote Telnet server transmits traffic in cleartext.	It is recommended to disable the Telnet service and use SSH instead.	**Open**	**Open**
SSL Certificate Chain Contains RSA Keys Less Than 2048 bits. **Impact:** According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits. Some browser SSL implementations may reject keys less than	192.168.6.160 192.168.6.161 192.168.6.200	Low	It was observed that at least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits	It is recommended to replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.	**Open**	**Open**

2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.						
SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) **Impact:** Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.	172.16.160.80 172.16.160.84 192.168.6.160 192.168.6.161 192.168.6.200	**Low**	It was observed that the remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.	It is recommended to reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.	**Open**	**Open**
SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam) **Impact:** The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time. A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.	172.16.160.80 172.16.160.84 192.168.6.160 192.168.6.161 192.168.6.200	**Low**	It is observed that the remote host supports a set of weak ciphers.	It is recommended to reconfigure the service to remove support for EXPORT_DHE cipher suites.	**Open**	**Open**

Terminal Services Encryption Level is not FIPS-140 Compliant **Impact:** The attacker observed the encryption setting used by the remote Terminal Services after the attacker easy to expose the all sensitive data	192.168.6.160 192.168.6.161	**Low**	It is observed the Client Compatible setting encrypts data sent between the client and the server at the maximum key strength supported by the client.	It is recommended to change RDP encryption level to: 4. FIPS Compliant **References:** https://www.tenable.com/plugins/nessus/30218	**Open**	**Open**

Asset Inventory

Inventory Overview

This section focuses on asset tracking, asset discovery and asset classification. These are the first steps for ensuring operational continuity, reliability and safety. They provide the user with a full context for security events and support routine procedures aimed at improving overall cyber hygiene. Creating an inventory of devices in the network, as well as understanding the relationships and connections between them, is a crucial component in network security.

Asset List DCS-1

Unit4_assets_DCS1.xlsx

Asset List DCS-2

Unit4_assets_1_DCS2.xlsx

Mapping of Vulnerabilities with Assets (DCS1)

Final Mapping of C&I Unit-4 Dept Assets:

Refer the below excel file contains mapping of vulnerabilities & open ports with the assets , it provides the details of vulnerabilities observed in each asset.

U4_DCS1_mapping of vulnerabilities wit

Mapping of Vulnerabilities with Assets (DCS2)

Final Mapping of C&I Unit-4 Dept Assets:

Refer the below excel file contains mapping of vulnerabilities & open ports with the assets , it provides the details of vulnerabilities observed in each asset.

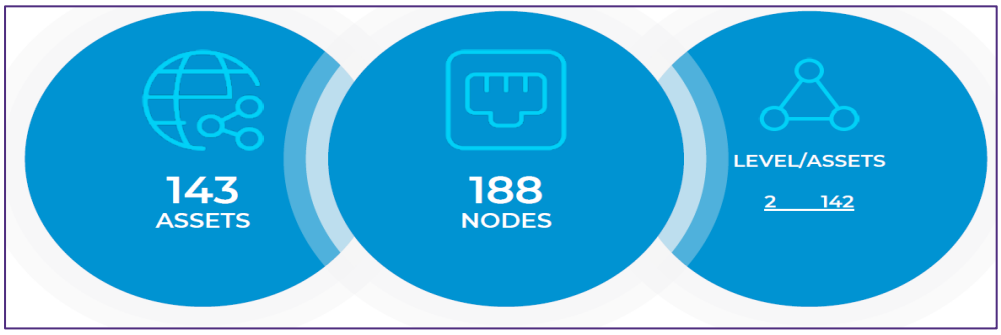
U4_DCS2_Mapping of Vulnerabilities of

Unit -6

Asset classification

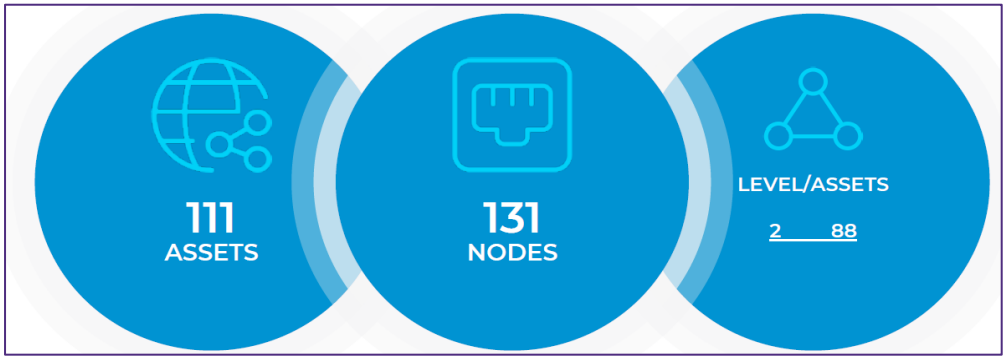
DCS 1 (BHEL Make)

The assessment was able to identify 143 all devices and discovered 86 vulnerabilities.
Based on the assessment, risk mitigation and remediation are needed to reduce the risk of nation-level threat vector and improve the cyber posture.



DCS 2 (Emerson Make)

The assessment was able to identify 111 all devices and discovered 38 vulnerabilities.
Based on the assessment, risk mitigation and remediation are needed to reduce the risk of nation-level threat vector and improve the cyber posture.



Vendors

DCS 1

undefined	Broadcom	Cisco	Hirschmann
101	6	3	3
Intel Corporate	**LCFC(HeFei) Electr...**	**TRANSMITTON LTD.**	**VMware, Inc.**
26	2	1	1

DCS 2

undefined	Dell Inc.	LCFC(HeFei) Electr...	VMware, Inc.
108	1	1	1

Asset Types

DCS 1

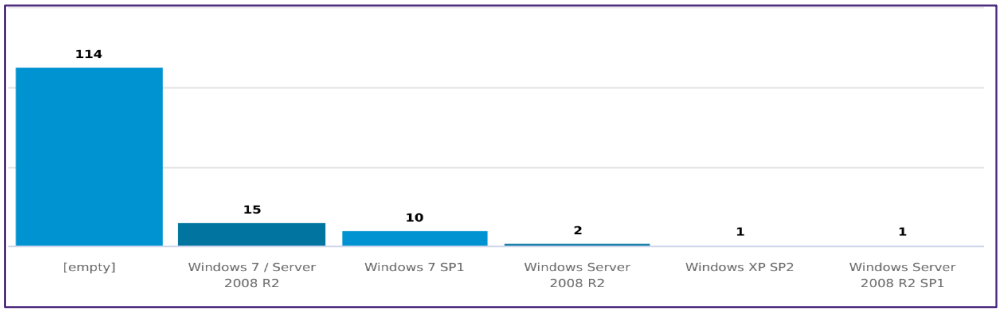
-	113	computer	29	switch	1

DCS 2

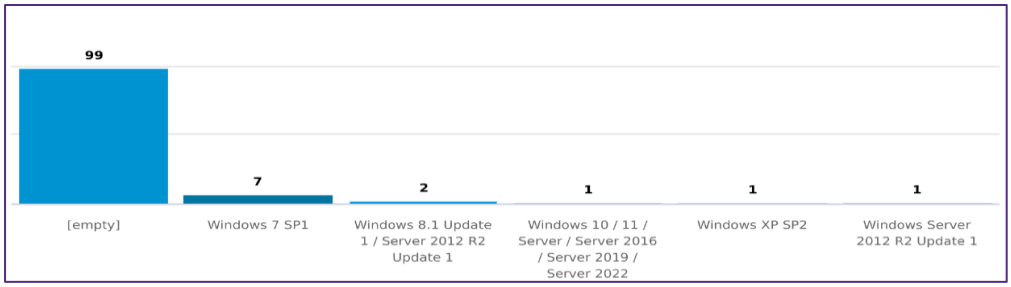
-	76	computer	12	router	23

Operating systems

DCS 1



DCS 2



Risk

Vulnerability Score

DCS 1

GT Risk Assessment Report provides a comprehensive risk analysis related to network behaviour and assets. Based on overall assessment for **NTPC TANDA**, all network risk score is 6.9 (Medium risk)

NAME	TYPE	OS/FIRMWARE	COUNT	SCORE DISTRIBUTION	SCORE GROUPS (Low, Medium, High)
2HMI-1A	-		48		1 39 7
2HMI-2A	-		48		1 39 7
2HMI-UPLINKA	switch	Firmware: 15.0(2)se8	96		2 78 14
WCCBLRLAP660.local	computer	Windows XP SP2	1065		27 528 510
6EWS1	computer	Windows Server 2008 R2 SP1	2193		39 1 667 487
172.16.160.31	computer	Windows Server 2008 R2	2315		40 1 766 509
172.16.160.32	computer	Windows Server 2008 R2	2315		40 1 766 509
6OWS1	computer	Windows 7 SP1	2226		40 1 741 445
172.16.160.34	computer	Windows 7 SP1	2226		40 1 741 445
6OWS3	computer	Windows 7 SP1	2226		40 1 741 445
6OWS4	computer	Windows 7 SP1	2226		40 1 741 445
172.16.160.37	computer	Windows 7 SP1	2226		40 1 741 445
6LVSOWS2	computer	Windows 7 SP1	2226		40 1 741 445
172.16.160.39	computer	Windows 7 SP1	2226		40 1 741 445
6LINKPC1	computer	Windows 7 SP1	2226		40 1 741 445
172.16.160.41	computer	Windows 7 SP1	2226		40 1 741 445
172.16.160.42	computer	Windows 7 SP1	2226		40 1 741 445

Assets with confirmed CPEs	2
Assets with Firmware Discovered	188
Number of Hosts with Vulnerabilities	2
Number of Vulnerabilities	86
Vulnerability Average Score	6.9

DCS 2

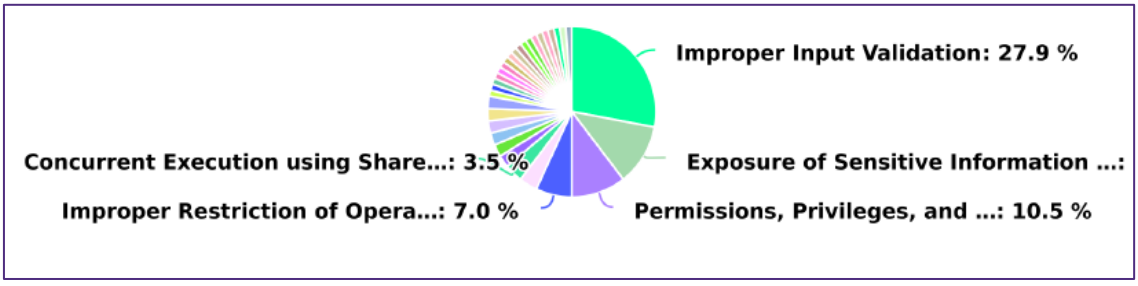
GT Risk Assessment Report provides a comprehensive risk analysis related to network behaviour and assets. Based on overall assessment for **NTPC TANDA**, all network risk score is 0.

NAME	TYPE	OS/FIRMWARE	COUNT	SCORE DISTRIBUTION	SCORE GROUPS (Low, Medium, High)
nessus	computer	Windows XP SP2	1065		27 528 510
DROP210	computer	Windows 7 SP1	2226		40 1 741 445
DROP214	computer	Windows 7 SP1	2226		40 1 741 445
DROP215	computer	Windows 7 SP1	2226		40 1 741 445
DROP216	computer	Windows 7 SP1	2226		40 1 741 445
DROP217	computer	Windows 7 SP1	2226		40 1 741 445
DROP218	computer	Windows 7 SP1	2226		40 1 741 445
DROP219	computer	Windows 7 SP1	2226		40 1 741 445
DROP200	computer	Windows Server 2012 R2 Update 1	2151		46 1 696 409

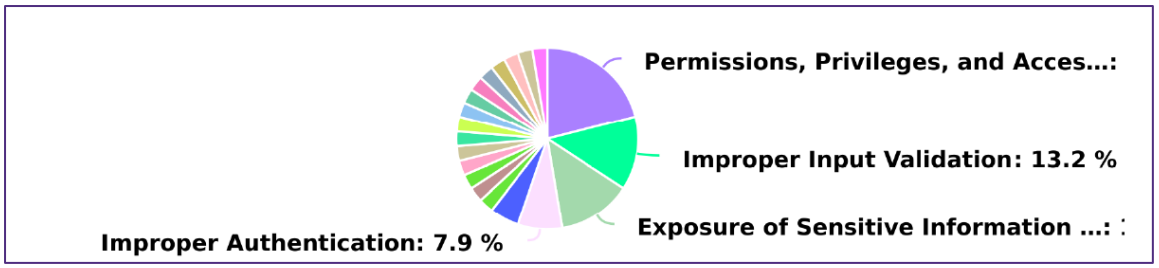
Assets with confirmed CPEs	1
Assets with Firmware Discovered	131
Number of Hosts with Vulnerabilities	1
Number of Vulnerabilities	38
Vulnerability Average Score	0

Vulnerabilities per type

DCS 1



DCS 2



Top 30 Vulnerabilities on Network Devices

DCS 1

CVE	LABEL	CVE SCORE	CWE NAME	CVE CREATION TIME	TIME
CVE-2017-12240	2HMI-UPLINKA	9.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-09-29 01:34:00	2022-12-16 12:05:42
CVE-2007-5552	2HMI-UPLINKA	9.3	Numeric Errors	2007-10-18 20:17:00	2022-12-16 12:05:42
CVE-2017-6743	2HMI-UPLINKA	8.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-07-17 21:29:00	2022-12-16 12:05:42
CVE-2019-16009	2HMI-UPLINKA	8.8	Cross-Site Request Forgery (CSRF)	2020-09-23 01:15:00	2022-12-16 12:05:42
CVE-2020-3225	2HMI-UPLINKA	8.6	Improper Input Validation	2020-06-03 18:15:00	2022-12-16 12:05:42
CVE-2017-3864	2HMI-UPLINKA	8.6	Improper Input Validation	2017-03-22 19:59:00	2022-12-16 12:05:42
CVE-2019-1737	2HMI-UPLINKA	8.6	Allocation of Resources Without Limits or Throttling	2019-03-27 23:29:00	2022-12-16 12:05:42
CVE-2011-3279	2HMI-UPLINKA	7.8	Improper Input Validation	2011-10-03 23:55:00	2022-12-16 12:05:42
CVE-2011-0946	2HMI-UPLINKA	7.8	Improper Input Validation	2011-10-03 23:55:00	2022-12-16 12:05:42
CVE-2013-1142	2HMI-UPLINKA	7.8	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	2013-03-28 23:55:00	2022-12-16 12:05:42
CVE-2015-6278	2HMI-UPLINKA	7.8	Improper Input Validation	2015-09-28 02:59:00	2022-12-16 12:05:42
CVE-2009-2051	2HMI-UPLINKA	7.8	Improper Input Validation	2009-08-27 17:00:00	2022-12-16 12:05:42
CVE-2020-3200	2HMI-UPLINKA	7.7	Interpretation Conflict	2020-06-03 18:15:00	2022-12-16 12:05:42
CVE-2021-34699	2HMI-UPLINKA	7.7	Interpretation Conflict	2021-09-23 03:15:00	2022-12-16 12:05:42
CVE-1999-0293	2HMI-UPLINKA	7.5	Improper Input Validation	1998-01-01 05:00:00	2022-12-16 12:05:42
CVE-2022-20726	2HMI-UPLINKA	7.5	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2022-04-15 15:15:00	2022-12-16 12:05:42
CVE-2022-20724	2HMI-UPLINKA	7.5	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	2022-04-15 15:15:00	2022-12-16 12:05:42
CVE-2020-3230	2HMI-UPLINKA	7.5	Improper Input Validation	2020-06-03 18:15:00	2022-12-16 12:05:42
CVE-2019-12655	2HMI-UPLINKA	7.5	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	2019-09-25 21:15:00	2022-12-16 12:05:42
CVE-2017-3857	2HMI-UPLINKA	7.5	Uncontrolled Resource Consumption	2017-03-22 19:59:00	2022-12-16 12:05:42
CVE-2017-12237	2HMI-UPLINKA	7.5	Uncontrolled Resource Consumption	2017-09-29 01:34:00	2022-12-16 12:05:42
CVE-2017-12235	2HMI-UPLINKA	7.5	Improper Input Validation	2017-09-29 01:34:00	2022-12-16 12:05:42
CVE-2016-6415	2HMI-UPLINKA	7.5	Exposure of Sensitive Information to an Unauthorized Actor	2016-09-19 01:59:00	2022-12-16 12:05:42
CVE-2016-6393	2HMI-UPLINKA	7.5	Resource Management Errors	2016-10-05 20:59:00	2022-12-16 12:05:42
CVE-2016-6384	2HMI-UPLINKA	7.5	Improper Input Validation	2016-10-05 17:59:00	2022-12-16 12:05:42
CVE-2016-1409	2HMI-UPLINKA	7.5	Improper Input Validation	2016-05-29 22:59:00	2022-12-16 12:05:42
CVE-2007-5551	2HMI-UPLINKA	7.1	Improper Restriction of Operations within the Bounds of a Memory Buffer	2007-10-18 20:17:00	2022-12-16 12:05:42
CVE-2008-4609	2HMI-UPLINKA	7.1	Configuration	2008-10-20 17:59:00	2022-12-16 12:05:42
CVE-2008-4963	2HMI-UPLINKA	7.1	Improper Input Validation	2008-11-06 15:55:00	2022-12-16 12:05:42
CVE-2007-5548	2HMI-UPLINKA	6.9	Improper Restriction of Operations within the Bounds of a Memory Buffer	2007-10-18 20:17:00	2022-12-16 12:05:42

DCS 2

<NONE>

Top 30 Vulnerabilities on Non-Switches
DCS 2

CVE	LABEL	CVE SCORE	CWE NAME	CVE CREATION TIME	TIME
CVE-2016-1908	nessus	9.8	Improper Authentication	2017-04-11 18:59:00	2022-12-16 13:01:39
CVE-2015-5600	nessus	8.5	Permissions, Privileges, and Access Controls	2015-08-03 01:59:00	2022-12-16 13:01:39

CVE	LABEL	CVE SCORE	CWE NAME	CVE CREATION TIME	TIME
CVE-2019-16905	nessus	7.8	Integer Overflow or Wraparound	2019-10-09 20:15:00	2022-12-16 13:01:39
CVE-2020-15778	nessus	7.8	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	2020-07-24 14:15:00	2022-12-16 13:01:39
CVE-2015-8325	nessus	7.8	Permissions, Privileges, and Access Controls	2016-05-01 01:59:00	2022-12-16 13:01:39
CVE-2016-10012	nessus	7.8	Improper Restriction of Operations within the Bounds of a Memory Buffer	2017-01-05 02:59:00	2022-12-16 13:01:39
CVE-2016-10708	nessus	7.5	NULL Pointer Dereference	2018-01-21 22:29:00	2022-12-16 13:01:39
CVE-2014-1692	nessus	7.5	Improper Restriction of Operations within the Bounds of a Memory Buffer	2014-01-29 16:02:05	2022-12-16 13:01:39
CVE-2016-6515	nessus	7.5	Improper Input Validation	2016-08-07 21:59:00	2022-12-16 13:01:39
CVE-2010-4478	nessus	7.5	Improper Authentication	2010-12-06 22:30:00	2022-12-16 13:01:39
CVE-2016-10009	nessus	7.3	Untrusted Search Path	2017-01-05 02:59:00	2022-12-16 13:01:39
CVE-2021-28041	nessus	7.1	Double Free	2021-03-05 21:15:00	2022-12-16 13:01:39
CVE-2016-10010	nessus	7.0	Permissions, Privileges, and Access Controls	2017-01-05 02:59:00	2022-12-16 13:01:39
CVE-2021-41617	nessus	7.0	Permissions, Privileges, and Access Controls	2021-09-26 19:15:00	2022-12-16 13:01:39
CVE-2015-6564	nessus	6.9	Permissions, Privileges, and Access Controls	2015-08-24 01:59:00	2022-12-16 13:01:39
CVE-2019-6109	nessus	6.8	Improper Encoding or Escaping of Output	2019-01-31 18:29:00	2022-12-16 13:01:39
CVE-2019-6110	nessus	6.8	Inappropriate Encoding for Output Context	2019-01-31 18:29:00	2022-12-16 13:01:39
CVE-2016-0777	nessus	6.5	Exposure of Sensitive Information to an Unauthorized Actor	2016-01-14 22:59:00	2022-12-16 13:01:39
CVE-2016-3115	nessus	6.4	Permissions, Privileges, and Access Controls	2016-03-22 10:59:00	2022-12-16 13:01:39
CVE-2019-6111	nessus	5.9	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	2019-01-31 18:29:00	2022-12-16 13:01:39
CVE-2016-6210	nessus	5.9	Exposure of Sensitive Information to an Unauthorized Actor	2017-02-13 17:59:00	2022-12-16 13:01:39
CVE-2020-14145	nessus	5.9	Observable Discrepancy	2020-06-29 18:15:00	2022-12-16 13:01:39
CVE-2014-2653	nessus	5.8	Improper Input Validation	2014-03-27 10:55:00	2022-12-16 13:01:39
CVE-2016-10011	nessus	5.5	Key Management Errors	2017-01-05 02:59:00	2022-12-16 13:01:39
CVE-2017-15906	nessus	5.3	Incorrect Permission Assignment for Critical Resource	2017-10-26 03:29:00	2022-12-16 13:01:39
CVE-2016-20012	nessus	5.3	Improper Input Validation	2021-09-15 20:15:00	2022-12-16 13:01:39
CVE-2018-15473	nessus	5.3	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	2018-08-17 19:29:00	2022-12-16 13:01:39
CVE-2018-15919	nessus	5.3	Exposure of Sensitive Information to an Unauthorized Actor	2018-08-28 08:29:00	2022-12-16 13:01:39
CVE-2018-20685	nessus	5.3	Incorrect Authorization	2019-01-10 21:29:00	2022-12-16 13:01:39
CVE-2010-5107	nessus	5.0	Improper Input Validation	2013-03-07 20:55:00	2022-12-16 13:01:39

Vulnerability summary

DCS 1

Malware detected	0
Different Operating Systems	6
Different Types of Technologies	7
Attempted Links to Public Internet	0
Multi-homed Assets	16
Different Firmware Versions	2
Clients Accessing SMB Shares	13
Insecure Protocol Links in the Environment	80

Clients accessing SMB Shares

FROM	TO	PROTOCOL	TX PACKETS	TX BYTES
172.16.202.99	172.16.160.42	smb		
172.16.202.99	172.16.160.38	smb		
172.16.202.99	172.16.160.37	smb		
172.16.202.99	172.16.160.36	smb		
172.16.202.99	172.16.160.32	smb		
172.16.202.99	172.16.160.33	smb		
172.16.202.99	172.16.160.31	smb		
172.16.202.99	172.16.160.41	smb		
172.16.202.99	172.16.160.40	smb		
172.16.202.99	172.16.160.39	smb		
172.16.202.99	172.16.160.35	smb		
172.16.202.99	172.16.160.34	smb		
172.16.202.99	172.16.160.30	smb		

DCS 2

Malware detected	0
Different Operating Systems	6
Different Types of Technologies	7
Attempted Links to Public Internet	0
Multi-homed Assets	0
Different Firmware Versions	1
Clients Accessing SMB Shares	11
Insecure Protocol Links in the Environment	193

Clients accessing SMB Shares

FROM	TO	PROTOCOL	TX PACKETS	TX BYTES
192.168.4.200	192.168.5.149	smb		
192.168.5.149	192.168.4.218	smb		
192.168.5.149	192.168.4.200	smb		
192.168.5.149	192.168.4.215	smb		
192.168.5.149	192.168.4.214	smb		
192.168.5.149	192.168.4.216	smb		
192.168.5.149	192.168.4.210	smb		
192.168.5.149	192.168.4.160	smb		
192.168.5.149	192.168.4.219	smb		
192.168.5.149	192.168.4.217	smb		
192.168.5.149	192.168.4.161	smb		

Devices Vulnerability Summary

Domain	Critical	High	Medium	Low	Total
Vulnerability Assessment	4	8	18	7	37
Re-validation(closed)	0	0	0	0	0
Re-validation(open)	4	8	18	7	37

Observation Summary

The chart given below represents the vulnerabilities found during network vulnerability testing:

Fig:1

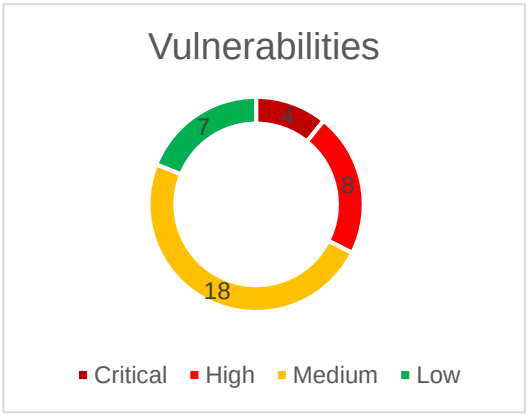


Fig:2

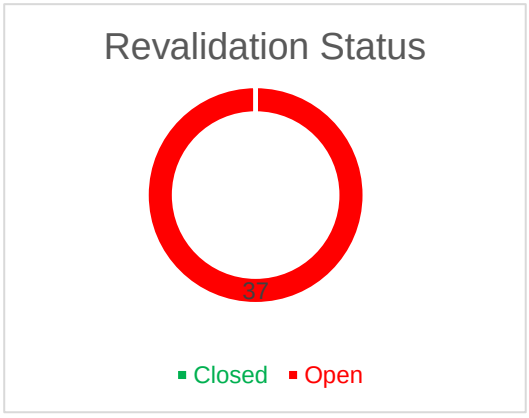


Figure 1: Vulnerability Assessment Test Observations

Illustrates the distribution of observations of Vulnerability testing based on the risk categorization i.e., Critical, High, Medium, and Low.

Figure 2: Vulnerability Assessment Test Observations- Revalidation

Illustrates the closure of Vulnerabilities based on the categorization i.e., Closed, Open.

Note:

Closed: Count considered having vulnerability in all the IP addresses as closed.

Open: Count considered having vulnerability in minimum one IP address as open/unreachable, it may have more different IP addresses which may have the same vulnerability as closed.

Vulnerability Assessment Test Observations

The below table illustrates the distribution of observations of Vulnerability testing based on the risk categorization i.e., Critical, High, Medium, and Low.

Vulnerabilities & Impact	Affected IP	Risk	Observations	Recommendations	Status	Revalidation status
Cisco IOS Cluster Management Protocol Telnet Option Handling RCE (cisco-sa-20170317-cmp) **Impact:** According to its self-reported version and configuration, the Cisco IOS software running on the remote device is affected by a remote code execution vulnerability in the Cluster Management Protocol (CMP) subsystem due to improper handling of CMP-specific Telnet options. An unauthenticated, remote attacker can exploit this by establishing a Telnet session with malformed CMP-specific telnet options, to execute arbitrary code.	172.16.202.50 172.16.202.51 172.16.202.55 172.17.202.50 172.17.202.51 172.17.202.55	**Critical**	It is observed that the remote device is missing a vendor-supplied security patch.	It is recommended to upgrade to the relevant fixed version referenced in Cisco bug ID CSCvd48893. Alternatively, as a workaround, disable the Telnet protocol for incoming connections.	**Open**	**Open**

Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check) **Impact:** An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.	172.16.160.30 172.16.160.33 172.16.160.34 172.16.160.35 172.17.160.30 172.17.160.33 172.17.160.34 172.17.160.35 192.168.4.214 192.168.4.218	**Critical**	It was observed that the remote host is affected by a remote code execution vulnerability.	It is recommended to implement patches for Windows XP, 2003, 2008, 7, and 2008 r2 released by Microsoft.	**Open**	**Open**
SSL Version 2 and 3 Protocol Detection **Impact**: An attacker can conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.	172.16.160.30 172.17.160.30	**Critical**	It has been observed that arbitrary commands can be run on this port.	It is recommended to disable SSL 2.0 and 3.0. Use TLS 1.2 with higher cipher suites listed below. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256k1) - A TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256k1) - A TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256k1) - A TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256k1) – A 2 **References:** How to Disable SSL 2.0 and SSL 3.0 in IIS 7 (sslshopper.com)	**Open**	**Open**
Unsupported Windows OS (remote) **Impact:** A system is unsupported when the developer is no longer issuing any software patches or security updates. From that point on, the operating system is stagnant.	172.16.160.30 172.16.160.31 172.16.160.32 172.16.160.33 172.16.160.34 172.16.160.35 172.16.160.36 172.16.160.37 172.16.160.38 172.16.160.39 172.16.160.40 172.16.160.41 172.16.160.42 172.17.160.30 172.17.160.31 172.17.160.32	**Critical**	It is observed the remote OS or service pack is no longer supported.	It is recommended to upgrade to a supported service pack or operating system. **References:** https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=windows	**Open**	**Open**

	172.17.160.33 172.17.160.34 172.17.160.35 172.17.160.36 172.17.160.37 172.17.160.38 172.17.160.39 172.17.160.40 172.17.160.42 192.168.4.210 192.168.4.214 192.168.4.215 192.168.4.216 192.168.4.217 192.168.4.218 192.168.4.219					
Microsoft Windows SMBv1 Multiple Vulnerabilities **Impact:** "The remote Windows host has Microsoft Server Message Block 1.0 (SMBv1) enabled. It is, therefore, affected by multiple vulnerabilities: - Multiple information disclosure vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to disclose sensitive information. (CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276) - Multiple denial of service vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of requests. An unauthenticated,	172.16.160.33 172.16.160.34 172.16.160.35 172.16.160.37 172.16.160.38 172.16.160.39 172.16.160.41 172.17.160.33 172.17.160.34 172.17.160.35 172.17.160.37 172.17.160.38 172.17.160.39	**High**	It was observed that the remote Windows host has Microsoft Server Message Block 1.0 (SMBv1) enabled.	"It is recommended to apply the applicable security update for your Windows version : - Windows Server 2008 : KB4018466 - Windows 7 : KB4019264 - Windows Server 2008 R2 : KB4019264 - Windows Server 2012 : KB4019216 - Windows 8.1 / RT 8.1. : KB4019215 - Windows Server 2012 R2 : KB4019215 - Windows 10 : KB4019474 - Windows 10 Version 1511 : KB4019473 - Windows 10 Version 1607 : KB4019472 - Windows 10 Version 1703 : KB4016871 - Windows Server 2016 : KB4019472"	**Open**	**Open**

remote attacker can exploit these vulnerabilities, via a specially crafted SMB request, to cause the system to stop responding. (CVE-2017-0269, CVE-2017-0273, CVE-2017-0280) - Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to execute arbitrary code. (CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279)"						
MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) **Impact:** An arbitrary remote code vulnerability exists in the implementation of the Remote Desktop Protocol (RDP) on the remote Windows host. The vulnerability is due to the way that RDP accesses an object in memory that has been improperly initialized or has been deleted. If RDP has been enabled on the affected system, an unauthenticated, remote attacker could	172.16.160.30 172.17.160.30 192.168.4.218	**High**	It was observed that the remote Windows host could allow arbitrary code execution.	It is recommended to implement patches for Windows XP, 2003, 2008, 7, and 2008 r2 released by Microsoft.	**Open**	**Open**

leverage this vulnerability to cause the system to execute arbitrary code by sending a sequence of specially crafted RDP packets to it.						
MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check) **Impact:** An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148) - An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)	172.16.160.30 172.16.160.31 172.16.160.32 172.16.160.33 172.16.160.34 172.16.160.35 172.16.160.37 172.16.160.38 172.16.160.39 172.16.160.41 172.17.160.30 172.17.160.31 172.17.160.32 172.17.160.33 172.17.160.34 172.17.160.35 172.17.160.37 172.17.160.38 172.17.160.39 192.168.4.218 192.168.4.219	**High**	It has been observed that device is not updated to the MS SMB security patch (MS17-010)	It is recommended to follow the below mentioned. Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8. REFERENCE: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010	**Open**	**Open**
SNMP Agent Default Community Name (public) **Impact:** It is possible to obtain the default community	172.16.202.50 172.16.202.51 172.16.202.55 172.17.202.50 172.17.202.51 172.17.202.55	**High**	It was observed that the community's name of the remote SNMP	It is recommended to disable the SNMP service on the remote host if you do not use it.	**Open**	**Open**

name of the remote SNMP server. An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).			server can be guessed	Either filter incoming UDP packets going to this port, or change the default community string.		
SSH Protocol Version 1 Session Key Retrieval **Impact:** These protocols are not completely cryptographically safe so they should not be used.	172.16.202.50 172.16.202.51 172.16.202.55 172.17.202.50 172.17.202.51 172.17.202.55	**High**	It has been observed that the remote service offers an insecure cryptographic protocol.	It is recommended to disable compatibility with version 1 of the SSH protocol. **References:** https://community.cisco.com/t5/security-knowledge-base/guide-to-better-ssh-security/ta-p/3133344 https://www.sonicwall.com/support/knowledge-base/how-to-fix-the-error-ssh-protocol-version-1-session-key-retrieval/170505477314897/	**Open**	**Open**
SSL Certificate Signed Using Weak Hashing Algorithm **Impact:** An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service	172.16.160.30 172.16.160.33 172.16.160.34 172.16.160.35 172.17.160.30 172.17.160.33 172.17.160.34 172.17.160.35 192.168.4.210 192.168.4.214 192.168.4.215 192.168.4.216 192.168.4.217 192.168.4.218 192.168.4.219	**High**	It has been observed that SSL certificate is signed using SHA-1 With RSA Encryption.	It is recommended to sign SSL certificate using strong encryption algorithm such as SHA-512. **References:** https://tools.ietf.org/html/rfc3279	**Open**	**Open**

SSL Medium Strength Cipher Suites Supported (SWEET32) **Impact:** The remote host supports the use of SSL ciphers that offer medium strength encryption that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.	172.16.160.30 172.16.160.33 172.16.160.34 172.16.160.35 172.16.202.50 172.16.202.51 172.16.202.55 172.17.160.30 172.17.160.33 172.17.160.34 172.17.160.35 172.17.202.50 172.17.202.51 172.17.202.55 192.168.4.160 192.168.4.161 192.168.4.200 192.168.4.210 192.168.4.214 192.168.4.215 192.168.4.216 192.168.4.217 192.168.4.218 192.168.4.219	**High**	It has been observed that SSL is using medium strength encryption such as DES-CBC3-SHA which can be easily compromised if the attacker is on the same physical network.	It is recommended to reconfigure the affected application, if possible, to avoid use of medium strength ciphers. **References:** https://www.openssl.org/blog/blog/2016/08/24/sweet32/	**Open**	**Open**
VNC Server Unauthenticated Access **Impact:** The VNC server installed on the remote host allows an attacker to connect to the remote host as no authentication is required to access this service. The VNC server sometimes sends the connected user to the XDM login screen. Unfortunately, Nessus cannot identify this situation. in such a case, it is not possible to go further without valid credentials and this alert may be ignored.	172.16.160.36 172.16.160.38 172.16.160.39 172.17.160.36 172.17.160.38 172.17.160.39	**High**	It is observed that the remote VNC server does not require authentication.	It is recommended to disable the No Authentication security type.	**Open**	**Open**
HTTP TRACE / TRACK Methods Allowed. **Impact:** The remote web server supports the TRACE	172.16.160.30 172.17.160.30	**Medium**	It is observed that debugging functions are enabled on the remote web server.	It is recommended to disable these HTTP methods.	**Open**	**Open**

and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.						
Microsoft Windows EFSRPC NTLM Reflection Elevation of Privilege (PetitPotam) (Remote). **Impact:** An unauthenticated, remote attacker can exploit this, by sending a specially crafted EFSRPC request, to cause the affected host to connect to a malicious server. An attacker can then utilize an NTLM relay to impersonate the target host and authenticate against remote services.	192.168.4.200	Medium	It is observed that the remote host is affected by an NTLM reflection elevation of privilege vulnerability.	It is recommended to apply the updates supplied by the vendor. Optionally, refer to Microsoft's KB5005413 for mitigation guidance. RPC filters may also be implemented to block remote access to the interface UUIDs necessary for this exploit.	Open	Open
MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) **Impact:** Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.0. Hence an attacker can perform man-in-the-middle attack against the remote host.	172.16.160.30 172.16.160.31 172.16.160.32 172.17.160.30 172.17.160.31 172.17.160.32 192.168.4.218 192.168.4.219	Medium	It has been observed that the remote Windows host is affected by an elevation of privilege vulnerability.	It is recommended to implement the Microsoft released set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10. **References:** http://badlock.org/	Open	Open
Network Time Protocol (NTP) Mode 6 Scanner **Impact:** An unauthenticated, remote attacker could potentially exploit this, via a specially crafted	172.16.202.50 172.16.202.51 172.16.202.55 172.17.202.50 172.17.202.51 172.17.202.55	Medium	It has been observed that a remote NTP server responds to mode 6 queries.	It is recommended to restrict NTP mode 6 queries. References: https://www.ibm.com/support/pages/ibm-aix-disable-ntp-	Open	Open

mode 6 query, to cause a reflected denial of service condition.				mode-6-and-7-queries https://community.cisco.com/t5/other-data-center-subjects/how-to-restrict-ntp-mode-6-queries/td-p/3335720		
Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness **Impact:** The MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.	172.16.160.30 172.16.160.33 172.16.160.34 172.16.160.35 172.17.160.30 172.17.160.33 172.17.160.34 172.17.160.35 192.168.4.200 192.168.4.214 192.168.4.218	Medium	It is observed the remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption.	It is recommended to force the use of SSL as a transport layer for this service if supported, or/and. Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available. **References:** http://technet.microsoft.com/en-us/library/cc782610.aspx https://www.tenable.com/plugins/nessus/18405	Open	Open
SMB Signing not required. **Impact:** Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.	172.16.160.30 172.16.160.31 172.16.160.32 172.16.160.33 172.16.160.34 172.16.160.35 172.16.160.36 172.16.160.37 172.16.160.38 172.16.160.39 172.16.160.40 172.16.160.41 172.16.160.42 172.17.160.30 172.17.160.31 172.17.160.32 172.17.160.33	Medium	It has been observed that remote host does not require SMB Signing.	It is recommended to enable signing is on the remote SMB server. **References:** How to resolve SMB Signing not required Vulnerability - GISPP	Open	Open

	172.17.160.34 172.17.160.35 172.17.160.36 172.17.160.37 172.17.160.38 172.17.160.39 172.17.160.40 172.17.160.42 192.168.4.160 192.168.4.161 192.168.4.210 192.168.4.214 192.168.4.215 192.168.4.216 192.168.4.217 192.168.4.218 192.168.4.219					
SNMP 'GETBULK' Reflection DDoS **Impact:** A remote attacker can use this SNMP server to conduct a reflected distributed denial of service attack on an arbitrary remote host.	172.16.202.50 172.16.202.51 172.17.202.50 172.17.202.51 172.17.202.55	**Medium**	It was observed that the remote SNMP daemon is affected by a vulnerability that allows a reflected distributed denial of service attack.	It is recommended to disable the SNMP service on the remote host if you do not use it. Otherwise, restrict and monitor access to this service, and consider changing the default 'public' community string.	**Open**	**Open**
SSL Certificate Chain Contains Weak RSA Keys. **Impact:** At least one of the X.509 certificates sent by the remote host has a key that is shorter than 1024 bits. Such keys are considered weak due to advances in available computing power decreasing the time required to factor cryptographic keys. Some SSL implementations, notably Microsoft's, may consider this SSL chain to be invalid due to the length of one or more of the RSA keys it contains.	172.16.202.50 172.16.202.51 172.16.202.55 172.17.202.50 172.17.202.51 172.17.202.55	**Medium**	It is observed that the X.509 certificate chain used by this service contains certificates with RSA keys shorter than 1024 bits.	It is recommended to replace the certificate in the chain with the weak RSA key with a stronger key, and reissue any certificates it signed	**Open**	**Open**

SSL Certificate with Wrong Hostname. **Impact:** The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.	192.168.4.160 192.168.4.161 192.168.4.200 192.168.4.210 192.168.4.214 192.168.4.215 192.168.4.216 192.168.4.217 192.168.4.218 192.168.4.219	Medium	The SSL certificate for this service is for a different host.	Purchase or generate a proper SSL certificate for this service.	Open	Open
SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) **Impact:** This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key.	172.16.160.30 172.17.160.30	Medium	It has been observed that the remote host may be affected by a vulnerability that allows a remote attacker to potentially decrypt captured TLS traffic.	It is recommended to Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections. **References:** https://drownattack.com/drown-attack-paper.pdf	Open	Open
SSL RC4 Cipher Suites Supported (Bar Mitzvah) **Impact:** If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.	172.16.160.30 172.16.160.33 172.16.160.34 172.16.160.35 172.16.202.50 172.16.202.51 172.16.202.55 172.17.160.30 172.17.160.33 172.17.160.34 172.17.160.35 172.17.202.50 172.17.202.51 172.17.202.55 192.168.4.160 192.168.4.161 192.168.4.200 192.168.4.210 192.168.4.214	Medium	It has been observed that remote host is using weak cipher suite such as MD5 and SHA-1.	It is recommended to reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support. **References:** http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/	Open	Open

	192.168.4.215 192.168.4.216 192.168.4.217 192.168.4.218 192.168.4.219			https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf		
SSL Weak Cipher Suites Supported. **Impact:** This is considerably easier to exploit if the attacker is on the same physical network.	172.16.160.30 172.16.202.50 172.16.202.51 172.16.202.55 172.17.160.30 172.17.202.50 172.17.202.51 172.17.202.55	**Medium**	It was observed that the remote host supports the use of SSL ciphers that offer weak encryption.	It is recommended to reconfigure the affected application, if possible, to avoid the use of weak ciphers.	**Open**	**Open**
SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK) **Impact:** The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time. A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.	172.16.160.30 172.17.160.30	**Medium**	It is observed that the remote host supports a set of weak ciphers.	It is recommended to reconfigure the service to remove support for EXPORT_RSA cipher suites.	**Open**	**Open**
SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability (POODLE) **Impact:** MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly	172.16.160.30 172.17.160.30	**Medium**	It was observed that the remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE.	It is recommended to disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.	**Open**	**Open**

created SSL 3.0 connections.						
Terminal Services Doesn't Use Network Level Authentication (NLA) Only **Impact:** An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS). Websites using TLS 1.0 will be considered non-compliant by PCI after 30 June 2018.	172.16.160.30 172.16.160.33 172.16.160.34 172.16.160.35 172.17.160.30 172.17.160.33 172.17.160.34 172.17.160.35 192.168.4.200 192.168.4.214 192.168.4.218	Medium	It is observed in addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.	It is recommended to enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows. **References:** https://appuals.com/fix-the-remote-computer-requires-network-level-authentication/	Open	Open
Terminal Services Encryption Level is Medium or Low **Impact:** An attacker can eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.	172.16.160.30 172.16.160.33 172.16.160.34 172.16.160.35 172.17.160.30 172.17.160.33 172.17.160.34 172.17.160.35 192.168.4.200 192.168.4.214 192.168.4.218	Medium	It has been observed that the remote Terminal Services is t configured to use Medium cryptography.	It is recommended to Change RDP encryption level to High & FIPS Compliant **References:** https://techgenix.com/Windows_Terminal_Services/#:~:text=Medium%3A%20encrypts%20both%20the%20data%20sent%20from%20client,40%20bit%20key%2C%20depending%20on%20the%20client%20version.	Open	Open
TLS Version 1.1 Protocol Deprecated **Impact:** Ciphers that support encryption before MAC computation, and authenticated	192.168.4.160 192.168.4.161 192.168.4.200 192.168.4.210 192.168.4.214 192.168.4.215 192.168.4.216 192.168.4.217	Medium	It has been observed that remote host supports TLS version 1.1.	It is recommended to enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. **References:** How to fix the vulnerability is...	Open	Open

encryption modes such as GCM cannot be used with TLS 1.1. Hence an attacker can perform man-in-the-middle attack against the remote host.				TLS Version 1.0 Protocol Detection (tableau.com)		
Unencrypted Telnet Server **Impact:** Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server. SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.	172.16.202.50 172.16.202.51 172.16.202.55 172.17.202.50 172.17.202.51 172.17.202.55	Medium	It is observed that the remote Telnet server transmits traffic in cleartext.	It is recommended to isable the Telnet service and use SSH instead.	Open	Open
SSH Server CBC Mode Ciphers Enabled **Impact:** The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.	172.16.202.50 172.16.202.51 172.16.202.55 172.17.202.50 172.17.202.51 172.17.202.55	Low	It has been observed that remote host is using CBC Mode Cipher. The following Cipher Block Chaining (CBC) algorithms are supported: 3des-cbc aes128-cbc aes256-cbc	It is recommended to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption. **References:** openssl - How to disable CBC-mode ciphers - Information Security Stack Exchange	Open	Open

SSH Weak Key Exchange Algorithms Enabled **Impact:** An attacker can easily exploit the remote SSH server that is configured to allow weak key exchange algorithms.	172.16.202.50 172.16.202.51 172.16.202.55 172.17.202.50 172.17.202.51 172.17.202.55	**Low**	It has been observed that remote host allow weak key exchange algorithms. The following are weak key exchange algorithms that are enabled: diffie-hellman-group-exchange-sha1 diffie-hellman-group1-sha1	It is recommended to disable the weak key exchange algorithms. **References:** SSH Weak Key Exchange Algorithms Enabled - Virtue Security	**Open**	**Open**
SSH Weak MAC Algorithms Enabled **Impact:** An attacker may try to exploit the host as the remote SSH server is configured to allow key exchange algorithms which are considered weak.	172.16.202.50 172.16.202.51 172.16.202.55 172.17.202.50 172.17.202.51 172.17.202.55	**Low**	It has been observed that the remote SSH server is configured to allow key exchange algorithms which are considered weak.	It is recommended to contact the vendor or consult product documentation to disable the weak algorithms. **References:** Disable SSH Weak MAC Algorithms in Linux - DbAppWeb.com	**Open**	**Open**
SSL Certificate Chain Contains RSA Keys Less Than 2048 bits **Impact:** An attacker can easily perform brute force in order to decrypt the encryption with key size shorter than 2048 bits.	172.16.160.30 172.17.160.30	**Low**	It has been observed that 2048-bit RSA key provides 112-bit of security.	It is recommended to replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate. **References:** https://community.hpe.com/t5/Integrity-Servers/SSL-Certificate-Chain-Contains-RSA-Keys-Less-Than-2048-bits-for/td-p/6440854#.Yuj7nHZBw2w	**Open**	**Open**

SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) **Impact:** Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.	172.16.160.30 172.16.160.33 172.16.160.34 172.16.160.35 172.16.202.50 172.16.202.51 172.16.202.55 172.17.160.30 172.17.160.33 172.17.160.34 172.17.160.35 172.17.202.50 172.17.202.51 172.17.202.55	**Low**	It has been observed that the remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.	It is recommended to reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater. **References:** https://www.ibm.com/mysupport/s/question/0D50z00005q4LjCCAU/ssltls-diffiehellman-modulus-1024-bits-logjam?language=en_US	**Open**	**Open**
SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam) **Impact:** The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time. A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.	172.16.160.30 172.17.160.30	**Low**	It is observed that the remote host supports a set of weak ciphers.	It is recommended to reconfigure the service to remove support for EXPORT_DHE cipher suites.	**Open**	**Open**
Terminal Services Encryption Level is not FIPS-140 Compliant **Impact:** The attacker observed the encryption setting	172.16.160.30 172.16.160.33 172.16.160.34 172.16.160.35 172.17.160.30 172.17.160.33 172.17.160.34 172.17.160.35 192.168.4.200	**Low**	It is observed the Client Compatible setting encrypts data sent between the client and the server at the maximum key	It is recommended to change RDP encryption level to: 4. FIPS Compliant **References:** Federal Information Processing Standard	**Open**	**Open**

used by the remote Terminal Services after the attacker easy to expose the all sensitive data.	192.168.4.214 192.168.4.218		strength supported by the client.	(FIPS) 140 Validation - Windows security | Microsoft Learn		

Asset Inventory

Inventory Overview

This section focuses on asset tracking, asset discovery and asset classification. These are the first steps for ensuring operational continuity, reliability and safety. They provide the user with a full context for security events and support routine procedures aimed at improving overall cyber hygiene. Creating an inventory of devices in the network, as well as understanding the relationships and connections between them, is a crucial component in network security.

Asset List DCS-1

Unit6_assets_DCS1.xlsx

S

Asset List DCS-2

Unit6_assets_1_DCS2.xlsx

Mapping of Vulnerabilities with Assets (DCS1)

Final Mapping of C&I Unit-6 Dept Assets:

Refer below excel file contains mapping of vulnerabilities & open ports with the assets , it provides the details of vulnerabilities observed in each asset.

U6_DCS1_Mapping of vulnerabilities wi

Mapping of Vulnerabilities with Assets (DCS2)

Final Mapping of C&I Unit-6 Dept Assets:

Refer **below** excel file contains mapping of vulnerabilities & open ports with the assets , it provides the details of vulnerabilities observed in each asset.

Unit6_Dcs2_Mapping of Vulnerabilities

Recommendations:

14. It is recommended to update the firewall to the latest firmware version.
15. Disable ping (ICMP) response on WAN port.
16. Disable UPnP (Universal plug-and-play).
17. Disable IDENT (i.e., port 113).
18. Disable remote management of the firewall.
19. The setting for a firewall policy should be as specific as possible. Do not use 0.0.0.0 as an address.
20. Regularly check for incoming/outgoing traffic security policy.
21. Allow only HTTPS access to the GUI and SSH access to the CLI.
22. Set up two-factor authentication for administrator.
23. Modify administrator account lockout duration and threshold values.
24. It is recommended that all management access from the internet is turned off.
25. Ensure that your SNMP setting are using SNMPv3 with encryption.
26. All firewall policies should be reviewed every 3 months.

Station LAN Vulnerability Summary

Domain	Critical	High	Medium	Low	Total
Vulnerability Assessment	3	1	3	1	8
Re-validation(closed)	0	0	0	0	0
Re-validation(open)	3	1	3	1	8

Observation Summary

The chart given below represents the vulnerabilities found during network vulnerability testing:

Fig:1

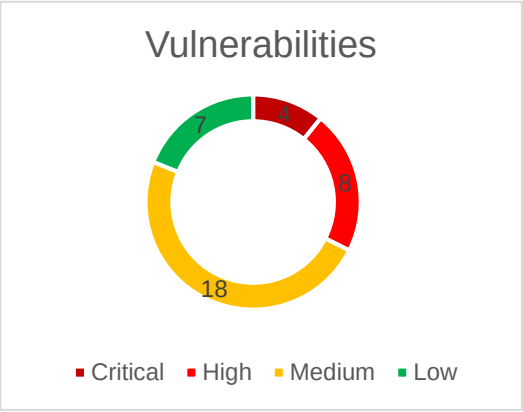


Fig:2

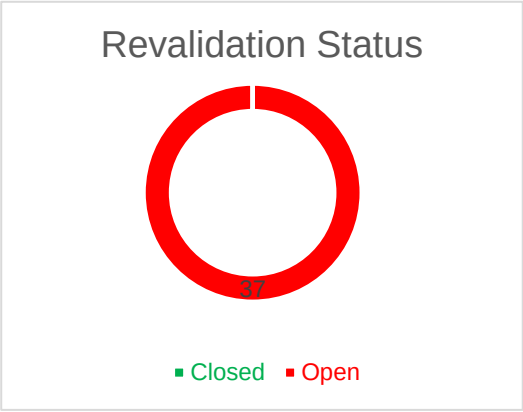


Figure 1: Vulnerability Assessment Test Observations

Illustrates the distribution of observations of Vulnerability testing based on the risk categorization i.e., Critical, High, Medium, and Low.

Figure 2: Vulnerability Assessment Test Observations- Revalidation

Illustrates the closure of Vulnerabilities based on the categorization i.e., Closed, Open.

Note:

Closed: Count considered having vulnerability in all the IP addresses as closed.

Open: Count considered having vulnerability in minimum one IP address as open/unreachable, it may have more different IP addresses which may have the same vulnerability as closed.

Vulnerability Assessment Test Observations

The below table illustrates the distribution of observations of Vulnerability testing based on the risk categorization i.e., Critical, High, Medium, and Low.

Vulnerabilities & Impact	Affected Devices	Risk	Observations	Recommendations	Status	Revalidation Status
SSL Version 2 and 3 Protocol Detection **Impact:** The flaws are as follows: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.	172.17.160.152	**Critical**	It was observed that the remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws	It is recommended to consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead. **Reference:** https://www.imperialviolet.org/2014/10/14/poodle.html https://www.openssl.org/~bodo/ssl-poodle.pdf	**Open**	**Open**
Unsupported Windows OS (remote) **Impact:** A system is unsupported when the developer is no longer issuing any software patches or security updates. From that point on, the operating system is stagnant.	172.17.160.152 172.17.160.153	**Critical**	It is observed the remote OS or service pack is no longer supported.	It is recommended to upgrade to a supported service pack or operating system. **References:** https://www.tenable.com/plugins/nessus/108797 https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=windows	**Open**	**Open**
Unsupported Web Server Detection **Impact:** Web Server is put longer the attacker easy to attack the web server and expose the sensitive data.	172.17.160.152	**Critical**	It is observed the remote web server is obsolete and no longer maintained by its vendor or provider.	It is recommended to remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server. **References:**	**Open**	**Open**

				Unsupported Web Server Detection | Tenable®		
SSL Medium Strength Cipher Suites Supported (SWEET32) **Impact:** The remote host supports the use of SSL ciphers that offer medium strength encryption.	172.17.160.152 172.17.160.153 172.17.160.154 172.18.160.50	**High**	It was observed that the remote service supports the use of medium strength SSL ciphers.	It is recommended to reconfigure the affected application to use strong cipher suited and to avoid use of medium strength ciphers. **References:** https://www.openssl.org/blog/blog/2016/08/24/sweet32/ https://sweet32.info	**Open**	**Open**
SMB Signing not required. **Impact:** An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.	172.17.160.152 172.17.160.153 172.17.160.154 172.18.160.50	**Medium**	It was observed that signing is not required on the remote SMB server.	It is recommended to enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. **References:** http://technet.microsoft.com/en-us/library/cc731957.aspx	**Open**	**Open**
TLS Version 1.1 Protocol Deprecated **Impact:** TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and	172.17.160.154 172.18.160.50	**Medium**	It was observed that the emote service accepts connections encrypted using TLS 1.1	It is recommended enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. **References:**	**Open**	**Open**

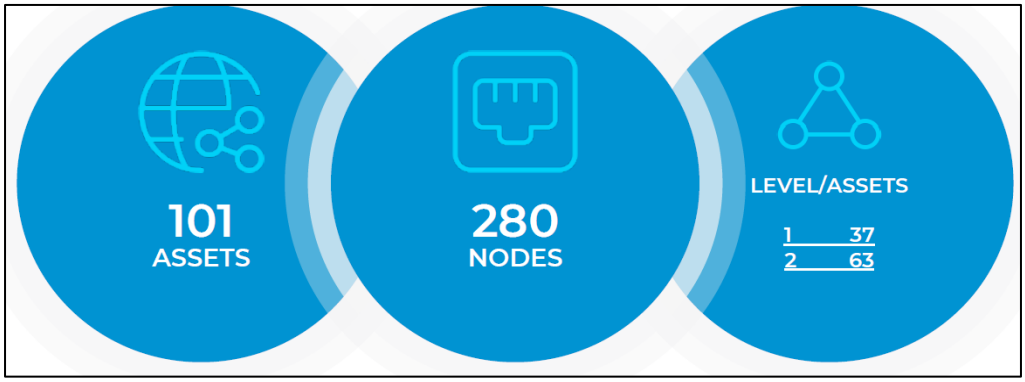
authenticated encryption modes such as GCM cannot be used with TLS 1.1				https://datatracker.ietf.org/doc/html/rfc8996		
Terminal Services Doesn't Use Network Level Authentication (NLA) Only **Impact:** An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS).	172.17.160.152 172.17.160.153 172.17.160.154 172.18.160.50	**Medium**	It was observed in addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.	It is recommended to enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows. **References:** https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11)	**Open**	**Open**
SSL Certificate Chain Contains RSA Keys Less Than 2048 bits. **Impact:** At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014, must be at least 2048 bits.	172.17.160.152	**Low**	It is observed a 2048-bit RSA key provides 112-bit of security. Given that TLS certificates are valid for two years maximum (soon to be decreased to one), 2048-bit RSA key length fulfills the NIST recommendation until late in this decade.	It is recommended to replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate. References: https://community.hpe.com/t5/Integrity-Servers/SSL-Certificate-Chain-Contains-RSA-Keys-Less-Than-2048-bits-for/td-p/6440854#.Yuj7nHZBw2w	**Open**	**Open**

Electrical Department

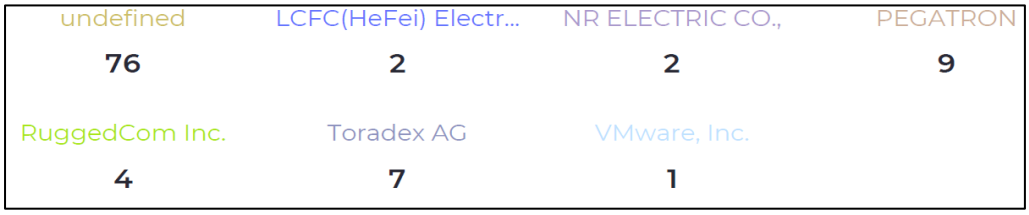
SAS Network

Asset classification

The assessment was able to identify 101 all devices and discovered 0 vulnerabilities.
Based on the assessment, risk mitigation and remediation are needed to reduce the risk of nation-level threat vector and improve the cyber posture.

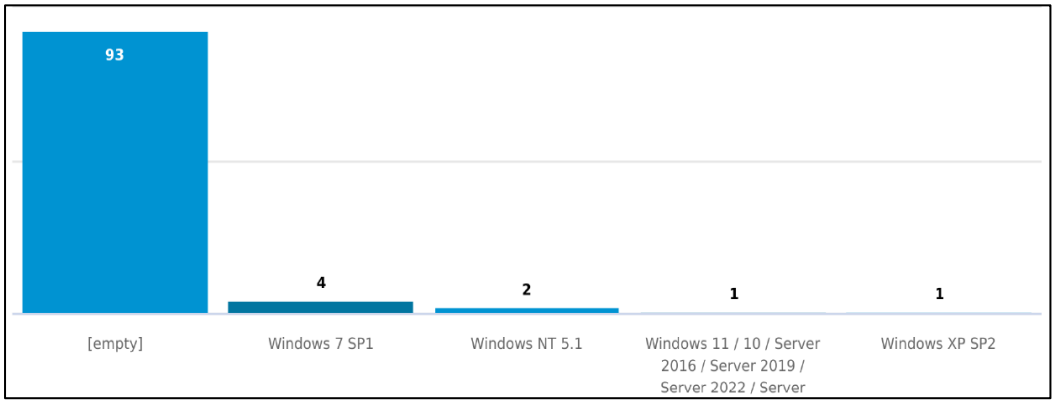


Vendors



Asset Types

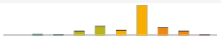
Operating systems



Risk

Vulnerability Score

GT Risk Assessment Report provides a comprehensive risk analysis related to network behaviour and assets. Based on overall assessment for **NTPC TANDA**, all network risk score is 0.

NAME	TYPE	OS/FIRMWARE	COUNT	SCORE DISTRIBUTION	SCORE GROUPS (Low, Medium, High)
LDCGW1	computer	Windows 7 SP1	2226		40 1 741 445
OWS1	computer	Windows 7 SP1	2226		40 1 741 445
CCROWS1	computer	Windows 7 SP1	2226		40 1 741 445
CCROWS2	computer	Windows 7 SP1	2226		40 1 741 445
WCCBLRLAP660	computer	Windows XP SP2	1027		21 498 508

Assets with confirmed CPEs	0
Assets with Firmware Discovered	280
Number of Hosts with Vulnerabilities	0
Number of Vulnerabilities	0
Vulnerability Average Score	0

Vulnerability summary

Malware detected	0
Different Operating Systems	5
Different Types of Technologies	10
Attempted Links to Public Internet	0
Multi-homed Assets	6
Different Firmware Versions	1
Clients Accessing SMB Shares	13
Insecure Protocol Links in the Environment	55

Clients accessing SMB Shares

FROM	TO	PROTOCOL	TX PACKETS	TX BYTES
192.168.1.1	192.168.1.101	smb		
192.168.1.22	192.168.1.101	smb		
192.168.1.101	192.168.1.67	smb		
192.168.1.101	192.168.1.21	smb		
192.168.1.101	192.168.1.37	smb		
192.168.1.101	192.168.1.22	smb		
192.168.1.101	192.168.1.1	smb		
192.168.1.101	192.168.1.23	smb		
192.168.1.101	192.168.1.20	smb		
192.168.1.21	192.168.1.101	smb		
192.168.1.67	192.168.1.101	smb		
192.168.1.20	192.168.1.101	smb		
192.168.1.37	192.168.1.101	smb		

Revalidation

Devices Vulnerability Summary

Switches

Domain	Critical	High	Medium	Low	Total
Vulnerability Assessment	1	1	6	0	8
Re-validation(closed)	0	0	0	0	0
Re-validation(open)	1	1	6	0	8

Servers

Domain	Critical	High	Medium	Low	Total
Vulnerability Assessment	0	0	5	0	5
Re-validation(closed)	0	0	0	0	0
Re-validation(open)	0	0	5	0	5

Workstations

Domain	Critical	High	Medium	Low	Total
Vulnerability Assessment	0	1	6	0	7
Re-validation(closed)	0	0	0	0	0
Re-validation(open)	0	1	6	0	7

LDGCW

Domain	Critical	High	Medium	Low	Total
Vulnerability Assessment	4	5	13	1	23
Re-validation(closed)	0	0	0	0	0
Re-validation(open)	4	5	13	1	23

Switches

Observation Summary

The chart given below represents the vulnerabilities found during network vulnerability testing:

Fig:1

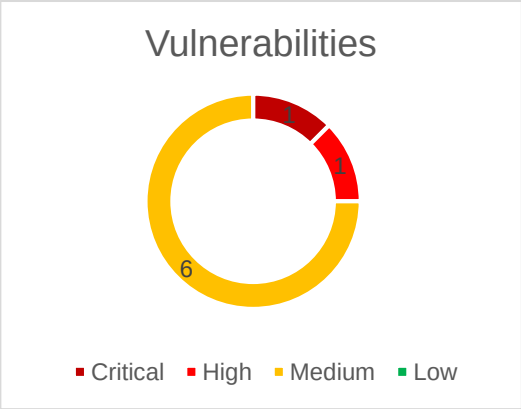


Fig:2

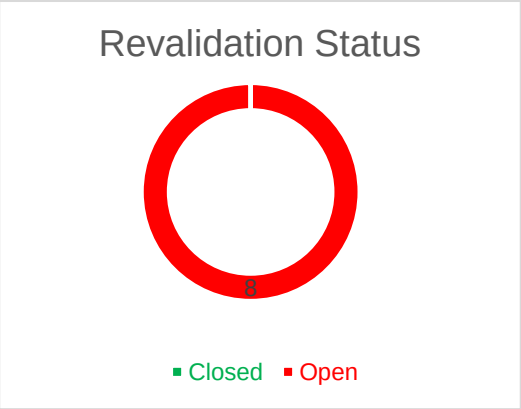


Figure 1: Vulnerability Assessment Test Observations

Illustrates the distribution of observations of Vulnerability testing based on the risk categorization i.e., Critical, High, Medium, and Low.

Figure 2: Vulnerability Assessment Test Observations- Revalidation

Illustrates the closure of Vulnerabilities based on the categorization i.e., Closed, Open.

Note:

Closed: Count considered having vulnerability in all the IP addresses as closed.

Open: Count considered having vulnerability in minimum one IP address as open/unreachable, it may have more different IP addresses which may have the same vulnerability as closed.

Vulnerability Assessment Test Observations

The below table illustrates the distribution of observations of Vulnerability testing based on the risk categorization i.e., Critical, High, Medium, and Low.

Vulnerabilities & Impact	Affected Devices	Risk	Observations	Recommendations	Status	Revalidation status
SSL/TLS Deprecated Ciphers Unsupported **Impact:** It allows an attacker to recover the plaintext or potentially violate the integrity of connections.	192.168.1.16 192.168.1.17 192.168.1.38 192.168.1.7	**Critical**	It was observed that the remote host has open SSL/TLS ports which advertise deprecated cipher suites. The ciphers contained in these suites are no longer supported by most major ssl libraries such as OpenSSL, NSS, Mbed TLS, and wolfSSL and, as such, should not be used for secure communication.	It is recommended to upgrade to a cipher suite which does not contain deprecated ciphers.	**Open**	**Open**
SSL Certificate Signed Using Weak Hashing Algorithm **Impact:** An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service	192.168.1.16 192.168.1.17 192.168.1.38 192.168.1.7	**High**	It has been observed that SSL certificate is signed using SHA-1 With RSA Encryption. .	It is recommended to sign SSL certificate using strong encryption algorithm such as SHA-512. **References:** https://tools.ietf.org/html/rfc3279	**Open**	**Open**
SSL Certificate Cannot Be Trusted **Impact:** If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web	192.168.1.16 192.168.1.17 192.168.1.38 192.168.1.7	**Medium**	It has been observed that remote host is using untrusted SSL certificate. SSL certificate expired on Jan 01 00:00:00 2020 GMT	It is recommended to purchase or generate a proper SSL certificate for this service. **References:** https://www.itu.int/rec/T-REC-X.509/en	**Open**	**Open**

server. This could make it easier to carry out man-in-the-middle attacks against the remote host.				https://en.wikipedia.org/wiki/X.509		
SSL Certificate Chain Contains RSA Keys Less Than 2048 bits. **Impact:** An attacker can perform man-in-the-middle attack.This can lead to sensitive data loss.	192.168.1.16 192.168.1.17 192.168.1.38 192.168.1.7	Medium	It was observed that the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, /certificates issued after January 1, 2014, must be at least 2048 bits.	It is recommended to replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.	Open	Open
SSL Self-Signed Certificate **Impact:** If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.	192.168.1.16 192.168.1.17 192.168.1.38 192.168.1.7	Medium	It has been observed that remote host is using SSL Self-Signed Certificate.	It is recommended to purchase or generate a proper SSL certificate for this service. **References:** https://confluence.atlassian.com/bitbucketserverkb/resolving-ssl-self-signed-certificate-errors-806029899.html	Open	Open
SSL Weak Cipher Suites Supported **Impact:** The attackers can spoof the identity of the victim. Unlike CA-issued certificates, self-signed certificates cannot be revoked. The inability to quickly find and revoke private key associated with a	192.168.1.16 192.168.1.17 192.168.1.38 192.168.1.7	Medium	It is observed this is considerably easier to exploit if the attacker is on the same physical network.	It is recommended to Reconfigure the affected application, if possible, to avoid the use of weak ciphers. **References:** How to Disable Weak SSL Protocols and Ciphers in IIS | Wayne Zimmerman's Blog	Open	Open

self-signed certificate creates serious risk.						
TLS Version 1.1 Protocol Detection **Impact:** Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1. Hence an attacker can perform man-in-the-middle attack against the remote host.	192.168.1.16 192.168.1.17 192.168.1.38 192.168.1.7	**Medium**	It has been observed that remote host supports TLS version 1.1.	It is recommended to enable support for TLS 1.2 and/or 1.3 and disable support for TLS 1.1. **References:** How to fix the vulnerability issue: TLS Version 1.0 Protocol Detection (tableau.com)	**Open**	**Open**
Unencrypted Telnet Server **Impact:** An attacker may eavesdrop on a Telnet session and obtain credentials or other sensitive information. Use of SSH is preferred nowadays as it protects credentials from eavesdropping and can tunnel additional data streams such as the X11 session.	192.168.1.16 192.168.1.17 192.168.1.38 192.168.1.7	**Medium**	It is observed SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.	It is recommended to Disable the Telnet service and use SSH instead. **References:** How to Disable Telnet and Enable SSH on Cisco IOS Devices (networkstraining.com)	**Open**	**Open**

Servers

Observation Summary

The chart given below represents the vulnerabilities found during network vulnerability testing:

Fig:1

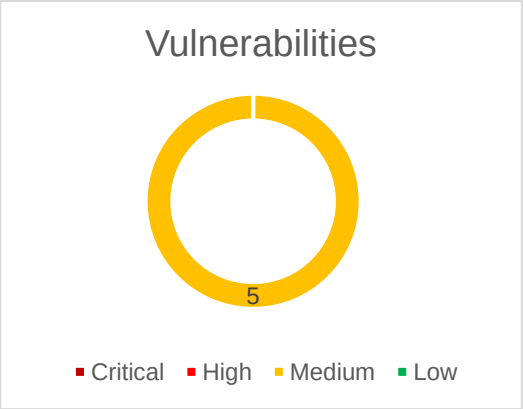


Fig:2

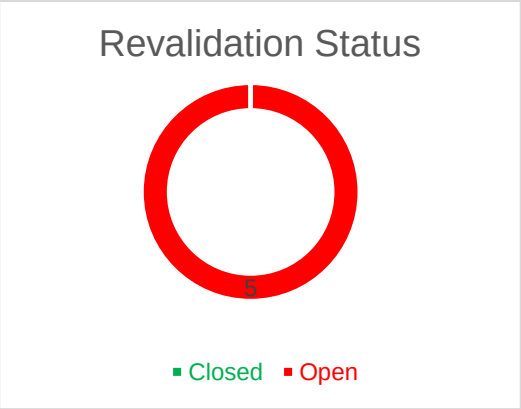


Figure 1: Vulnerability Assessment Test Observations

Illustrates the distribution of observations of Vulnerability testing based on the risk categorization i.e., Critical, High, Medium, and Low.

Figure 2: Vulnerability Assessment Test Observations- Revalidation

Illustrates the closure of Vulnerabilities based on the categorization i.e., Closed, Open.

Note:

Closed: Count considered having vulnerability in all the IP addresses as closed.

Open: Count considered having vulnerability in minimum one IP address as open/unreachable, it may have more different IP addresses which may have the same vulnerability as closed.

Vulnerability Assessment Test Observations

The below table illustrates the distribution of observations of Vulnerability testing based on the risk categorization i.e., Critical, High, Medium, and Low.

Vulnerabilities & Impact	Affected Devices	Risk	Observations	Recommendations	Status	Revalidation Status
SMB Signing not required. **Impact:** Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.	192.168.1.23	Medium	It has been observed that remote host does not require SMB Signing.	It is recommended to enable signing is on the remote SMB server. **References:** How to resolve SMB Signing not required Vulnerability - GISPP	Open	Open
SSL Certificate Cannot Be Trusted **Impact:** If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.	192.168.1.23	Medium	It has been observed that remote host is using untrusted SSL certificate. SSL certificate expired on Jan 01 00:00:00 2020 GMT	It is recommended to purchase or generate a proper SSL certificate for this service. **References:** https://www.itu.int/rec/T-REC-X.509/en https://en.wikipedia.org/wiki/X.509	Open	Open
SSL Certificate with Wrong Hostname **Impact:** It allows an attacker to perform man-in-the-middle attack.	192.168.1.23	Medium	It was observed that the 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.	It is recommended to purchase or generate a proper SSL certificate for this service. **References:** https://www.tenable.com/plugins/nessus/45411	Open	Open

SSL Self-Signed Certificate **Impact:** If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.	192.168.1.23	**Medium**	It has been observed that remote host is using SSL Self-Signed Certificate.	It is recommended to purchase or generate a proper SSL certificate for this service. **References:** https://confluence.atlassian.com/bitbucketserverkb/resolving-ssl-self-signed-certificate-errors-806029899.html	**Open**	**Open**
TLS Version 1.1 Protocol Deprecated / Detection **Impact**: An attacker may perform man-in-the-middle attack. As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.	192.168.1.23	**Medium**	It was observed that the service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. It was observed that the service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.	It is recommended to enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.	**Open**	**Open**

Workstation

Observation Summary

The chart given below represents the vulnerabilities found during network vulnerability testing:

Fig:1

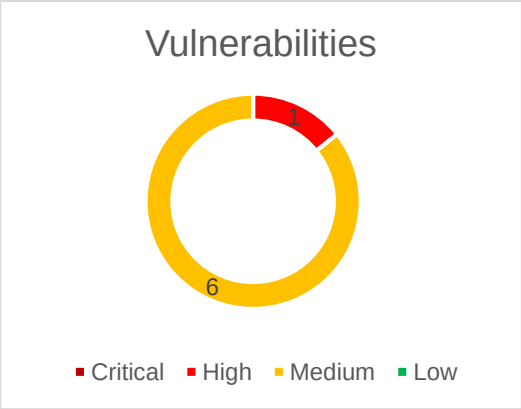


Fig:2

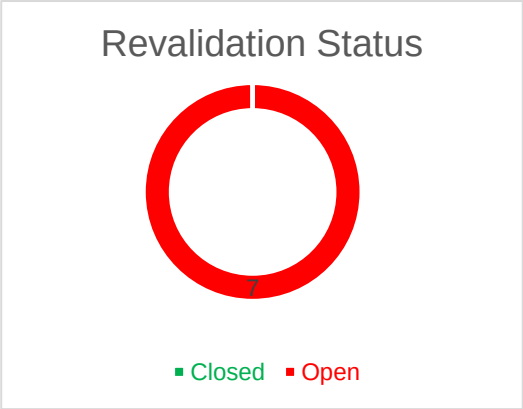


Figure 1: Vulnerability Assessment Test Observations

Illustrates the distribution of observations of Vulnerability testing based on the risk categorization i.e., Critical, High, Medium, and Low.

Figure 2: Vulnerability Assessment Test Observations- Revalidation

Illustrates the closure of Vulnerabilities based on the categorization i.e., Closed, Open.

Note:

Closed: Count considered having vulnerability in all the IP addresses as closed.

Open: Count considered having vulnerability in minimum one IP address as open/unreachable, it may have more different IP addresses which may have the same vulnerability as closed.

Grant Thornton
An instinct for growth™

Vulnerability Assessment Test Observations

The below table illustrates the distribution of observations of Vulnerability testing based on the risk categorization i.e., Critical, High, Medium, and Low.

Vulnerabilities & Impact	Affected Devices	Risk	Observations	Recommendations	Status	Revalidation status
SMB Server DOUBLEPULSAR Backdoor / Implant Detection (EternalRocks) **Impact:** The implant allows an unauthenticated, remote attacker to use SMB as a covert channel to exfiltrate data, launch remote commands, or execute arbitrary code.	192.168.1.20 192.168.1.21 192.168.1.22 192.168.1.37	**High**	It was observed that presence of DOUBLEPULSAR on the remote Windows host. DOUBLEPULSAR is one of multiple Equation Group SMB implants and backdoors disclosed on 2017/04/14 by a group known as the Shadow Brokers.	It is recommended to remove the DOUBLEPULSAR backdoor / implant and disable SMBv1.	**Open**	**Open**
Network Time Protocol (NTP) Mode 6 Scanner **Impact:** An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause a reflected denial of service condition.	192.168.1.20	**Medium**	It was observed that the remote NTP server responds to mode 6 queries. Devices that respond to these queries have the potential to be used in NTP amplification attacks.	It is recommended to restrict NTP mode 6 queries.	**Open**	**Open**
SMB Signing not required. **Impact:** Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.	192.168.1.23	**Medium**	It has been observed that remote host does not require SMB Signing.	It is recommended to enable signing is on the remote SMB server. **References:** How to resolve SMB Signing not required Vulnerability - GISPP	**Open**	**Open**
SSL Certificate Cannot Be Trusted **Impact:** If the remote host is a public host in production, any break in the chain	192.168.1.23	**Medium**	It has been observed that remote host is using untrusted SSL certificate. SSL certificate expired	It is recommended to purchase or generate a proper SSL certificate for this service.	**Open**	**Open**

makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.			on Jan 01 00:00:00 2020 GMT	**References:** https://www.itu.int/rec/T-REC-X.509/en https://en.wikipedia.org/wiki/X.509		
SSL Certificate with Wrong Hostname **Impact:** It allows an attacker to perform man-in-the-middle attack	192.168.1.23	**Medium**	It was observed that the 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.	It is recommended to purchase or generate a proper SSL certificate for this service. **References:** https://www.tenable.com/plugins/nessus/45411	**Open**	**Open**
SSL Self-Signed Certificate **Impact:** If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.	192.168.1.23	**Medium**	It has been observed that remote host is using SSL Self-Signed Certificate.	It is recommended to purchase or generate a proper SSL certificate for this service. **References:** https://confluence.atlassian.com/bitbucketserverkb/resolving-ssl-self-signed-certificate-errors-806029899.html	**Open**	**Open**
TLS Version 1.1 Protocol Deprecated / Detection **Impact**: An attacker may perform man-in-the-middle attack. As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.	192.168.1.23	**Medium**	It was observed that the service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. It was observed that the service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate	It is recommended to enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.	**Open**	**Open**

			these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.			

LDGCW

Observation Summary

The chart given below represents the vulnerabilities found during network vulnerability testing:

Fig:1

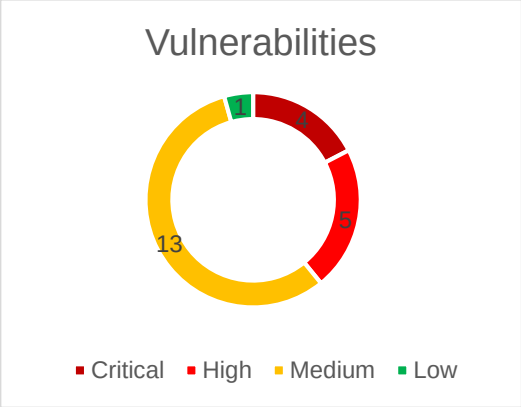


Fig:2

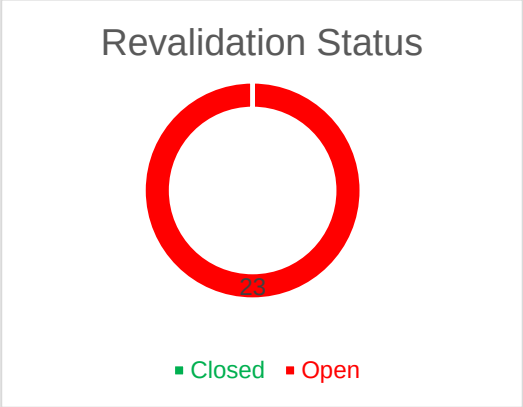


Figure 1: Vulnerability Assessment Test Observations

Illustrates the distribution of observations of Vulnerability testing based on the risk categorization i.e., Critical, High, Medium, and Low.

Figure 2: Vulnerability Assessment Test Observations- Revalidation

Illustrates the closure of Vulnerabilities based on the categorization i.e., Closed, Open.

Note:

Closed: Count considered having vulnerability in all the IP addresses as closed.

Open: Count considered having vulnerability in minimum one IP address as open/unreachable, it may have more different IP addresses which may have the same vulnerability as closed.

Vulnerability Assessment Test Observations

The below table illustrates the distribution of observations of Vulnerability testing based on the risk categorization i.e., Critical, High, Medium, and Low.

Vulnerabilities & Impact	Affected Devices	Risk	Observations	Recommendations	Status	Revalidation Status
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check) **Impact:** An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.	192.168.1.1	**Critical**	It was observed that remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP).	It is recommended that Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.	**Open**	**Open**
SSL Version 2 and 3 Protocol Detection **Impact**: An attacker can conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.	192.168.1.1	**Critical**	It has been observed that devices are using SSL version 2.0 and 3.0.	It is recommended to disable SSL 2.0 and 3.0. Use TLS 1.2 with higher cipher suites listed below. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256k1) - A TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256k1) - A TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256k1) - A TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256k1) – A 2 **References:** https://www.imperialviolet.org/2014/10/14/poodle.html https://tools.ietf.org/html/rfc7507	**Open**	**Open**

Unsupported Web Server Detection **Impact:** Web Server is put longer the attacker easy to attack the web server and expose the sensitive data.	192.168.1.1	**Critical**	It is observed the remote web server is obsolete and no longer maintained by its vendor or provider.	It is recommended to remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server. **References:** https://www.tenable.com/plugins/nessus/34460 https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=apache+httpcore+4.4.3 https://cwe.mitre.org/data/definitions/447.html	**Open**	**Open**
Unsupported Windows OS (remote) **Impact:** An attacker easy to attack the web server and expose the sensitive data.	192.168.1.1	**Critical**	It was observed that remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.	It is recommended to upgrade to a supported service pack or operating system	**Open**	**Open**
MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check) **Impact:** An attacker can exploit this issue by sending specially crafted packets to a Windows server.	192.168.1.1	**High**	It was observed that remote Windows host is affected by a remote code execution vulnerability due to improper processing of packets by the Secure Channel (Schannel) security package.	It is recommended that Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2.	**Open**	**Open**

MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check) **Impact:** Successful exploitation of this vulnerability leads to Remote code execution. Also, this may lead to installation of ransomware, malwares, crypto-jacking, or any other worm-like software's.	192.168.1.1	**High**	It was observed that he remote Windows host is affected by the remote code execution vulnerability.	It is recommended to install the patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8. It is also recommended for unsupported Windows operating systems, e.g., Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft. Additionally, it is recommending that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.	**Open**	**Open**
Network Time Protocol Daemon (ntpd) read_mru_list() Remote DoS **Impact:** An unauthenticated, remote attacker can exploit this, via a specially crafted NTP	192.168.1.1	**High**	It was observed that remote NTP server is affected by a denial of service vulnerability due to improper validation of mrulist queries.	It is recommended to upgrade to NTP version 4.2.8p9 or later.	**Open**	**Open**

mrulist query packet, to terminate the ntpd process.						
SSL Certificate Signed Using Weak Hashing Algorithm **Impact:** An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.	192.168.1.1	**High**	It has been observed that SSL certificate is signed using SHA-1 With RSA Encryption. .	It is recommended to sign SSL certificate using strong encryption algorithm such as SHA-512. **References:** https://tools.ietf.org/html/rfc3279	**Open**	**Open**
SSL Medium Strength Cipher Suites Supported (SWEET32) **Impact:** The remote host supports the use of SSL ciphers that offer medium strength encryption that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.	192.168.1.1	**High**	It has been observed that SSL is using medium strength encryption such as DES-CBC3-SHA which can be easily compromised if the attacker is on the same physical network.	It is recommended to reconfigure the affected application if possible, to avoid use of medium strength ciphers. **References:** https://www.openssl.org/blog/blog/2016/08/24/sweet32/	**Open**	**Open**
MS13-006: Vulnerability in Microsoft Windows Could Allow Security Feature Bypass (2785220) (uncredentialed check) **Impact:** An attacker can inject specially crafted content into an SSL/TLS session, which could allow an attacker to bypass security features of SSLv3 and TLS protocols in order to intercept communications.	192.168.1.1	**Medium**	It was observed that remote host contains a flaw in the handling of SSL version 3 (SSLv3) and TLS (Transport Layer Security) protocols.	It was recommended that Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, and 2012. For other SSL/TLS implementations, contact the vendor for updates.	**Open**	**Open**

MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) **Impact:** A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.	192.168.1.1	**Medium**	It was observed that remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper	It is recommended to Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.	**Open**	**Open**
Network Time Protocol (NTP) Mode 6 Scanner **Impact:** An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause a reflected denial of service condition.	192.168.1.1	**Medium**	It was observed that the remote NTP server responds to mode 6 queries. Devices that respond to these queries have the potential to be used in NTP amplification attacks.	It is recommended to restrict NTP mode 6 queries.	**Open**	**Open**
Remote Desktop Protocol Server Man-in-the-Middle Weakness **Impact:** A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.	192.168.1.1	**Medium**	It was observed that the remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client	It is recommended to - Force the use of SSL as a transport layer for this service if supported, or/and - On Microsoft Windows operating systems, select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	**Open**	**Open**

			and server without being detected.	**References:** http://www.nessus.org/u?8033da0d		
SMB Signing not required. **Impact:** Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.	192.168.1.1	**Medium**	It has been observed that remote host does not require SMB Signing.	It is recommended to enable signing is on the remote SMB server. **References:** How to resolve SMB Signing not required Vulnerability - GISPP	**Open**	**Open**
SSL Certificate Cannot Be Trusted **Impact:** If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.	192.168.1.1	**Medium**	It has been observed that remote host is using untrusted SSL certificate. SSL certificate expired on Jan 01 00:00:00 2020 GMT	It is recommended to purchase or generate a proper SSL certificate for this service. **References:** https://www.itu.int/rec/T-REC-X.509/en https://en.wikipedia.org/wiki/X.509	**Open**	**Open**
SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) **Impact:** A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key.	192.168.1.1	**Medium**	It was observed hat remote host supports SSLv2 and therefore may be affected by a vulnerability that allows a cross-protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured	It is recommended to Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections.	**Open**	**Open**

			TLS traffic to be decrypted.			
SSL RC4 Cipher Suites Supported (Bar Mitzvah) **Impact:** If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.	192.168.1.1	**Medium**	It has been observed that remote host is using weak cipher suite.	It is recommended to reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support. **References:** SSL RC4 Cipher Suites Supported (Bar Mitzvah) (microsoft.com)	**Open**	**Open**
SSL Self-Signed Certificate **Impact:** If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.	192.168.1.1	**Medium**	It has been observed that remote host is using SSL Self-Signed Certificate.	It is recommended to purchase or generate a proper SSL certificate for this service. **References:** https://confluence.atlassian.com/bitbucketserverkb/resolving-ssl-self-signed-certificate-errors-806029899.html	**Open**	**Open**
SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability (POODLE) **Impact:** An attacker can perform a man-in-the-middle (MitM) information disclosure known as POODLE. MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.	192.168.1.1	**Medium**	It has been observed that the remote host is vulnerable to padding oracle attack.	It is recommended to disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled. **References:** How to fix POODLE vulnerability (SSL v3) in Windows - Windows VPS Hosting Blog - AccuWeb Hosting	**Open**	**Open**

Terminal Services Doesn't Use Network Level Authentication (NLA) Only **Impact:** An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS). Websites using TLS 1.0 will be considered non-compliant by PCI after 30 June 2018.	192.168.1.1	Medium	It is observed in addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.	It is recommended to enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows. **References:** https://appuals.com/fix-the-remote-computer-requires-network-level-authentication/	Open	Open
Terminal Services Encryption Level is Medium or Low **Impact:** The Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.	192.168.1.1	Medium	It is observed the Client Compatible setting encrypts data sent between the client and the server at the maximum key strength supported by the client.	Change RDP encryption level to one of: 3. High 4. FIPS Compliant **References:** https://techgenix.com/Windows_Terminal_Services/#:~:text=Medium%3A%20encrypts%20both%20the%20data%20sent%20from%20client,40%20bit%20key%2C%20depending%20on%20the%20client%20version.	Open	Open
TLS Version 1.0 Protocol Detection **Impact:** An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS). Websites using TLS 1.0 will be considered non-	192.168.1.1	Medium	It is observed to TLS 1.2 is more secure, an attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities.	It is recommended to Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0. **References:** https://datatracker.ietf.org/doc/html/rfc8996	Open	Open

compliant by PCI after 30 June 2018.						
Terminal Services Encryption Level is not FIPS-140 Compliant **Impact:** The attacker observed the encryption setting used by the remote Terminal Services after the attacker easy to expose the all sensitive data.	192.168.1.1	**Low**	It is observed the Client Compatible setting encrypts data sent between the client and the server at the maximum key strength supported by the client.	It is recommended to change RDP encryption level to: 4. FIPS Compliant **References:** https://www.tenable.com/plugins/nessus/30218	**Open**	**Open**

Asset Inventory

Inventory Overview

This section focuses on asset tracking, asset discovery and asset classification. These are the first steps for ensuring operational continuity, reliability and safety. They provide the user with a full context for security events and support routine procedures aimed at improving overall cyber hygiene. Creating an inventory of devices in the network, as well as understanding the relationships and connections between them, is a crucial component in network security.

Electrical Asset List

Electrical_Assets_List.xlsx

Final Mapping of Electrical Dept Assets:

Refer below excel file contains mapping of vulnerabilities & open ports with the assets, it provides the details of vulnerabilities observed in each asset.

Mapping of vulnerabilities with a

Recommendations

- All unwanted ports & services running on the systems should be disabled. During this process, it is always good to check the effect on running SCADA system performance (with the help of SCADA vendor). System availability is more important in OT environment.
- Unused ports of network/OT devices such as switch should be disabled.
- Device control and application control policy for OT environment should be implemented.
- Upgradation of system OS should be carried out and the systems should be on latest OS.
- Upgradation of Network Device Firmware should be carried out are regular intervals and should be on latest Firmware.
- Antivirus definitions and OS patch update rule should be defined and implemented.
- Monitor and implement security controls for the communication involving DCS systems (System PC and PLC) which are having the data flow between DCS systems and third-party sources / devices for security checks (with the support of vendor). This will add another layer of security in third party communication involving TCP/IP, OPC, Modbus, etc between DCS systems and third-party sources / devices.

Disclaimer: The audit / assessment has been performed (Point in Time Basis) against most of the technical security controls. It is important to note that tests are valid as on the date of testing. New issues / vulnerabilities are being discovered daily hence it is recommended to conduct proactive assessment periodically and ensure any new changes introduced on the systems/ environment should undergo a comprehensive security assessment to identify and mitigate new threats.

End Of Document

Due to the obsolescence and future unavailability of ET200M modules (phase-out status), we recommend replacing the I/O peripherals with ET200SP-HA I/O peripherals with redundant communication bus PROFINET instead of the current communication bus PROFIBUS-DP.

In connection with the possible installation of the I/O peripheral ET200SP-HA with PROFINET communication, it is also necessary to replace the CPU unit CPU-414-4H with a modern type CPU 410-H which supports PROFINET communication.

In addition, the ET200M and CPU-414-4H do not meet the requirements of the cyber security standard IEC 62443.

1.2. Recommended hardware upgrade of automation station (For 4 units)

DSPW recommend the complete replacing of the existing I/O peripherals ET200M with modern I/O peripherals ET200SP-HA I/O with redundant communication bus PROFINET in the following configuration include replacing of all CPU units CPU-414-4-H by CPU 410-H.

- 10 pcs of processor modules CPU 410-5H incl. the relevant synchr. modules
- 7 pcs of ET200SP-HA interface module IM155-6 PN incl. bus adapters
- 14 pcs of ET200SP-HA digital input module (32x DI, 24Vdc)
- 14 pcs of ET200SP-HA digital output module (32x DO, 24Vdc, 0,5A)
- 14 pcs of ET200SP-HA analog input module (8x AI U/I/TC/4xRTD 2-/3-/4-wire)
- 14 pcs of ET200SP-HA fast multi I/O and counter module (4xAI,8xAO,10xDI/DO)
- 12 pcs of ET200SP-HA carrier module for 8 I/O modules
- 36 pcs of ET200SP-HA terminal block, 32 push-in terminals
- 12 pcs of ET200SP-HA terminal block, 16 push-in terminals

1.3. Recommended upgrade of engineering and operator station (For 4 units)

Hardware delivery (computers):

- 1 pcs of engineering station, notebook DELL Precission, Win 11, WM Player V17
- 8 pcs of operator stations computers SIEMENS IPC 647E, Win10 LTSC 2019
- 16 pcs of monitor DELL Professional P2222H, 22”
- 8x keyboard
- 8x mouse

Software delivery (licences)

- 1 pcs of PCS7 Upgrade Package Engineering from v. 7.1 to v. 8.2
- 1 pcs of PCS7 Upgrade Package Engineering from v. 8.x to v. 9.1
- 8 pcs of PCS7 Upgrade Package OS Server from v. 7.1 to v. 8.2
- 8 pcs of PCS7 Upgrade Package OS Server from v. 8.x to v. 9.1
- 8 pcs of PCS7 Upgrade Softnet-IE S7 Lean

1.4. Related services in the factory (invelt-elektro s.r.o., Pilsen, CZ)

- 8x installation and setting of system upgrade PCS7 (v.7.1 – v.9.1) for new OS IPC647E
- 1x installation and setting of system upgrade PCS7 (v.7.1 – v.9.1) for new engineering

stations (notebook DELL Precission).

- 4x upgrade of process software application PCS7 for automation station
- 8x complete implementation of upgrade process software application into PCS7 v.9.1 in OS IPC647E
- Hardware design modification for ET200M by ET200SP-HA replacement
- Preassembly of I/O peripherals of ET200SP-HA
- Trial and testing of ES, OS, CPU, I/O peripherals ET200SP-HA

1.5. Related services On-Site (NTPC- Tanda) – Supervision only (Assembly in Client Scope)

- Installation of 8 pcs CPU modules CPU410 inside control system cabinets in exchange for existing ones CPU 414-4H
- Installation of 12 racks of I/O peripheral ET200SP-HA inside control system cabinets in exchange of existing ones ET200M
- Reconnection of connectors of I/O modules of ET200SP-HA inside control system cabinets according to modified hardware design
- Connection of communication bus PROFINET inside control system cabinets according to modified hardware design
- Hardware installation of new operator stations
- Verification and testing of communication buses PROFINET, ETHERNET
- Complete testing of system functions of the control system after the upgrade implementation incl. SAT test

All activities of the System Expert (DSPW/INVELT) technicians on the site are billed at an hourly rate include related travel and accommodation costs.

2. Delivery date:

8-10 months after ordering

3. Delivery conditions:

FCA SITE according to the international rules INCOTERMS 2020.

Deliveries will be packed in packaging for oversee transport – wooden boxes.

4. Counter Obligation:

- The control system of the relevant TG available for upgrade, under voltage
- Ensuring of entrances and entrances to the NTPC Tanda complex
- Provision of electrical installation works remain in Client Scope

ANNEXURE-R7

भारत हेवी इलेक्ट्रिकल्स लिमिटेड

Bharat Heavy Electricals Limited

(A GOVERNMENT OF INDIA UNDERTAKING)
ELECTRONICS DIVISION

र.के. तिवारी
पिालक निदेशक

.K. TIWARI
ECUTIVE DIRECTOR

PHONE : OFF : 080-26989000
FAX : 080-26742780
e-mail : rktiwari@bheledn.co.in
P. B. No. 2606, MYSORE ROAD
BANGALORE - 560 026

EDN/CE/SM/DPU/NTPC
9th September 2015

Dear Shri Venkateshwara Rao,

Sub: Processor upgrades (DPU4E to DPU4F) in BHEL's maxDNA C&I systems at various NTPC Projects – reg.

I am pleased to inform that BHEL-EDn has very closely partnered with NTPC in meeting the **C&I** system requirements of various projects through our maxDNA based controls. As a part of our continuous product development, innovation and commitment to offer the latest controls, we have come out with superior processor **DPU4F** and the same is currently being supplied to NTPC projects with good response. As a consequence of this development and due to component obsolescence, we have phased out **DPU4E** processors and withdrawn spares and services support. However, we are presently supplying and supporting the latest processor **DPU4F** with compatible **HMIs** and associated **software.**

In view of this, I strongly suggest that the processor upgrades may please be implemented for all the units of NTPC projects using DPU4E, by which we can ensure continuous availability of your plants and thereby extend the life cycle of C&I systems. In this context I would like to inform you that we have already implemented processor upgrades at NTPC- Rihand (Unit-3).

I request you to examine the above and advice all the NTPC project sites to consider for procurement of processor upgrades (**DPU4E to DPU4F)** at the earliest with the help of EDN.

You may instruct the concerned officials to interact with our Mr.G A Saravanan, AGM (Ph:080-26989241 & 09972249827, email:saravananga@bheledn.co.in) on the above subject.

With warm regards.

Yours sincerely,

09/09/15

(R.K. TIWARI)

Shri Y Venkateshwara Rao,
Executive Director (Operation Services)
National Thermal Power Corporation Ltd.,
Engineering Office Complex (EOC),
Sector 24,
Noida – 201 301.

17/15

Signature Not Verified
Digitally signed by PARIMAL PIYUSH
Date: 2024.11.26 22:55:12 IST
Reason: AGM(Commercial)
Location: NTPC Limited

ANNEXURE-R8

Date: April 18, 2023

Subject: Autrosafe Detectors Phase Out

Dear Sir/Madam,

Please note that all Autrosafe detector variants (Smoke/Heat/Multi) below are now obsolete and are no longer manufactured.

- 116-BDH-200
- 116-BDH-300
- 116-BDH-500
- 116-BHH-200
- 116-BHH-300
- 116-BHH-500
- 116-BHH-220
- 116-BHH-320
- 116-BHH-520

Our new AutroGuard protector V-430 and V-530 variants are available as replacements for the above detectors

Please do not hesitate to contact me for further clarifications.

Kind Regards,

Oussama El Khatib
Regional Sales Manager
Global Land
Tel +44 0 1784262836 | Mobile +44 0 7553229381
Oussama.elkhatib@carrier.com
www.autronicafire.com

RE: Regarding budgetary offer for Screw terminal 140xts00200 for modicon quantum

Deepak Kumar <Deepak3.Kumar@se.com>
Tue 8/6/2024 8:39 PM

To:VISHWAS <VISHWASSINGH@NTPC.CO.IN>
Cc:Suresh Kumar <SURESHKUMAR02@NTPC.CO.IN>;Alok Mandliya <ALOKMANDLIYA@NTPC.CO.IN>;Tushar Johari <Tushar.Johari@se.com>;Amit Kumar Arya <AmitKumar.Arya@non.se.com>;Renugopan Arunagiri <renugopan.arunagiri@se.com>

5 attachments (1 MB)

SESIPL PLC Spare Offer to NTPC, Tanda_R00_06-08-2024.pdf; Quantum EoC - Customer Letter_Signed.pdf; Annexure-3 End Use Statement (EUS). version Feb 2018.docx; Annexure-1 Simplified T&Cs -Supply of Equipment and Services v1.5.pdf; Annexure-2 Schneider Principles of Responsibility.pdf;

Dear Sir,

Please ignore my previous mail.
Referring to your below mail and our telephonic discussion, please find attached our techno-commercial proposal for supply of PLC spare. You are requested to release the Purchase Order to our company on below address:

Schneider Electric Systems India Private Limited (NTPC Vendor Code: 1040064)
Tamarai Tech Park, SP Plot# 16-19 and 20A,
Thiru Vi Ka Industrial Estate, Guindy,
Chennai - 600032, Tamil Nadu, India

Being OEM, we would also like to inform you that our installed Quantum PLC starting with 140CPU series has already crossed End-of Commercialization in Year 01-Dec-2018 and will reach end-of-service by 01-Dec-2026. Therefore, kindly initiate the PLC upgradation phase-by-phase before end-of-service period to avail our continued service support. As per our telephonic discussion, we are attaching our EoC Letter for your kind reference and record.

In case of any queries/clarifications, please feel free to contact the undersigned.

Thanks & Best Regards,

Deepak Kumar
General Manager - Sales
Automation Solutions & Services
Industry 4.0 I Digital Solutions

Schneider Electric Systems India Pvt. Ltd.
Mobile: 9717361325
Customer Care: 18001030011 / 18004194272
Email: deepak3.kumar@se.com

9th Floor, DLF Building No. 10
Tower C, DLF Cyber City, Ph-II
Gurgaon-122002,Haryana,India
Website: www.se.com

General

From: VISHWAS VISHWASSINGH@NTPC.CO.IN
Sent: Tuesday, August 6, 2024 4:41 PM
To: Deepak Kumar Deepak3.Kumar@se.com
Cc: Suresh Kumar SURESHKUMAR02@NTPC.CO.IN; Alok Mandliya ALOKMANDLIYA@NTPC.CO.IN
Subject: Regarding budgetary offer for Screw terminal 140xts00200 for modicon quantum

Dear Sir
Kindly provide budgetary offer for modicon quantum Screw terminal 140xts00200 for 3 quantity .

यह आपकी जानकारी और आवश्यक कार्रवाई के लिए है।
This is for your kind inf. and necessary action at your end please.
धन्यवाद/Thanks.

भवदीय/Regards

विश्वास सिंह/Vishwas Singh
प्रबंधक/Manager
एनटीपीसी टांडा सुपर थर्मल पावर स्टेशन
NTPC Tanda Super Thermal Power Station
विद्युत नगर, टांडा, उत्तर प्रदेश 224238
Vidyut Nagar, Tanda, Uttar Pradesh 224238
Mob. (मोबाइल)-7250687370/9473196703

ANNEXURE-R9

Life Is On | Schneider Electric

Schneider Electric

Subject: Modicon Quantum EoC (End of Commercialization)

Over the past 20 years, technological advancements in industrial automation have brought higher performance processors with more memory, better performance, and enhanced capabilities. In plant environments, these advancements translate to increased productivity, efficiency, security and sustainability. Schneider Electric has taken full advantage of these technological advancements to provide you with a PAC to address your needs now and into the future.

Important information about the future of Modicon range of processors

We have a great opportunity to take advantage of these new technologies, which is why we have developed the Modicon M580 ePAC. Introduced in 2013, this latest generation of Programmable Automation Controller has been designed to replace the Quantum range.

On December 1, 2018, Modicon Quantum processor has reached end of active sales.

Modicon PAC Range	End of Commercialization	End of Service
Quantum CPU (140CPU*)	December 1, 2018	December 1, 2026

We strongly recommend you take this opportunity to take a look at the Modicon M580 ePAC platform and how it helps you address your current and future needs. We also have a strong service offer to ease the modernization and ensure access to products during your planned transition period.

Modicon M580 addresses your needs now and into the future

Awarded the 2015 Engineers' Choice by Control Engineering, the Modicon M580 is one of the highest performance processors in the industry with increased power and greater connectivity. We understand the importance of having an open yet secure processor. The Modicon M580 has cyber security built into its core. Independently certified by global third-party organization to mitigate operational technology (OT) threats and vulnerabilities. The increased capabilities of the Modicon M580 help you improve operational efficiency and maintenance for the life of your control systems.

Efficient, low risk upgrades

Automation is often at the heart of the industrial process. That's why we have developed a range of tools and techniques to make it as efficient as possible for customers to upgrade from our legacy CPUs to our latest controllers. With more than 20 years of experience, we can provide you with smooth, step by step upgrade paths to our latest platforms. We have worked hard to make sure that the Modicon M580 will make the most of your existing automation investment. It minimizes the time and cost it takes to upgrade due to its compatibility with existing Quantum I/O plus software utilities available to import your existing application programs. The Modicon M580 platform is designed to continue leveraging the innovative benefits of the range to help you with your future upgrade plans.

Schneider Electric is committed to supporting your business.

Yours Sincerely,

Schneider Electric Systems India Private Limited.

Tamarai Tech Park, SP Plot # 16-19 & 20A,
Thiru Vi Ka Industrial Estate,
Inner Ring Road, Guindy,
Chennai - 600032

ANNEXURE-R10

RE: NTPC, TANDA/Regarding upgradation of ILK make pneumatic actuator with SMART Positioners in NTPC TANDA STAGE#1.

sparenorth <sparenorth@ilpgt.com>

Mon 8/12/2024 2:25 PM

To:BIKRAM KUMAR <BIKRAMKUMAR@NTPC.CO.IN>;madhu@ilpgt.com <madhu@ilpgt.com>
Cc:ARENDRA KUMAR ARYA <ARENDRAARYA@NTPC.CO.IN>;Suresh Kumar <SURESHKUMAR02@NTPC.CO.IN>

1 attachments (590 KB)
NTPC TANDA MOM.PDF;

ILP/OR-4810765/NS

Dear Sir,
Please refer the attached MOM dated 25/03/2023 regarding up-gradation of IL Make Pneumatic Actuators installed at various units of NTPC.
As per the MOM we have already executed purchase order number 4000313775 for Spares required for upgrading of FD/PA IGV Fan IGV, ID Fan Scoop and Fuel Oil control Valves for UNIT # 2.
Since the existing Actuators and Positioners Mounted are of Obsolete Model, it is suggested to upgrade the Actuators of the balance 3 units also.

With Regards सादर,

MADHU मधु

Sr.Engineer (Commercial) वरिष्ठ अभियंता (वाणिज्य)

Instrumentation Limited इंस्ट्रुमेंटेशन लिमिटेड
PALAKKAD - 678623 (Kerala)पालक्काड
PIN CODE- 678623 (केरल)
PH: 0491-2566844
Mob:9496946766/8921602300
E Mail: sparenorth@ilpgt.com
GeM Seller ID विक्रेता आईडी - E5FF20001308318
For Complaints visit - सेवा शिकायतों के लिए कृपया देखें https://www.ilpgt.com/html/complaints.php
IL's official Youtube channel https://youtube.com/channel/UCTyfGXgaIO0eD2GvDnqLfQQ
IL's official Twitter handle https://twitter.com/limited_unit?t=LPGTT-gz1ov1yJ26FCKI2g&s=03

From: BIKRAM KUMAR [mailto:BIKRAMKUMAR@NTPC.CO.IN]
Sent: 03 February 2023 09:05
To: sparenorth@ilpgt.com; madhu@ilpgt.com
Cc: ARENDRA KUMAR ARYA; Suresh Kumar
Subject: Regarding upgradation of ILK make pneumatic actuator with SMART Positioners in NTPC TANDA STAGE#1.

Sir,

ANNEXURE-R11

Basic Information Regarding Cast basalt

Basalt is basically a volcanic rock that possesses perfect characteristics including resistance to abrasion as well as corrosion.

The process of **basalt casting** starts with discerning quarrying of the rock. It is then melted at 1280°C and then casted in the form of moulds and cylinders. The **basalt castings** that are produced are then exposed to a cycle of heat treatment. They are placed in kilns for the production of basalt in a re-crystallized form. The product contains various **cast basalt properties** like inertness in it. This inertness is inherited from the parent material. It is homogenous, non porous and denser as compared to the raw form. Amazing qualities of abrasion resistance are acquired by the processed form of basalt after going through the process of **basalt casting**.

Basalt casts are considered the best lining materials for industries dealing with abrasion resistance. The other application areas of **basalt casts** are bends, lining pipers and trenches.

Application Areas of Basalt Casting

- Because of the specialized **cast basalt properties**, they can be used in thermal power stations for the manufacture of hoppers, bottom ash, bends, pipelines, trenches, coal piping, dust lines, disposal slurries etc.
- **Cast basalt** is also used in cement plants for making air separators, chain conveyor, silica hoppers, nozzles, coal hoppers, cement hoppers, cyclones, raw mill ducts, chutes, thick slurry lines, mixers, grate cooler housing, coal ventury etc.
- Steel plants also make exceptional use of **basalt casting** materials. They use if for making lime bunkers, coke breeze, telescopic pipers, cyclones, sieves, floatation cells, coke sorting units, sinter plant cyclones, iron slurry line, granulated slag, thick slurry lines, hot mill flume, flow conveyors etc.
- Furthermore, coal washeries make effective use of **cast basalt** for the manufacture of media sumps, coal transportation, coal washing plans, cyclones, conveyor pipes, floatation cells, centrifuges etc.

Cast Basalt Properties

- **Cast basalt** is resistant to abrasion.
- It is resistant to many chemicals.
- **Cast basalt** can be easily cast in various shapes including flat, hexagonal and radial tiles or cylinders. They can also be made up into special castings and different circular pipelines can be made of it.

Some Technical Properties of Cast Basalt

- **Cast basalt** gets polished up when more material is passed over it. This reduces friction in it and improves the service that it renders.
- **Cast basalt** is considered the best for abrasion. A basalt pipe has a stronger strength as compared with that of a bare pipe. Its external effect of strength is higher than the raw form.
- Another important feature of cast basalt is that it is resistant to chemicals including alkalis and acids. As it is resistant to chemicals; therefore, it is resistant to corrosion as well.
- **Cast basalt** tiles can be easily found in a regular size of 200x200x30 mm. The weight of a regular shaped cast basalt tile is 78 kg/sq m. The pipes and bends that contain lining of cast basalt possess a size of 40-1100 NB.
- The maximum temperature that can be withstood by cast basalt is 450°C.
- The life span of an average pipe made up of cast basalt lining is more as compared with that of cast iron. It is 3-4 times more than the wear of cast iron.

Cast basalt is a durable, resistant, and reliable and widely used manufacturing material being used in variant construction projects and industries. The linings made from cast basalt are strong and have long lasting effects. This is why most of the industries prefer using cast basalt linings in most of their manufacturing operations.

EUTIT s. r. o., Basalt and eucor casting plant, č.p. 196, 353 01 Stará Voda
Tel.: +420 354 789 111, +420 354 391 301, Fax: +420 354 691 480
e-mail: eutit@eutit.cz, www.eutit.cz</

ANNEXURE-R12

CONDITION ASSESSMENT STUDY OF CONCRETE STRUCTURES OF NTPC TANDA

FOR

NTPC TANDA, UTTAR PRADESH

REPORT OF CLARIFLOCATORS-1, 2
CDR/SP-6325
APRIL 2024

Centre for Construction Development and Research
NATIONAL COUNCIL FOR CEMENT AND BUILDING MATERIALS
Old Bombay Road, Near Raidurgh Police Station, Hyderabad-500104

Prepared By	A. Bharath	for Charath
Checked By	Adarsh Kumar N.S	Charath
Approved By	B S Rao	25/04/24

Electronic File Ref:	Report No. NCB/CDR/	No. of Pages/Appendices
CDR-2/F:/Report/SP-6325		

1.0 INTRODUCTION

NTPC Tanda, Uttar Pradesh approached National Council for Cement and Building Materials (NCB). To carry out condition assessment study of Clariflocators-1, 2 using Non Destructive Evaluation Technique including preparation of Quantities (BOQ), Cost Estimation for repair and restoration at NTPC Tanda. NCB took up the work as per PO No: 4000269971-026-1035 Dated 31.12.2021

Scope of works

a) To carry out condition assessment using Non Destructive Evaluation Technique including repair methodology, preparation of quantities (BOQ), Cost estimate of Clariflocators-1, 2 at NTPC Tanda, Uttar Pradesh.

i) Visual observations of Clariflocators-1, 2: To collect data of distress on RCC members of Clariflocators shall be carried out up to safely accessible heights which were made accessible for testing. Visual observation data will be supplemented by photographs and other pertinent information wherever available.

ii) To conduct experimental investigation by Non Destructive Testing technique on the selected representative RCC members at different locations of the Clariflocators-1,2 -

a. Quality assessment of selected RCC members using Rebound Hammer testing technique as per IS 516 (Part 5/Sec 4):2020
b. Quality assessment of selected RCC members using Ultrasonic Pulse Velocity testing technique as per IS: IS: 516 (Part V) – 2019
c. Determination of equivalent cube compressive strength of concrete in RCC structure using concrete core extraction & testing technique as per IS: 456-2000 & IS: 516-1959.
d. Assessment of Carbonation depth of the extracted concrete cores.
e. Determine the corrosion status of reinforcement steel using Half-cell potential survey as per IS: 516 (PART 5, SECTION 2) – 2021 on few selected safely accessible RCC Members.
f. Determination of concrete cover thickness in RCC members using Ferro scanning technique at identified & safely accessible location.

g. Chemical Analysis to determine Chloride content, Sulphate content and pH value of Concrete Powder Samples in laboratory.

iii) Analysis and interpretation of test results/data obtained in (i) & (ii) above.

iv) Recommendations on remedial measures using indigenously available compatible repair materials. Preparation of BOQ covering selected items for repair including rate analysis & preparation of specifications and methodology for carrying out effective repair shall also be provided.

v) The report covering (i) to (iv) above.

2.0 DATA PROVIDED BY SPONSOR

- Year of Construction of the subject structure was around 1990

3.0 INVESTIGATION CARRIED OUT BY NCB

To collect the data of distress on RCC members of Clariflocators at **NTPC, TANDA, Uttar Pradesh,** and Visual observation survey was carried out jointly by NCB team and the concerned NTPC officials during the visits for condition assessment from 06th September to 10th September 2022.

3.1 Rebound Hammer Testing (RHT) As Per IS 516 (Part 5/Sec 4):2020

Rebound hammer testing technique was used for assessing the likely surface compressive strength of concrete. Basic principle of rebound hammer test is given below.

When the plunger of rebound hammer is pressed against the surface of the concrete, the spring-controlled mass rebounds and the extent of such rebound depends upon the surface hardness of concrete. The surface hardness and therefore the rebound are taken to be related to the compressive strength of the concrete. The rebound is read off along a graduated scale and is designated as the rebound number or rebound index. It is also to be noted that rebound indices are indicative of compressive strength of concrete to a limited depth from the surface. If the concrete in a particular member has internal micro cracking, flaws or heterogeneity across the cross-section, rebound hammer indices will not indicate the same. **IS: 516 (Part 5/Sec 4): 2020 states,** "*As such, the estimation of strength of concrete by rebound hammer method cannot be held to be very accurate and probable accuracy of prediction of concrete strength in a structure is ±25 percent*." However, the test should only be used as indication of the probable compressive strength of concrete.

The test was carried out using a Schmidt's Rebound Hammer on randomly selected accessible Mill foundations at **NTPC Tanda, Uttar Pradesh.** The members which were tested were made accessible. So the testing done on accessible members represents other members also. The surfaces at the chosen locations were thoroughly cleaned with carborandum stone/grinding stone and readings were taken around each point. The average of the readings becomes the rebound index at that point of observation.

3.2 Ultrasonic Pulse Velocity (UPV) Method As per IS: 516 (Part V) – 2018.

UPV is a non-destructive evaluation method for assessing the quality of concrete; density, homogeneity and uniformity. Basic principle of UPV method is given below.

In this method, an ultrasonic pulse of longitudinal vibrations is produced by an electro-acoustical transducer which is held in contact with one surface of the concrete member under test. After traversing a known path length of the member, the pulse of vibrations is converted into an electric signal by a second electro-acoustical transducer, and an electric timing circuit enables the transit time of the pulse to be measured, from which the pulse velocity is calculated. For the present investigation, the pulse velocity measurements were obtained by direct transmission of ultrasonic pulses through the concrete, i.e. by "cross probing" & "Surface probing". For this purpose, the transducers were held on opposite faces of the beam and columns.

The Ultrasonic Pulse Velocity in concrete is mainly related to its density and modulus of elasticity. This in turn depends upon the materials and mix proportions used in making concrete as well as methods of placing, compaction and curing of concrete. If the concrete is not thoroughly compacted, or if there is segregation of concrete during placing or there are internal cracks or flaws, the pulse velocity will be lower, although the same materials and mix proportions are used.

The underlying principle of assessing the quality of concrete from UPV method is that, comparatively higher pulse velocities are obtained when the 'quality' of concrete in terms of density, homogeneity and uniformity is good. In case of concrete of poorer quality, lower velocities are obtained.

On this basis, guidelines have been evolved for characterizing the quality of concrete in structures in terms of ultrasonic pulse velocity. Such guideline reproduced from IS**: 516 (Part V) – 2018.**

3.3 Concrete Core Testing

Concrete cores of 60-mm diameter were extracted from different structural members identified, to estimate equivalent cube compressive strength of the structure. Equivalent cube strength does not indicate 28 days' standard cube strength rather it represents the in-situ cube strength, and is compared vis-à-vis strength used in design calculation with safety of the structure under load in mind.

There are a number of parameters, which influence the measured compressive strengths. Such parameters include size (diameter) of the specimen, length-to-diameter ratio, direction of drilling, method of capping, drilling operations, moisture conditions of cores at the time of testing etc. Many of these parameters have been standardized.

The second set of variables relates to the intrinsic difference that exists between the concrete in structure and in standard laboratory controlled specimens, the core specimens representing the former. Such intrinsic differences are due to inherent differences that may occur in mixing constituents, degree of compaction, extent of curing and temperature condition in two cases. The procedure for sampling, preparing, testing and calculating the equivalent compressive strength with corrections are given in **IS: 516-2018.**

The net effect of all these parameters is that the strength of concrete cores is in general lower than those of laboratory controlled specimens, for this reason **IS: 456-2000** (Code of Practice for Plain and Reinforced Concrete)consider that concrete in the area represented by a core test is adequate if" *the average equivalent cube strength of the cores is equal to at least 85 percent of the specified for the corresponding age and if no single core has strength lower than 75 percent of the specified value".*

3.4 Carbonation Test

Carbonation is the formation of calcium carbonate ($CaCO_3$) by chemical reactions in concrete. When CO_2penetrates into the hardened concrete, it reacts with portlandite [Portlandite is a mineral formed during the curing of concrete, calcium hydroxide Ca $(OH)_2$] in the presence of moisture forming $CaCO_3$. The rate of carbonation depends mainly on the relative humidity, the concentration of CO_2, the penetration pressure and the temperature of the environment where concrete is placed.

As carbon dioxide enters the concrete from the environment, it reacts with calcium hydroxide present in the concrete and depending upon the quality of concrete it reduces the

alkalinity of the pore fluids, depassivating ferric oxide layer on reinforcing bar which in turn initiates the process of corrosion in reinforcement.

To determine the depth of carbonation, concrete is exposed and sprayed with a pH indicator (solutions of 1%phenolphthalein in 70% ethyl alcohol). The demarcation between the region, which turns into magenta (dark pink colour) and the region showing no change in colour indicate the carbonation front.

Carbonation measurements were recorded immediately after the cores specified in col. 3.4 were extracted.

3.5 Half-Cell Potential (HCP) Measurements

This test method covers the estimation of electrical Half Cell Potential of uncoated reinforcing steel, to determine corrosion activity using reference electrode copper; copper sulphate half-cell. It is not possible to expose all the reinforcements in the structural element and observe the extent of corrosion. So, this method has been very convenient to assess the condition of the entire length of a member by exposing a portion of the reinforcement at a suitable location, which measures the half-cell potential on the entire length, by placing the reference electrode on the wet concrete surface.

The Half-Cell Potential measurement is based on the principal of the corrosion, being an electro-chemical process, induces certain voltage to the reinforcement steel that is corroding. The wetting of the concrete is required to make the portion between the concrete surface and the reinforcing bar as electrolytes.

A criterion for assessment for corrosion of steel is given as under **IS: 516 (Part 5, Section 2)-2021** below.

- If potentials over an area are more positive than -200 mV, there is a greater than 90% probability that no reinforcing steel corrosion is occurring in that area at the time of measurement.
- If potentials over an area are in the range of -200 mV to -350 mV, corrosion activity of the reinforcing steel in that area is uncertain.
- If potentials over an area are more negative than -350 mV, there is a greater than 90% probability that reinforcing steel corrosion is occurring in that area at the time of measurement.

Adequate numbers of accessible RCC members were selected from various locations to conduct Half-Cell Potential test.

3.6 Concrete Cover Study

Concrete cover depth to reinforcing bars shall be done by using Ferro Scanner instrument on safe & accessible locations. This instrument detects the reinforcing bars and mesh, to measure their cover depth and determine the bar diameter. The instrument is based on the magnetic technique and is calibrated for different purposes. The cover depth is important from the point of view of estimation of initiation of corrosion of reinforcing bars.

For a longitudinal reinforcing bar in a Column nominal cover shall in any case not be less than 40mm or less than the diameter of such bar as per clause 26.4.2.1 of IS: 456-2000. Nominal cover to meet durability requirement for footing, minimum cover shall be 50mm as per clause 26.4.2.2 of IS: 456-2000.

Minimum values of nominal cover of normal weight aggregate concrete to be provided to all reinforcement including links to meet specified period of fire resistance shall be as per Table 16A of IS:456-2000.

Minimum values for the nominal cover of normal weight aggregate concrete which should be provided all reinforcement including links depending of exposure condition shall be as per the Table 5 of IS: 456-2000.

3.7 Chemical Analysis

Corrosion of reinforcing steel due to chlorides in concrete is one of the most common environmental attacks that lead to deterioration of concrete structures. Whenever there is chloride in concrete there is an increased risk of corrosion of embedded metal. Chloride content is then expressed in kg per cubic meter of concrete and compared with the values of limits of chloride contents of concrete (**Table 7 of IS: 456–2000**).

Sulphates (SO_3) are present in most cements and in some aggregates; excessive amounts of water-soluble sulphate from these or other mix constituents can cause expansion and disruption of concrete. To prevent it, **IS: 456-2000 clause-8.2.5.3** states that the total water-soluble sulphate content of the concrete mix, expressed as SO_3, should not exceed 4 percent by mass of the cement in the mix. The sulphate content should be calculated as the total from the various constituents of the mix.

The pH value of the concrete should be above 11.5 to maintain alkalinity of concrete surrounding the embedded steel. A reduction in the pH value of concrete indicates loss of passive layer around the reinforcement which protects the steel from distress.

For analyzing Chloride content and pH of concrete, concrete powder samples were extracted from 0-25mm, 25-50mm depths at identified locations and then tested as per IS:14959(Part 2) -2001 (Determination of water soluble and acid soluble Chlorides in Mortar and Concrete – Method of Test).

Adequate numbers of accessible RCC members were selected from various locations to extract concrete powders for chemical test.

4.0 RESULTS AND DISCUSSION

4.1. Visual Observations

Visual observations and testing carried out at Different levels of Clariflocators. Distress was found in the form of cracks, Honeycombs and Seepage of Water through concrete surface. Colour deterioration, spalling of Concrete was noticed at few locations of Clariflocators. The visual observations and photographs are shown in Annexure I.

4.2. Rebound Hammer Testing:

Rebound Hammer testing was carried out on various identified RCC (Reinforced Cement Concrete) members of Clariflocators-1, 2 using random sampling technique the results of surface compressive strength obtained by Rebound Hammer testing are given in Table 2 to 17.

Surface Compressive strength results of concrete as obtained on different hardened concrete surfaces of RCC Members are summarized as:

1) Surface compressive strength of concrete obtained Clariflocator-1 East side wall by Rebound Hammer Testing is found with an average surface compressive strength of **31.75 N/mm^2** (Refer Table 2).
2) Surface compressive strength of concrete obtained on Clariflocator-1 West side wall by Rebound Hammer Testing is found with an average surface compressive strength of **34.80 N/mm^2** (Refer Table 3).

3) Surface compressive strength of concrete obtained on Clariflocator-1 South side wall by Rebound Hammer Testing is found with an average surface compressive strength **34.16 N/mm^2** (Refer Table 4).

4) Surface compressive strength of concrete obtained on Clariflocator-1 North side wall by Rebound Hammer Testing is found with an average surface compressive strength of **33.95 N/mm^2** (Refer Table 5).

5) Surface compressive strength of concrete obtained on Clariflocator-1 North East side wall by Rebound Hammer Testing is found with an average surface compressive strength of **36.07 N/mm^2** (Refer Table 6).

6) Surface compressive strength of concrete obtained on Clariflocator-1 South West side wall by Rebound Hammer Testing is found with an average surface compressive strength of **33.66 N/mm^2** (Refer Table 7).

7) Surface compressive strength of concrete obtained on Clariflocator-1 North West side wall by Rebound Hammer Testing is found with an average surface compressive strength of **31.97 N/mm^2** (Refer Table 8).

8) Surface compressive strength of concrete obtained on Clariflocator-1 North West side wall by Rebound Hammer Testing is found with an average surface compressive strength of **35.64 N/mm^2** (Refer Table 9).

9) Surface compressive strength of concrete obtained on Clariflocator-2 North side wall by Rebound Hammer Testing is found with an average surface compressive strength of **32.81 N/mm^2** (Refer Table 10).

10) Surface compressive strength of concrete obtained on Clariflocator-2 South side wall by Rebound Hammer Testing is found with an average surface compressive strength of **33.10 N/mm^2** (Refer Table 11).

11) Surface compressive strength of concrete obtained on Clariflocator-2 East side wall by Rebound Hammer Testing is found with an average surface compressive strength of **33.73 N/mm^2** (Refer Table 12).

12) Surface compressive strength of concrete obtained on Clariflocator-2 West side wall by Rebound Hammer Testing is found with an average surface compressive strength of **32.74 N/mm^2** (Refer Table 13).

13) Surface compressive strength of concrete obtained on Clariflocator-2 North East side wall by Rebound Hammer Testing is found with an average surface compressive strength of **33.03 N/mm^2** (Refer Table 14).

14) Surface compressive strength of concrete obtained on Clariflocator-2 South West side wall by Rebound Hammer Testing is found with an average surface compressive strength of **32.96 N/mm^2** (Refer Table 15).

15) Surface compressive strength of concrete obtained on Clariflocator-2 North West side wall by Rebound Hammer Testing is found with an average surface compressive strength of **33.66 N/mm^2** (Refer Table 16).

16) Surface compressive strength of concrete obtained on Clariflocator-2 North West side wall by Rebound Hammer Testing is found with an average surface compressive strength of **34.09 N/mm^2** (Refer Table 17).

4.3 Ultrasonic Pulse Velocity Testing (UPV):

The Ultrasonic Pulse Velocity testing was conducted on Clariflocators for #1, 2 in the presence of concerned engineering team of NTPC Tanda. The results of the UPV values obtained on various RCC members are as follows:

1) The UPV measurements were taken using Surface probing technique on the Clariflocator-1 East side wall are in the range of **3.77 to 4.6 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018(Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table -19).
2) The UPV measurements were taken using Cross probing technique on the Clariflocator-1 West side wall are in the range of **3.62 to 4.09 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 20).
3) The UPV measurements were taken using Cross probing technique on the Clariflocator-1 South side wall are in the range of **3.64 to 4.27 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 21).
4) The UPV measurements were taken using Cross probing technique on the Clariflocator-1 North side wall are in the range of **3.58 to 4.13 km/sec**. When these values are

compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 22).

5) The UPV measurements were taken using Cross probing technique on the Clariflocator-1 North East side wall are in the range of **3.56 to 4.08 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 23).
6) The UPV measurements were taken using Surface probing technique on the Clariflocator-1 South West side wall are in the range of **3.54 to 3.98 km/sec**. When these values are compared with the velocity criteria of IS:516 (Part V)–2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 24).
7) The UPV measurements were taken using Surface probing technique on the Clariflocator-1 North West side wall are in the range of **3.55 to 3.98 km/sec**. When these values are compared with the velocity criteria of IS:516 (Part V)–2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 25).
8) The UPV measurements were taken using Surface probing technique on the Clariflocator-1 North West side wall are in the range of **3.51 to 3.88 km/sec**. When these values are compared with the velocity criteria of IS:516 (Part V)–2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 26).
9) The UPV measurements were taken using Surface probing technique on the Clariflocator-2 North side wall are in the range of **3.98 to 4.66km/sec**. When these values are compared with the velocity criteria of IS:516 (Part V)–2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 27).
10) The UPV measurements were taken using Cross probing technique on the Clariflocator-2 North side wall are in the range of **3.61 to 4.19 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 28).
11) The UPV measurements were taken using Cross probing technique on the Clariflocator-2 East side wall are in the range of **3.59 to 4.08 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 29).

12) The UPV measurements were taken using Cross probing technique on the Clariflocator-2 West side wall are in the range of **3.64 to 4.02 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 30).

13) The UPV measurements were taken using Cross probing technique on the Clariflocator-2 North East side wall are in the range of **3.73 to 4.08 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 31).

14) The UPV measurements were taken using Surface probing technique on the Clariflocator-2 South West side wall are in the range of **4.06 to 4.41 km/sec**. When these values are compared with the velocity criteria of IS:516 (Part V)–2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 32).

15) The UPV measurements were taken using Surface probing technique on the Clariflocator-2 North West side wall are in the range of **3.86 to 4.26 km/sec**. When these values are compared with the velocity criteria of IS:516 (Part V)–2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 33).

16) The UPV measurements were taken using Surface probing technique on the Clariflocator-2 North West side wall are in the range of **3.89 to 4.22 km/sec**. When these values are compared with the velocity criteria of IS: 516(Part V) – 2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 34).

4.4 Concrete Core Testing:

Corresponding to the 60mm concrete core extracted by random sampling technique covering different locations of Clariflocators- 1, 2 in power plant of NTPC Tanda and tested at NCCBM laboratory Hyderabad, the equivalent cube compressive strength of concrete RCC members are shown in Tables- 40, 41. In total, 28 nos. of concrete cores were extracted from different members of the Clariflocators all are found to be testable either due to short length of the cores.

The test results indicate that the equivalent cube compressive strength values for

Clariflocator-1

1. Clariflocator-1 East side wall is found to be **48.30 N/mm²**
2. Clariflocator-1 West side wall is found to be **64.63 N/mm2**
3. Clariflocator-1 South side wall is found to be **31.00 N/mm2**
4. Clariflocator-1 North side wall is found to be **47.00 N/mm2**
5. Clariflocator-1 North East side wall is found to be **33.41 N/mm2**
6. Clariflocator-1 South West side wall is found to be **39.13 N/mm2**
7. Clariflocator-1 North West side wall is found to be **33.26 N/mm2**
8. Clariflocator-1 North West side wall is found to be **36.80 N/mm2**

Clariflocator-2

1. Clariflocator-2 North side wall is found to be **35.49 N/mm2**
2. Clariflocator-2 South side wall is found to be **31.93 N/mm2**
3. Clariflocator-2 East side wall is found to be **25.53 N/mm2**
4. Clariflocator-2 West side wall is found to be **34.32 N/mm2**
5. Clariflocator-2 North East side wall is found to be **37.92 N/mm2**
6. Clariflocator-2 South West side wall is found to be **35.34 N/mm2**
7. Clariflocator-2 North West side wall is found to be **36.34 N/mm2**
8. Clariflocator-2 North West side wall is found to be **32.87 N/mm2**

In total, 16 nos tested cores all of them found to have equivalent cube compressive strength more than specified characteristic compressive strength of M25 grade concrete (which is produced in Table- 40,41).

4.5 Concrete Cover :

The concrete cover depth to rebars in RCC members is measured with Ferro-scanner and a measuring tape/scale in the places where concrete is exposed and accessible for direct measurement. Nominal cover to reinforcement to meet durability requirement is given in **IS-456: Table 16-clause 26.4.2** (Also reproduced in Table-35), the measured cover to reinforcement steel in the selected RCC members are given in Table 36,37**.**

Clariflocator-1

1. The Concrete cover to Reinforcing bars of Clariflocator-1 East side wall during testing using Ferro scanner meter is found with an average of **50 mm.**

2. The Concrete cover to Reinforcing bars of Clariflocator-1 West side wall during testing using Ferro scanner meter is found with an average of **54 mm.**
3. The Concrete cover to Reinforcing bars of Clariflocator-1 South side wall during testing using Ferro scanner meter is found with an average of **57 mm.**
4. The Concrete cover to Reinforcing bars of Clariflocator-1 North side wall during testing using Ferro scanner meter is found with an average of **56 mm.**
5. The Concrete cover to Reinforcing bars of Clariflocator-1 North East side wall during testing using Ferro scanner meter is found with an average of **52 mm.**
6. The Concrete cover to Reinforcing bars of Clariflocator-1 South West side wall during testing using Ferro scanner meter is found with an average of **53 mm.**
7. The Concrete cover to Reinforcing bars of Clariflocator-1 North West side wall during testing using Ferro scanner meter is found with an average of **57 mm.**
8. The Concrete cover to Reinforcing bars of Clariflocator-1 North West side wall during testing using Ferro scanner meter is found with an average of **54 mm.**

Clariflocator-2

1. The Concrete cover to Reinforcing bars of Clariflocator-2 North side wall during testing using Ferro scanner meter is found with an average of **51 mm.**
2. The Concrete cover to Reinforcing bars of Clariflocator-2 South side wall during testing using Ferro scanner meter is found with an average of **52 mm.**
3. The Concrete cover to Reinforcing bars of Clariflocator-2 East side wall during testing using Ferro scanner meter is found with an average of **58 mm.**
4. The Concrete cover to Reinforcing bars of Clariflocator-2 West side wall during testing using Ferro scanner meter is found with an average of **57 mm.**
5. The Concrete cover to Reinforcing bars of Clariflocator-2 North East side wall during testing using Ferro scanner meter is found with an average of **52 mm.**
6. The Concrete cover to Reinforcing bars of Clariflocator-2 South West side wall during testing using Ferro scanner meter is found with an average of **55 mm.**
7. The Concrete cover to Reinforcing bars of Clariflocator-2 North West side wall during testing using Ferro scanner meter is found with an average of **54 mm.**
8. The Concrete cover to Reinforcing bars of Clariflocator-2 North West side wall during testing using Ferro scanner meter is found with an average of **55 mm.**

The Concrete cover within the specified limits to meet durability requirement as per IS: 456-2000 (Refer Table 16 of IS: 456-2000) which is Reproduced in Table 35.

4.6 Carbonation:

Table-38,39 shows test results of carbonation testing done on 16 nos. of Concrete Cores extracted from various representative concrete samples. The results indicate that the values of depth of carbonation in all different locations of Clariflocators-1, 2 are found to be **0-8**mm, on RCC members.

Based on the above carbonation study carried on different selected RCC members at several locations the carbonation depth is found to be within the concrete cover region.

4.7 Half-Cell Potential Test :

Half-cell potential (HCP) measurements using copper, copper-sulfate half-cell technique as per IS: 516 (Part 5, Section 2)-2021 (Standard test method for corrosion potentials of uncoated reinforcing steel in concrete) were taken at site to ascertain corrosion status of reinforcing bars of various locations of Clariflocators-1, 2 at NTPC TANDA. The measurements were done on different locations randomly selected locations and comprising of representative samples of for the structure.

Test results (refer Table- 43,44) when compared with the corrosion criteria as per ASTM C-876 (Table-42) indicate that probability of corrosion is found to be in “90% Possibility of no corrosion”.

4.8 Chemical Analysis :

The chemical analysis of water and powdered samples extracted from different elements of Clariflocators-1, 2 collecting by random sampling technique. This covered chloride content, sulphate content per cum of concrete as well pH value of powdered samples. The test results as obtained in NCCBM laboratory are shown in Table- 45,46. Analysis of interpretation of test results given as under:

1) Based on the results obtained from laboratory the range of chloride content in the Clariflocators-1 East side wall was found with an average value of **0.09 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3)

content by mass of the cement in mix with an average value of **1.57%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.3** which is within the specified limit to resist the corrosion.

2) Based on the results obtained from laboratory the range of chloride content in the Clariflocators-1 West side wall was found with an average value of **0.13 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.58%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.46** which is within the specified limit specified limit to resist the corrosion.

3) Based on the results obtained from laboratory the range of chloride content in the Clariflocators-1 South side wall was found with an average value of **0.16 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.44%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.52** which is within the specified limit to resist the corrosion.

4) Based on the results obtained from laboratory the range of chloride content in the Clariflocators-1 North side wall was found with an average value of **0.14 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.5%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.54** which is within the specified limit to resist the corrosion.

5) Based on the results obtained from laboratory the range of chloride content in the Clariflocators-1 North East side wall was found with an average value of **0.18 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.5%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of

pH value is found with an average of **11.55** is within the specified limit to resist the corrosion.

6) Based on the results obtained from laboratory the range of chloride content in the Clariflocators-2 North side wall was found with an average value of **0.13 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.62%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.35** which is within the specified limit to resist the corrosion.

7) Based on the results obtained from laboratory the range of chloride content in the Clariflocators-2 South side wall was found with an average value of **0.15 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.58%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.48** which is within the specified limit to resist the corrosion.

8) Based on the results obtained from laboratory the range of chloride content in the Clariflocators-2 East side wall was found with an average value of **0.16 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.44%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.57** is within the specified limit to resist the corrosion.

9) Based on the results obtained from laboratory the range of chloride content in the Clariflocators-2 West side wall was found with an average value of **0.15 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.5%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.58** which is within the specified limit to resist the corrosion.

10) Based on the results obtained from laboratory the range of chloride content in the Clariflocators-2 North East side wall was found with an average value of **0.17 kg/m^3** is

within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.47%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.57** which is within the specified limit to resist the corrosion.

5.0 Conclusions:

The following Conclusions can be broadly made from the testing results Clariflocators-,1,2:

i) Based on visual observations carried out in the Clariflocators-,1,2 locations Distress was found in the form of cracks, Honey combs and Seepage of Water on concrete surface. Colour deterioration, Peeling of Concrete was developing at few locations.

ii) Based on Rebound hammer test surface hardness and likely compressive strength found satisfactory and meeting the required limits as per data furnished by the client.

iii) Based on Ultrasonic Pulse Velocity (random sampling technique) to find quality and homogeneity of concrete on RCC members, the results were found to be good quality of concrete.

iv) The equivalent cube compressive strength of the core samples extracted from the Clariflocators-1, 2 is found meeting more than the required limit for M25 Grade of concrete.

v) Carbonation is found 0-8mm after 30 years 'whereas concrete cover of RCC members is found to vary from 51 – 58 mm and found within the limits of concrete cover region.

vi) Based on the Half-Cell potential measurements done by random sampling technique at various locations and visual observations of Clariflocators-1, 2 given an initiation signal of either in "90% Possibility of no corrosion".

vii) The amount of Acid soluble chloride content and soluble sulphates in the concrete of Clariflocators-1, 2 is within the specified limits for all the samples and pH values for few of tested samples slightly less than 11.5 as per (IS: 456-2000& IS: 3025 -1984).

6.0 Recommendations

The following steps shall be taken to repair the cracks & strengthening of Clariflocators-1, 2 :

i) Chipping:

Cover concrete around the horizontal, vertical cracks & spalling of concrete shall be chipped off to the depth up to 40mm on RCC walls. The chipping in the spalled portion of the Shells and RCC Walls shall be limited up to the cover region. Chipping of loose/hollow sounding concrete can be done by striking the doubtful surfaces with 2 lb. hammer.

ii) Treatment for Cracks:

a. The cracks are to be widened by cutting V-grooves of 10mm x 10mm size and sealed with approved epoxy repair mortar.

b. After the sealing, 12mm dia galvanized steel injection nipples are to be inserted in the crack area and also wherever honeycombing is found by drilling holes of required diameter up to the depth of 30 – 80 mm at required spacing (generally 350 mm staggered spacing). The drilled holes must be made dust free by blowing compressed air and should be sealed after the insertion of the nozzle with approved adhesive and allowed to cure.

c. After the nipples are injected and cured, grouting in the proportion recommended by the manufacturer into the cracks/honeycombed area of concrete/masonry shall be done using suitable gun/pump at required pressure. Once the grouting work is finished, the extruding nipples can be cut-off after the curing period.

iii) Reinforcement Corrosion Treatment:

Wherever reinforcing rebar is found corroded in RCC walls

a) Remove the rust by manually or suitable means to make corroded reinforcing bars rust free.

b) Provide and apply corrosion protection using 2 coats of anticorrosive Zn rich epoxy phenolic rebar protection system of approved brand on the exposed old reinforcement by brush with interval of 24 hours between coats and corrosion protection of exposed old reinforcing bars.

c) Provide and apply concrete penetrating corrosion inhibitor (CPCI) of approved brand over the entire finished surface are obtained after removal of distressed concrete in 2 coats @ of $4m^2$/ltr/coat approximately.

iv) Bond Coat:

After chipping off the concrete cover, provide and apply structural grade two component epoxy bond coat prior to application of any type of mortar conforming to ASTM C - 881 -13 Type - II tested as per ASTM C –882-13 to ensure bond between old and new concrete by brush application. (Material manufacture from SYNORGANIC /BASF/SIKA/FOSRAC/KRISHNA Conchem/Pidilite or equivalent)

v) Making up lost section with Polymer Modified Mortar (PMM):

For repair of patches having, apply average 40mm PMM in 2-3 layers using SBR Latex conforming to ASTM C-1059-13 Type-I in damaged areas (1 Cement-3 part graded cleaned river sand + 20 % latex by weight of cement) with 0.35 w/c ratio, in 10-15 mm thick layers by applying bond coat between successive/each. (Material manufacture either from SYNORGANIC/BASF/SIKA/FOSRAC or equivalent)

vi) Protective coating:

Before applying the protective coating on RCC walls and the outer wall surface shall be cleaned by scrubbing with hard steel brush to remove loose particles, disintegrated concrete, deposited smoke and dust particles etc. The scrubbed surface is cleaned by air blowing and then dries it completely. Apply min. 2 coats of two part high performance moisture compatible corrosion resistant coating material (base and curing agent) of approved manufacturer over prepared surface, using not less than theoretical consumption as per the manufacturer's specification. Total dry film thickness (DFT) including primer will be 300 - 400 microns.

Note:

1. Before taking up any repair work, the dryness of substrate concrete must be ensured for effective application of several repair materials. Remove oil, grease, wax, Cement laitance, loose particles and other contaminants by shot blasting, scarifying or mechanically wire brushing followed by vacuum cleaning from the substrate concrete.
2. During repair works of Clariflocators-1,2 measures should be taken up in accordance with relevant safety standards and safety guidelines of Occupational safety & Health Administration (OSHA) for construction, arrangement like safety nets/platforms should be done.

.....

CONDITION ASSESSMENT STUDY OF CONCRETE STRUCTURES OF NTPC TANDA

FOR

NTPC TANDA, UTTAR PRADESH

FINAL REPORT OF MILL FOUNDATION
CDR/SP-6325
FEBRUARY 2024

Centre for Construction Development and Research
NATIONAL COUNCIL FOR CEMENT AND BUILDING MATERIALS
Old Bombay Road, Near Raidurgh Police Station, Hyderabad-500104

Prepared By	**A. Bharath**	A. Bharath (Signature)
Checked By	**Adarsh Kumar N.S**	(Signature)
Approved By	**B S Rao**	(Signature)

Electronic File Ref:	**Report No. NCB/CDR/**	**No. of Pages/Appendices**
CDR-2/F:/Report/SP-6325		

1.0 INTRODUCTION

Scope of works

a) To carry out condition assessment using Non Destructive Evaluation Technique including repair methodology, preparation of quantities (BOQ), Cost estimate of Mill foundations for units #1, 2, 3 & 4 at NTPC Tanda, Uttar Pradesh.

i) Visual observations of Mill foundations for units #1, 2, 3 & 4: To collect data of distress on RCC members of Mill foundations shall be carried out up to safely accessible heights which were made accessible for testing. Visual observation data will be supplemented by photographs and other pertinent information wherever available.

ii) To conduct experimental investigation by Non Destructive Testing technique on the selected representative RCC members at different locations of the RCC Mill foundations for units #1, 2, 3 & 4: -

a. Quality assessment of selected RCC members using Rebound Hammer testing technique as per IS 516 (Part 5/Sec 4):2020
b. Quality assessment of selected RCC members using Ultrasonic Pulse Velocity testing technique as per IS: IS: 516 (Part V) – 2019
c. Determination of equivalent cube compressive strength of concrete in RCC structure using concrete core extraction & testing technique as per IS: 456-2000 & IS: 516-1959.
d. Assessment of Carbonation depth of the extracted concrete cores.
e. Determine the corrosion status of reinforcement steel using Half-cell potential survey as per IS: 516 (PART 5, SECTION 2) – 2021 on few selected safely accessible RCC Members.
f. Determination of concrete cover thickness in RCC members using Ferro scanning technique at identified & safely accessible location.
g. Chemical Analysis to determine Chloride content, Sulphate content and pH value of Concrete Powder Samples in laboratory.

iii) Analysis and interpretation of test results/data obtained in (i) & (ii) above.

iv) Recommendations on remedial measures using indigenously available compatible repair materials. Preparation of BOQ covering selected items for repair including rate analysis & preparation of specifications and methodology for carrying out effective repair shall also be provided.

v) The report covering (i) to (iv) above.

2.0 DATA PROVIDED BY SPONSOR

- Year of Construction of the subject structure was around 1990

3.0 INVESTIGATION CARRIED OUT BY NCB

To collect the data of distress on RCC members of Mill foundations at **NTPC, TANDA, Uttar Pradesh,** and Visual observation survey was carried out jointly by NCB team and the concerned NTPC officials during the visits for condition assessment from 06th September to 09th September 2022.

3.1 Rebound Hammer Testing (RHT) As Per IS 516 (Part 5/Sec 4):2020

Rebound hammer testing technique was used for assessing the likely surface compressive strength of concrete. Basic principle of rebound hammer test is given below.

When the plunger of rebound hammer is pressed against the surface of the concrete, the spring-controlled mass rebounds and the extent of such rebound depends upon the surface hardness of concrete. The surface hardness and therefore the rebound are taken to be related to the compressive strength of the concrete. The rebound is read off along a graduated scale and is designated as the rebound number or rebound index. It is also to be noted that rebound indices are indicative of compressive strength of concrete to a limited depth from the surface. If the concrete in a particular member has internal micro cracking, flaws or heterogeneity across the cross-section, rebound hammer indices will not indicate the same. **IS: 516 (Part 5/Sec 4): 2020 states,** "*As such, the estimation of strength of concrete by rebound hammer method cannot be held to be very accurate and probable accuracy of prediction of concrete strength in a structure is ±25 percent*." However, the test should only be used as indication of the probable compressive strength of concrete.

The test was carried out using a Schmidt's Rebound Hammer on randomly selected accessible Mill foundations at **NTPC Tanda, Uttar Pradesh.** The members which were tested were made accessible. So the testing done on accessible members represents other members also.

The surfaces at the chosen locations were thoroughly cleaned with carborandum stone/grinding stone and readings were taken around each point. The average of the readings becomes the rebound index at that point of observation.

3.2 Ultrasonic Pulse Velocity (UPV) Method As per IS: 516 (Part V) – 2018.

UPV is a non-destructive evaluation method for assessing the quality of concrete; density, homogeneity and uniformity. Basic principle of UPV method is given below.

In this method, an ultrasonic pulse of longitudinal vibrations is produced by an electro-acoustical transducer which is held in contact with one surface of the concrete member under test. After traversing a known path length of the member, the pulse of vibrations is converted into an electric signal by a second electro-acoustical transducer, and an electric timing circuit enables the transit time of the pulse to be measured, from which the pulse velocity is calculated. For the present investigation, the pulse velocity measurements were obtained by direct transmission of ultrasonic pulses through the concrete, i.e. by "cross probing" & "Surface probing". For this purpose, the transducers were held on opposite faces of the beam and columns.

The Ultrasonic Pulse Velocity in concrete is mainly related to its density and modulus of elasticity. This in turn depends upon the materials and mix proportions used in making concrete as well as methods of placing, compaction and curing of concrete. If the concrete is not thoroughly compacted, or if there is segregation of concrete during placing or there are internal cracks or flaws, the pulse velocity will be lower, although the same materials and mix proportions are used.

The underlying principle of assessing the quality of concrete from UPV method is that, comparatively higher pulse velocities are obtained when the 'quality' of concrete in terms of density, homogeneity and uniformity is good. In case of concrete of poorer quality, lower velocities are obtained.

On this basis, guidelines have been evolved for characterizing the quality of concrete in structures in terms of ultrasonic pulse velocity. Such guideline reproduced from IS**: 516 (Part V) – 2018.**

3.3 Concrete Core Testing

Concrete cores of 60-mm diameter were extracted from different structural members identified, to estimate equivalent cube compressive strength of the structure. Equivalent cube strength does not indicate 28 days' standard cube strength rather it represents the in-situ cube

strength, and is compared vis-à-vis strength used in design calculation with safety of the structure under load in mind.

There are a number of parameters, which influence the measured compressive strengths. Such parameters include size (diameter) of the specimen, length-to-diameter ratio, direction of drilling, method of capping, drilling operations, moisture conditions of cores at the time of testing etc. Many of these parameters have been standardized.

The second set of variables relates to the intrinsic difference that exists between the concrete in structure and in standard laboratory controlled specimens, the core specimens representing the former. Such intrinsic differences are due to inherent differences that may occur in mixing constituents, degree of compaction, extent of curing and temperature condition in two cases. The procedure for sampling, preparing, testing and calculating the equivalent compressive strength with corrections are given in **IS: 516-2018.**

The net effect of all these parameters is that the strength of concrete cores is in general lower than those of laboratory controlled specimens, for this reason **IS: 456-2000** (Code of Practice for Plain and Reinforced Concrete)consider that concrete in the area represented by a core test is adequate if" *the average equivalent cube strength of the cores is equal to at least 85 percent of the specified for the corresponding age and if no single core has strength lower than 75 percent of the specified value".*

3.4 Carbonation Test

Carbonation is the formation of calcium carbonate ($CaCO_3$) by chemical reactions in concrete. When CO_2penetrates into the hardened concrete, it reacts with portlandite [Portlandite is a mineral formed during the curing of concrete, calcium hydroxide Ca $(OH)_2$] in the presence of moisture forming $CaCO_3$. The rate of carbonation depends mainly on the relative humidity, the concentration of CO_2, the penetration pressure and the temperature of the environment where concrete is placed.

As carbon dioxide enters the concrete from the environment, it reacts with calcium hydroxide present in the concrete and depending upon the quality of concrete it reduces the alkalinity of the pore fluids, depassivating ferric oxide layer on reinforcing bar which in turn initiates the process of corrosion in reinforcement.

To determine the depth of carbonation, concrete is exposed and sprayed with a pH indicator (solutions of 1%phenolphthalein in 70% ethyl alcohol). The demarcation between the

region, which turns into magenta (dark pink colour) and the region showing no change in colour indicate the carbonation front.

Carbonation measurements were recorded immediately after the cores specified in col. 3.4 were extracted.

3.5 Half-Cell Potential (HCP) Measurements

This test method covers the estimation of electrical Half Cell Potential of uncoated reinforcing steel, to determine corrosion activity using reference electrode copper; copper sulphate half-cell. It is not possible to expose all the reinforcements in the structural element and observe the extent of corrosion. So, this method has been very convenient to assess the condition of the entire length of a member by exposing a portion of the reinforcement at a suitable location, which measures the half-cell potential on the entire length, by placing the reference electrode on the wet concrete surface.

The Half-Cell Potential measurement is based on the principal of the corrosion, being an electro-chemical process, induces certain voltage to the reinforcement steel that is corroding. The wetting of the concrete is required to make the portion between the concrete surface and the reinforcing bar as electrolytes.

A criterion for assessment for corrosion of steel is given as under **IS: 516 (Part 5, Section 2)-2021** below.

- If potentials over an area are more positive than -200 mV, there is a greater than 90% probability that no reinforcing steel corrosion is occurring in that area at the time of measurement.
- If potentials over an area are in the range of -200 mV to -350 mV, corrosion activity of the reinforcing steel in that area is uncertain.
- If potentials over an area are more negative than -350 mV, there is a greater than 90% probability that reinforcing steel corrosion is occurring in that area at the time of measurement.

Adequate numbers of accessible RCC members were selected from various locations to conduct Half-Cell Potential test.

3.6 Concrete Cover Study

Concrete cover depth to reinforcing bars shall be done by using Ferro Scanner instrument on safe & accessible locations. This instrument detects the reinforcing bars and gives cover depth

their cover depth and determine the bar diameter. The instrument is based on the magnetic technique and is calibrated for different purposes. The cover depth is important from the point of view of estimation of initiation of corrosion of reinforcing bars.

For a longitudinal reinforcing bar in a Column nominal cover shall in any case not be less than 40mm or less than the diameter of such bar as per clause 26.4.2.1 of IS: 456-2000. Nominal cover to meet durability requirement for footing, minimum cover shall be 50mm as per clause 26.4.2.2 of IS: 456-2000.

Minimum values of nominal cover of normal weight aggregate concrete to be provided to all reinforcement including links to meet specified period of fire resistance shall be as per Table 16A of IS:456-2000.

Minimum values for the nominal cover of normal weight aggregate concrete which should be provided all reinforcement including links depending of exposure condition shall be as per the Table 5 of IS: 456-2000.

3.7 Chemical Analysis

Corrosion of reinforcing steel due to chlorides in concrete is one of the most common environmental attacks that lead to deterioration of concrete structures. Whenever there is chloride in concrete there is an increased risk of corrosion of embedded metal. Chloride content is then expressed in kg per cubic meter of concrete and compared with the values of limits of chloride contents of concrete (**Table 7 of IS: 456–2000**).

Sulphates (SO_3) are present in most cements and in some aggregates; excessive amounts of water-soluble sulphate from these or other mix constituents can cause expansion and disruption of concrete. To prevent it, **IS: 456-2000 clause-8.2.5.3** states that the total water-soluble sulphate content of the concrete mix, expressed as SO_3, should not exceed 4 percent by mass of the cement in the mix. The sulphate content should be calculated as the total from the various constituents of the mix.

The pH value of the concrete should be above 11.5 to maintain alkalinity of concrete surrounding the embedded steel. A reduction in the pH value of concrete indicates loss of passive layer around the reinforcement which protects the steel from distress.

For analyzing Chloride content and pH of concrete, concrete powder samples were extracted from 0-20mm, 20-40mm & 40-60mm depths at identified locations and then tested as

per IS:14959(Part 2) -2001 (Determination of water soluble and acid soluble Chlorides in Mortar and Concrete – Method of Test).

Adequate numbers of accessible RCC members were selected from various locations to extract concrete powders for chemical test.

4.0 RESULTS AND DISCUSSION

4.1. Visual Observations

Visual observations and testing carried out at Different levels of Mill foundations. Minor distress was found in the form of cracks, Honey Combs and surface voids on concrete surface. Whitish color powdered deposition of salts and efflorescence was developing at few locations of Mill foundations. The visual observations and photographs are shown in Annexure I.

4.2. Rebound Hammer Testing

Rebound Hammer testing was carried out on various identified RCC (Reinforced Cement Concrete) members of Mill foundations for units #1, 2, 3 & 4using random sampling technique the results of surface compressive strength obtained by Rebound Hammer testing are given in Table 2 to 25.

Surface Compressive strength results of concrete as obtained on different hardened concrete surfaces of RCC Members are summarized as:

1) Surface compressive strength of concrete obtained Mill Foundation-1A by Rebound Hammer Testing is found with an average surface compressive strength of **28.22 N/mm^2** (Refer Table 2).
2) Surface compressive strength of concrete obtained on Mill foundation-1B by Rebound Hammer Testing is found with an average surface compressive strength of **27.79 N/mm^2** (Refer Table 3).
3) Surface compressive strength of concrete obtained on Mill foundation-1C by Rebound Hammer Testing is found with an average surface compressive strength **29.35 N/mm^2** (Refer Table 4).

4) Surface compressive strength of concrete obtained on Mill foundation-1D by Rebound Hammer Testing is found with an average surface compressive strength of **27.79 N/mm^2** (Refer Table 5).

5) Surface compressive strength of concrete obtained on Mill Foundation-1E by Rebound Hammer Testing is found with an average surface compressive strength of **27.08 N/mm^2** (Refer Table 6).

6) Surface compressive strength of concrete obtained on Mill Foundation -1F by Rebound Hammer Testing is found with an average surface compressive strength of **28.07 N/mm^2** (Refer Table 7).

7) Surface compressive strength of concrete obtained on Mill Foundation-1G by Rebound Hammer Testing is found with an average surface compressive strength of **27.79 N/mm^2** (Refer Table 8).

8) Surface compressive strength of concrete obtained on Mill foundation-2A by Rebound Hammer Testing is found with an average surface compressive strength of **28.64 N/mm^2** (Refer Table 9).

9) Surface compressive strength of concrete obtained on Mill Foundation-2B by Rebound Hammer Testing is found with an average surface compressive strength of **28.85 N/mm^2** (Refer Table 10).

10) Surface compressive strength of concrete obtained on Mill Foundation-2C by Rebound Hammer Testing is found with an average surface compressive strength of **31.97 N/mm^2** (Refer Table 11).

11) Surface compressive strength of concrete obtained on Mill Foundation-2D by Rebound Hammer Testing is found with an average surface compressive strength of **30.69 N/mm^2** (Refer Table 12).

12) Surface compressive strength of concrete obtained on Mill Foundation-2E by Rebound Hammer Testing is found with an average surface compressive strength of **31.19 N/mm^2** (Refer Table 13).

13) Surface compressive strength of concrete obtained on Mill Foundation-2F by Rebound Hammer Testing is found with an average surface compressive strength of **32.60 N/mm^2** (Refer Table 14).

14) Surface compressive strength of concrete obtained on Mill Foundation-2G by Rebound Hammer Testing is found with an average surface compressive strength of **32.74 N/mm^2** (Refer Table 15).

15) Surface compressive strength of concrete obtained on Mill Foundation-3A by Rebound Hammer Testing is found with an average surface compressive strength of **34.09 N/mm^2** (Refer Table 16).

16) Surface compressive strength of concrete obtained on Mill Foundation-3B by Rebound Hammer Testing is found with an average surface compressive strength of **33.66 N/mm^2** (Refer Table 17).

17) Surface compressive strength of concrete obtained on Mill Foundation-3C by Rebound Hammer Testing is found with an average surface compressive strength of **33.66 N/mm^2** (Refer Table 18).

18) Surface compressive strength of concrete obtained on Mill Foundation-3D by Rebound Hammer Testing is found with an average surface compressive strength of **33.80 N/mm^2** (Refer Table 19).

19) Surface compressive strength of concrete obtained on Mill Foundation-3E by Rebound Hammer Testing is found with an average surface compressive strength of **32.74 N/mm^2** (Refer Table 20).

20) Surface compressive strength of concrete obtained on Mill Foundation-3F by Rebound Hammer Testing is found with an average surface compressive strength of **32.32 N/mm^2** (Refer Table 21).

21) Surface compressive strength of concrete obtained on Mill Foundation-3G by Rebound Hammer Testing is found with an average surface compressive strength of **33.24 N/mm^2** (Refer Table 22).

22) Surface compressive strength of concrete obtained on Mill Foundation-4A by Rebound Hammer Testing is found with an average surface compressive strength of **33.52 N/mm^2** (Refer Table 23).

23) Surface compressive strength of concrete obtained on Mill Foundation-4B by Rebound Hammer Testing is found with an average surface compressive strength of **33.38 N/mm^2** (Refer Table 24).

24) Surface compressive strength of concrete obtained on Mill Foundation-4C by Rebound Hammer Testing is found with an average surface compressive strength of **36.56 N/mm^2** (Refer Table 25).

4.3 Ultrasonic Pulse Velocity Testing (UPV):

The Ultrasonic Pulse Velocity testing was conducted on Mill foundations for units #1, 2, 3 & 4 in the presence of concerned engineering team of NTPC Tanda. The results of the UPV values obtained on various RCC members are as follows:

1) The UPV measurements were taken using Surface probing technique on the Mill Foundation -1A are in the range of **3.55 to 4.02km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018(Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table -27).
2) The UPV measurements were taken using Surface probing technique on the Mill Foundation -1Bare in the range of **3.54 to 4.09 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 28).
3) The UPV measurements were taken using Surface probing technique on the Mill Foundation -1Care in the range of **3.58 to 4.10 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 29).
4) The UPV measurements were taken using Cross probing technique on the Mill Foundation -1Dare in the range of **3.80 to 4.60 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 30).
5) The UPV measurements were taken using Cross probing technique on the Mill Foundation -1Eare in the range of **3.99 to 4.88 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 31).

6) The UPV measurements were taken using Cross probing technique on the Mill Foundation -1Fare in the range of **4.21 to 4.86 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 32).
7) The UPV measurements were taken using Surface probing technique on the Mill Foundation -1Gare in the range of **3.71 to 4.62 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 33).
8) The UPV measurements were taken using Surface probing technique on the Mill Foundation -2Aare in the range of **3.86 to 4.32 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 34).
9) The UPV measurements were taken using Surface probing technique on the Mill Foundation -2Bare in the range of **3.84 to 4.33 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 35).
10) The UPV measurements were taken using Surface probing technique on the Mill Foundation -2Care in the range of **3.75 to 4.23 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 36).
11) The UPV measurements were taken using Cross probing technique on the Mill Foundation -2Dare in the range of **3.93 to 4.47 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 37).
12) The UPV measurements were taken using Cross probing technique on the Mill Foundation -2Eare in the range of **3.91 to 4.49 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 38).
13) The UPV measurements were taken using Surface probing technique on the Mill Foundation -2Fare in the range of **3.75 to 4.44 km/sec**. When these values are compared

with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 39).

14) The UPV measurements were taken using Surface probing technique on the Mill Foundation -2Gare in the range of **3.62 to 4.48 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 40).

15) The UPV measurements were taken using Surface probing technique on the Mill Foundation -3Aare in the range of **3.75 to 4.22 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 41).

16) The UPV measurements were taken using Surface probing technique on the Mill Foundation -3Bare in the range of **3.86 to 4.67 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 42).

17) The UPV measurements were taken using Surface probing technique on the Mill Foundation -3Care in the range of **3.68 to 4.25 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 43).

18) The UPV measurements were taken using Cross probing technique on the Mill Foundation -3Dare in the range of **3.94 to 4.58 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 44).

19) The UPV measurements were taken using Cross probing technique on the Mill Foundation -3Eare in the range of **3.56 to 4.58 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 45).

20) The UPV measurements were taken using Cross probing technique on the Mill Foundation -3Fare in the range of **3.96 to 4.53 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 46).

21) The UPV measurements were taken using Surface probing technique on the Mill Foundation -3Gare in the range of **3.74 to 4.04 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 47).

22) The UPV measurements were taken using Surface probing technique on the Mill Foundation -4Aare in the range of **3.67 to 4.08 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 48).

23) The UPV measurements were taken using Surface probing technique on the Mill Foundation -4Bare in the range of **3.69 to 4.18 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 49).

24) The UPV measurements were taken using Cross probing technique on the Mill Foundation -4Care in the range of **3.51 to 3.91 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 50).

4.4 Concrete Core Testing

Corresponding to the 60mm concrete core extracted by random sampling technique covering different locations of Mill foundations for units #1, 2, 3 & 4in power plant of NTPC Tanda and tested at NCCBM laboratory Hyderabad, the equivalent cube compressive strength of concrete RCC members are shown in Table 54. In total, 28 nos. of concrete cores were extracted from different members of the Mill foundations all are found to be testable either due to short length of the cores.

The test results indicate that the equivalent cube compressive strength values for

1. Mill Foundation -1A is found to be **30.01 N/mm²**
2. Mill Foundation -1B is found to be **16.85N/mm2**
3. Mill Foundation -1C is found to be **20.28 N/mm2**
4. Mill Foundation -1D is found to be **16.51N/mm2**
5. Mill Foundation -1E is found to be **13.22N/mm2**
6. Mill Foundation-1Fis found to be **29.93N/mm2**

7. Mill Foundation -1Gis found to be **26.40N/mm2**
8. Mill Foundation -2Ais found to be **46.19N/mm2**
9. Mill Foundation -2Bis found to be **32.42N/mm2**
10. Mill Foundation -2Cis found to be **24.12N/mm2**
11. Mill Foundation -2Dis found to be **24.70N/mm2**
12. Mill Foundation -2Eis found to be **27.19N/mm2**
13. Mill Foundation -2F is found to be **30.81N/mm2**
14. Mill Foundation -2Gis found to be **25.62N/mm2**
15. Mill Foundation -3A is found to be **33.13N/mm2**
16. Mill Foundation -3Bis found to be **19.85N/mm2**
17. Mill Foundation -3C is found to be **18.50 N/mm2**
18. Mill Foundation -3D is found to be **39.35N/mm2**
19. Mill Foundation -3E is found to be**29.18N/mm2**
20. Mill Foundation -3F is found to be **22.77N/mm2**
21. Mill Foundation -3G is found to be **28.18N/mm2**
22. Mill Foundation -4A is found to be **28.95N/mm2**
23. Mill Foundation -4B is found to be **22.59N/mm2**
24. Mill Foundation -4C is found to be**28.20N/mm2**
25. Mill Foundation -4D is found to be**35.40N/mm2**
26. Mill Foundation -4E is found to be**34.66N/mm2**
27. Mill Foundation -4F is found to be**35.19N/mm2**
28. Mill Foundation -4G is found to be**38.85N/mm2**

In total, 28 nos. tested cores 25 of them found to have equivalent cube compressive strength more than specified characteristic compressive strength of M25 grade concrete (which is produced in Table 54).

4.5 Concrete Cover

The concrete cover depth to rebars in RCC members is measured with Ferro-scanner and a measuring tape/scale in the places where concrete is exposed and accessible for direct measurement. Nominal cover to reinforcement to meet durability requirement is given in **IS-456:**

Table 16-clause 26.4.2 (Also reproduced in Table-51), the measured cover to reinforcement steel in the selected RCC members are given in Table 52**.**

1. The Concrete cover to Reinforcing bars of Mill Foundation -1Aduring testing using Ferro scanner meter is found with an average of **62 mm.**
2. The Concrete cover to Reinforcing bars of Mill Foundation -1Bduring testing using Ferro scanner meter is found with an average of **48 mm.**
3. The Concrete cover to Reinforcing bars of Mill Foundation -1Cduring testing using Ferro scanner meter is found with an average of **57 mm.**
4. The Concrete cover to Reinforcing bars of Mill Foundation -1Dduring testing using Ferro scanner meter is found with an average of **51 mm.**
5. The Concrete cover to Reinforcing bars of Mill Foundation -1Eduring testing using Ferro scanner meter is found with an average of **62 mm.**
6. The Concrete cover to Reinforcing bars of Mill Foundation -1Fduring testing using Ferro scanner meter is found with an average of **72 mm.**
7. The Concrete cover to Reinforcing bars of Mill Foundation -1Gduring testing using Ferro scanner meter is found with an average of **74 mm.**
8. The Concrete cover to Reinforcing bars of Mill Foundation -2Aduring testing using Ferro scanner meter is found with an average of **65 mm.**
9. The Concrete cover to Reinforcing bars of Mill Foundation -2Bduring testing using Ferro scanner meter is found with an average of **65 mm.**
10. The Concrete cover to Reinforcing bars of Mill Foundation -2Cduring testing using Ferro scanner meter is found with an average of **69 mm.**
11. The Concrete cover to Reinforcing bars of Mill Foundation -2Dduring testing using Ferro scanner meter is found with an average of **66 mm.**
12. The Concrete cover to Reinforcing bars of Mill Foundation -2Eduring testing using Ferro scanner meter is found with an average of **70 mm.**
13. The Concrete cover to Reinforcing bars of Mill Foundation -2Fduring testing using Ferro scanner meter is found with an average of **71 mm.**
14. The Concrete cover to Reinforcing bars of Mill Foundation -2Gduring testing using Ferro scanner meter is found with an average of **70 mm.**

15. The Concrete cover to Reinforcing bars of Mill Foundation -3Aduring testing using Ferro scanner meter is found with an average of **62 mm.**
16. The Concrete cover to Reinforcing bars of Mill Foundation -3B during testing using Ferro scanner meter is found with an average of **75 mm.**
17. The Concrete cover to Reinforcing bars of Mill Foundation -3C during testing using Ferro scanner meter is found with an average of **69 mm.**
18. The Concrete cover to Reinforcing bars of Mill Foundation -3D during testing using Ferro scanner meter is found with an average of **77 mm.**
19. The Concrete cover to Reinforcing bars of Mill Foundation -3E during testing using Ferro scanner meter is found with an average of **68 mm.**
20. The Concrete cover to Reinforcing bars of Mill Foundation -3F during testing using Ferro scanner meter is found with an average of **69 mm.**
21. The Concrete cover to Reinforcing bars of Mill Foundation -3G during testing using Ferro scanner meter is found with an average of **77 mm.**
22. The Concrete cover to Reinforcing bars of Mill Foundation -4A during testing using Ferro scanner meter is found with an average of **67 mm.**
23. The Concrete cover to Reinforcing bars of Mill Foundation -4B during testing using Ferro scanner meter is found with an average of **74 mm.**
24. The Concrete cover to Reinforcing bars of Mill Foundation -4C during testing using Ferro scanner meter is found with an average of **67 mm.**
25. The Concrete cover to Reinforcing bars of Mill Foundation -4D during testing using Ferro scanner meter is found with an average of **73 mm.**
26. The Concrete cover to Reinforcing bars of Mill Foundation -4E during testing using Ferro scanner meter is found with an average of **69 mm.**
27. The Concrete cover to Reinforcing bars of Mill Foundation -4F during testing using Ferro scanner meter is found with an average of **67 mm.**
28. The Concrete cover to Reinforcing bars of Mill Foundation -4G during testing using Ferro scanner meter is found with an average of **69 mm.**

The Concrete cover within the specified limits to meet durability requirement as per IS: 456-2000 (Refer Table 16 of IS: 456-2000) which is Reproduced in Table 51.

4.6 Carbonation

Table-53shows test results of carbonation testing done on 28 nos. of Concrete Cores extracted from various representative concrete samples. The results indicate that the values of depth of carbonation in all different locations of Mill foundation for the unit's #1, 2, 3 & 4 are found to be **0-16**mm, on RCC members.

Based on the above carbonation study carried on different selected RCC members at several locations the carbonation depth is found to be within the concrete cover region.

4.7 Half-Cell Potential Test

Half-cell potential (HCP) measurements using copper, copper-sulfate half-cell technique as per IS: 516 (Part 5, Section 2)-2021 (Standard test method for corrosion potentials of uncoated reinforcing steel in concrete) were taken at site to ascertain corrosion status of reinforcing bars of various locations of Mill foundation for the unit's #1, 2, 3 & 4 at NTPC TANDA. The measurements were done on different locations randomly selected locations and comprising of representative samples of for the structure.

Test results (refer Table-56) when compared with the corrosion criteria as per ASTM C-876 (Table-55) indicate that probability of corrosion is found to be in "90% Possibility of no corrosion" & "Transit state of corrosion".

4.8 Chemical Analysis

The chemical analysis of water and powdered samples extracted from different elements of Mill foundation for the unit's #1, 2, 3 & 4 collecting by random sampling technique. This covered chloride content, sulphate content per cum of concrete as well pH value of powdered samples. The test results as obtained in NCCBM laboratory are shown in Table- 57. Analysis of interpretation of test results given as under:

1) Based on the results obtained from laboratory the range of chloride content in the Mill foundation Unit-1A was found with an average value of **0.35 kg/m^3**is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.38%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.65** which is slightly more than the specified limit to resist the corrosion.

2) Based on the results obtained from laboratory the range of chloride content in the Mill foundation Unit-1C was found with an average value of **0.28 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **2.22%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.5** which is slightly more than the specified limit to resist the corrosion.

3) Based on the results obtained from laboratory the range of chloride content in the Mill foundation Unit-1E was found with an average value of **0.32 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **2.2%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.46** which is slightly less than the specified limit to resist the corrosion.

4) Based on the results obtained from laboratory the range of chloride content in the Mill foundation Unit-1G was found with an average value of **0.22 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.62%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.60** which is slightly less than the specified limit to resist the corrosion.

5) Based on the results obtained from laboratory the range of chloride content in the Mill foundation Unit-2B was found with an average value of **0.31 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.44%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.64**which is slightly less than the specified limit to resist the corrosion.

6) Based on the results obtained from laboratory the range of chloride content in the Mill foundation Unit-2D was found with an average value of **0.16 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.88%** which is within the permissible

limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.65**which is slightly less than the specified limit to resist the corrosion.

7) Based on the results obtained from laboratory the range of chloride content in the Mill foundation Unit-2F was found with an average value of **0.26 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.7%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.7**which is slightly less than the specified limit to resist the corrosion.

8) Based on the results obtained from laboratory the range of chloride content in the Mill foundation Unit-3A was found with an average value of **0.21 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **2.7%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.2**which is slightly less than the specified limit to resist the corrosion.

9) Based on the results obtained from laboratory the range of chloride content in the Mill foundation Unit-3C was found with an average value of **0.49 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.88%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.3**which is slightly less than the specified limit to resist the corrosion.

10) Based on the results obtained from laboratory the range of chloride content in the Mill foundation Unit-3G was found with an average value of **0.08 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **2.54%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.63**which is slightly less than the specified limit to resist the corrosion.

11) Based on the results obtained from laboratory the range of chloride content in the Mill foundation Unit-4B was found with an average value of **0.13 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **3.0%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.58**which is slightly less than the specified limit to resist the corrosion.

12) Based on the results obtained from laboratory the range of chloride content in the Mill foundation Unit-4D was found with an average value of **0.17 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **3.02%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.45**which is slightly less than the specified limit to resist the corrosion.

5.0 Conclusions:

The following Conclusions can be broadly made from the testing results Mill foundation for the unit's #1, 2, 3 & 4:

i) Based on visual observations carried out in the Mill foundations, Minor distress was found in the form of cracks, Honey Comb and surface voids on concrete surface. Whitish color powdered deposition of salts and efflorescence was developing at few locations.

ii) Based on Rebound hammer test surface hardness and likely compressive strength found satisfactory and meeting the required limits as per data furnished by the client.

iii) Based on Ultrasonic Pulse Velocity (random sampling technique) to find quality and homogeneity of concrete on RCC members, the results were found to be good quality of concrete.

iv) The equivalent cube compressive strength of the core samples extracted from the Mill foundation for the unit's #1, 2, 3 & 4 is found meeting more than the required limit for M25 Grade of concrete.

v) Carbonation is found 0-16 mm after 30 years 'whereas concrete cover of RCC members is found to vary from 48 – 77 mm and found within the limits of concrete cover region.

vi) Based on the Half-Cell potential measurements done by random sampling technique at various locations and visual observations of Mill foundation for the unit's #1, 2, 3 & 4 given an initiation signal of either in "90% Possibility of no corrosion "&" Transit state of corrosion".

vii) The amount of Acid soluble chloride content and soluble sulphates in the concrete of Mill foundation for the unit's #1, 2, 3 & 4 is within the specified limits for all the samples and pH values for few of tested samples slightly less than 11.5 as per (IS: 456-2000& IS: 3025 -1984).

6.0 Recommendations

The following steps shall be taken to repair the cracks & strengthening of Mill foundations:

i) Chipping:

Cover concrete around the horizontal, vertical cracks & spalling of concrete shall be chipped off to the depth up to 40mm on RCC walls. The chipping in the spalled portion of the Shells and RCC Walls shall be limited up to the cover region. Chipping of loose/hollow sounding concrete can be done by striking the doubtful surfaces with 2 lb. hammer.

ii) Treatment for Cracks:

a. The cracks are to be widened by cutting V-grooves of 10mm x 10mm size and sealed with approved epoxy repair mortar.

b. After the sealing, 12mm dia galvanized steel injection nipples are to be inserted in the crack area and also wherever honeycombing is found by drilling holes of required diameter up to the depth of 30 – 80 mm at required spacing (generally 350 mm staggered spacing). The drilled holes must be made dust free by blowing compressed air and should be sealed after the insertion of the nozzle with approved adhesive and allowed to cure.

c. After the nipples are injected and cured, grouting in the proportion recommended by the manufacturer into the cracks/honeycombed area of concrete/masonry shall be done using suitable gun/pump at required pressure. Once the grouting work is finished, the extruding nipples can be cut-off after the curing period.

iii) Reinforcement Corrosion Treatment:

Wherever reinforcing rebar is found corroded in RCC walls

a) Remove the rust by manually or suitable means to make corroded reinforcing bars rust free.

b) Provide and apply corrosion protection using 2 coats of anticorrosive Zn rich epoxy phenolic rebar protection system of approved brand on the exposed old reinforcement by brush with interval of 24 hours between coats and corrosion protection of exposed old reinforcing bars.

c) Provide and apply concrete penetrating corrosion inhibitor (CPCI) of approved brand over the entire finished surface are obtained after removal of distressed concrete in 2 coats @ of $4m^2$/ltr/coat approximately.

iv) Bond Coat:

After chipping off the concrete cover, provide and apply structural grade two component epoxy bond coat prior to application of any type of mortar conforming to ASTM C - 881 -13 Type - II tested as per ASTM C –882-13 to ensure bond between old and new concrete by brush application. (Material manufacture from STP/BASF/SIKA/FOSRAC/KRISHNA Conchem/Pidilite or equivalent)

v) Making up lost section with Polymer Modified Mortar (PMM):

For repair of patches having, apply average 40mm PMM in 2-3 layers using SBR Latex conforming to ASTM C-1059-13 Type-I in damaged areas (1 Cement-3 part graded cleaned river sand + 20 % latex by weight of cement) with 0.35 w/c ratio, in 10-15 mm thick layers by applying bond coat between successive/each. (Material manufacture either from STP/BASF/SIKA/FOSRAC or equivalent)

vi) Fiber Wrapping (Single layer):

Strengthening structural elements with single layer of nonmetallic composite fiber wrapping system (TYFO Fiber wrap of M/s FYFE & Co., GOLD BOND 1892 of M/s

Krishna Conchem Products Pvt. Ltd OR EQUIVALENT) comprise of two layers of unidirectional E -glass fiber wrap (900 GSM) and compatible epoxy saturant, by wet layup system including,

Surface preparation: Grinding/ moulding concrete substrate, cleaning it with wire brush removing oil, laitance if present, rounding sharp edges to min 25 mm radius etc. complete.

Profiling: Applying compatible primer on prepared substrate, Filling the holes and uneven surface with thixotropic putty etc. complete Wrapping:

Wrapping: The fiber sheet to structural element at desired orientation using tamping roller to avoid any air voids etc. repeat the same procedure for multiple layer with the interval of 8 hrs.

Sand pasting: Applying second coat of saturant after min. 12 hrs., rectify air voids if any paste the river sand on it to make surface rough to take further finishes and plastering the surface after complete curing using 10 mm thick PMM (PMM to be paid extra), to give uniform finish. All complete as per direction of Engineer-In-Charge.

vi) Protective coating:

Before applying the protective coating on RCC walls and the outer wall surface shall be cleaned by scrubbing with hard steel brush to remove loose particles, disintegrated concrete, deposited smoke and dust particles etc. The scrubbed surface is cleaned by air blowing and then dries it completely. Apply min. 2 coats of two part high performance moisture compatible corrosion resistant coating material (base and curing agent) of approved manufacturer over prepared surface, using not less than theoretical consumption as per the manufacturer's specification. Total dry film thickness (DFT) including primer will be 300 - 400 microns.

Note:

1. Before taking up any repair work, the dryness of substrate concrete must be ensured for effective application of several repair materials. Remove oil, grease, wax, Cement laitance, loose particles and other contaminants by shot blasting, scarifying or mechanically wire brushing followed by vacuum cleaning from the substrate concrete.
2. During repair works of Mill foundations measures should be taken up in accordance with relevant safety standards and safety guidelines of Occupational safety & Health Administration (OSHA) for construction, arrangement like safety nets/platforms should be done.

.....

CONDITION ASSESSMENT STUDY OF CONCRETE STRUCTURES OF NTPC TANDA

FOR

NTPC TANDA, UTTAR PRADESH

REPORT OF TG UNIT#1
CDR/SP-6325
APRIL 2024

Centre for Construction Development and Research
NATIONALCOUNCILFORCEMENTANDBUILDINGMATERIALS
Old Bombay Road, Near Raidurgh Police Station,Hyderabad-500104

Prepared By	**A. Bharath**	for Adarsh
Checked By	**Adarsh Kumar N.S**	Adarsh
ApprovedBy	**BSRao**	10/4/24

ElectronicFileRef:	**Report No. NCB/CDR/**	**No. of Pages/Appendices**
CDR/F:/Report/SP-6325		

1.0 INTRODUCTION

NTPC Tanda, Uttar Pradesh approached National Council for Cement and Building Materials (NCB). To carry out condition assessment study of Turbine Generator (TG) unit#1 using Non Destructive Evaluation Technique including preparation of Quantities (BOQ), Cost Estimation for repair and restoration at NTPC Tanda. NCB took up the work as per PO No: 4000269971-026-1035 Dated 31.12.2021

Scope of works

a) To carry out condition assessment using Non-Destructive Evaluation Technique including Repair Methodology, preparation of Quantities (BOQ), Cost Estimate of Turbine Generator (TG) unit#1 at NTPC Tanda.

i) Visual observations of Turbine Generator (TG) unit#1: In this study visual observation indicating any sign of distress in members shall be carried out up to safely accessible heights. Visual observation data will be supplemented by photographs and other pertinent information wherever available.

ii) To conduct experimental investigation by Non-Destructive Testing technique on the selected representative members of each cell at different locations of the TG Unit#1:-

   a. Quality assessment of selected members using Rebound Hammer testing technique as per IS: 516-2020 (Part-V, Sec-IV).
   b. Quality assessment of selected members using Ultrasonic Pulse Velocity testing technique as per IS: IS: 516 (Part V) – 2018
   c. Determination of equivalent cube compressive strength of concrete in structure using concrete core extraction & testing technique as per IS: 456-2000 & IS: 516-2018.
   d. Assessment of Carbonation depth of the extracted concrete cores.
   e. Determine the corrosion status of reinforcement steel using Half-cell potential survey as per ASTM C876 on few selected safely accessible Members.
   f. Determination of concrete cover thickness in members using Ferro scanning technique at identified & safely accessible location.

CONDITION ASSESSMENT STUDY OF CONCRETE STRUCTURES OF NTPC TANDA

FOR

NTPC TANDA, UTTAR PRADESH

FINAL REPORT OF CHIMNEY UNIT#1&2
CDR/SP-6325
MARCH 2024

Centre for Construction Development and Research
NATIONAL COUNCIL FOR CEMENT AND BUILDING MATERIALS
Old Bombay Road, Near Raidurgh Police Station, Hyderabad-500104

Prepared By	**A. Bharath**	for Laash
Checked By	**Adarsh Kumar N.S**	Laash
Approved By	**B S Rao**	Sr. 06/03/24.

Electronic File Ref:	**Report No. NCB/CDR/**	**No. of Pages/Appendices**
CDR-2/F:/Report/SP-6325		

1.0 INTRODUCTION

NTPC Tanda, Uttar Pradesh approached National Council for Cement and Building Materials (NCB). To carry out condition assessment study of RCC Chimney unit#1&2 using Non Destructive Evaluation Technique including preparation of Quantities (BOQ), Cost Estimation for repair and restoration of RCC Chimney Unit#1&2 at NTPC Tanda. The structures were constructed around the year 1995. NCB took up the work as per PO No: 4000245388-026-1026 Dated 24.9.2020

Scope of works

a) To carry out condition assessment using Non-Destructive Evaluation Technique including Repair Methodology, preparation of Quantities (BOQ), Cost Estimate of RCC Chimney Unit#1&2 at NTPC Tanda, Uttar Pradesh

i) Visual observations of RCC chimney Unit#1&2: In this study visual observation indicating any sign of distress in RCC members shall be carried out up to safely accessible heights. Visual observation data will be supplemented by photographs and other pertinent information wherever available.

ii) To conduct experimental investigation by Non-Destructive Testing technique on the selected representative RCC members of each cell at different locations of the RCC Chimney: -

a. Quality assessment of selected RCC members using Rebound Hammer testing technique as per IS: 516 (Part V, Sec-IV) – 2020.
b. Quality assessment of selected RCC members using Ultrasonic Pulse Velocity testing technique as per IS: IS: 516 (Part V, Sec-I) – 2018
c. Determination of equivalent cube compressive strength of concrete in RCC structure using concrete core extraction & testing technique as per IS: 456-2000 & IS: 516-2018.
d. Assessment of Carbonation depth of the extracted concrete cores.
e. Determine the corrosion status of reinforcement steel using Half-cell potential survey as per ASTM C876 on few selected safely accessible RCC Members.
f. Determination of concrete cover thickness in RCC members using Ferro scanning technique at identified & safely accessible location.

CONDITION ASSESSMENT STUDY OF CONCRETE STRUCTURES OF NTPC TANDA

FOR

NTPC TANDA, UTTAR PRADESH

REPORT OF CLARIFLOCATORS-1, 2
CDR/SP-6325
APRIL 2024

Centre for Construction Development and Research
NATIONAL COUNCIL FOR CEMENT AND BUILDING MATERIALS
Old Bombay Road, Near Raidurgh Police Station, Hyderabad-500104

Prepared By	A. Bharath	for Charath
Checked By	Adarsh Kumar N.S	Charath
Approved By	B S Rao	25/04/24

Electronic File Ref:	Report No. NCB/CDR/	No. of Pages/Appendices
CDR-2/F:/Report/SP-6325		

1.0 INTRODUCTION

NTPC Tanda, Uttar Pradesh approached National Council for Cement and Building Materials (NCB). To carry out condition assessment study of Clariflocators-1, 2 using Non Destructive Evaluation Technique including preparation of Quantities (BOQ), Cost Estimation for repair and restoration at NTPC Tanda. NCB took up the work as per PO No: 4000269971-026-1035 Dated 31.12.2021

Scope of works

a) To carry out condition assessment using Non Destructive Evaluation Technique including repair methodology, preparation of quantities (BOQ), Cost estimate of Clariflocators-1, 2 at NTPC Tanda, Uttar Pradesh.

i) Visual observations of Clariflocators-1, 2: To collect data of distress on RCC members of Clariflocators shall be carried out up to safely accessible heights which were made accessible for testing. Visual observation data will be supplemented by photographs and other pertinent information wherever available.

ii) To conduct experimental investigation by Non Destructive Testing technique on the selected representative RCC members at different locations of the Clariflocators-1,2 -

a. Quality assessment of selected RCC members using Rebound Hammer testing technique as per IS 516 (Part 5/Sec 4):2020
b. Quality assessment of selected RCC members using Ultrasonic Pulse Velocity testing technique as per IS: IS: 516 (Part V) – 2019
c. Determination of equivalent cube compressive strength of concrete in RCC structure using concrete core extraction & testing technique as per IS: 456-2000 & IS: 516-1959.
d. Assessment of Carbonation depth of the extracted concrete cores.
e. Determine the corrosion status of reinforcement steel using Half-cell potential survey as per IS: 516 (PART 5, SECTION 2) – 2021 on few selected safely accessible RCC Members.
f. Determination of concrete cover thickness in RCC members using Ferro scanning technique at identified & safely accessible location.

g. Chemical Analysis to determine Chloride content, Sulphate content and pH value of Concrete Powder Samples in laboratory.

iii) Analysis and interpretation of test results/data obtained in (i) & (ii) above.

iv) Recommendations on remedial measures using indigenously available compatible repair materials. Preparation of BOQ covering selected items for repair including rate analysis & preparation of specifications and methodology for carrying out effective repair shall also be provided.

v) The report covering (i) to (iv) above.

2.0 DATA PROVIDED BY SPONSOR

- Year of Construction of the subject structure was around 1990

3.0 INVESTIGATION CARRIED OUT BY NCB

To collect the data of distress on RCC members of Clariflocators at **NTPC, TANDA, Uttar Pradesh,** and Visual observation survey was carried out jointly by NCB team and the concerned NTPC officials during the visits for condition assessment from 06th September to 10th September 2022.

3.1 Rebound Hammer Testing (RHT) As Per IS 516 (Part 5/Sec 4):2020

Rebound hammer testing technique was used for assessing the likely surface compressive strength of concrete. Basic principle of rebound hammer test is given below.

When the plunger of rebound hammer is pressed against the surface of the concrete, the spring-controlled mass rebounds and the extent of such rebound depends upon the surface hardness of concrete. The surface hardness and therefore the rebound are taken to be related to the compressive strength of the concrete. The rebound is read off along a graduated scale and is designated as the rebound number or rebound index. It is also to be noted that rebound indices are indicative of compressive strength of concrete to a limited depth from the surface. If the concrete in a particular member has internal micro cracking, flaws or heterogeneity across the cross-section, rebound hammer indices will not indicate the same. **IS: 516 (Part 5/Sec 4): 2020 states,** "*As such, the estimation of strength of concrete by rebound hammer method cannot be held to be very accurate and probable accuracy of prediction of concrete strength in a structure is ±25 percent*." However, the test should only be used as indication of the probable compressive strength of concrete.

The test was carried out using a Schmidt's Rebound Hammer on randomly selected accessible Mill foundations at **NTPC Tanda, Uttar Pradesh.** The members which were tested were made accessible. So the testing done on accessible members represents other members also. The surfaces at the chosen locations were thoroughly cleaned with carborandum stone/grinding stone and readings were taken around each point. The average of the readings becomes the rebound index at that point of observation.

3.2 Ultrasonic Pulse Velocity (UPV) Method As per IS: 516 (Part V) – 2018.

UPV is a non-destructive evaluation method for assessing the quality of concrete; density, homogeneity and uniformity. Basic principle of UPV method is given below.

In this method, an ultrasonic pulse of longitudinal vibrations is produced by an electro-acoustical transducer which is held in contact with one surface of the concrete member under test. After traversing a known path length of the member, the pulse of vibrations is converted into an electric signal by a second electro-acoustical transducer, and an electric timing circuit enables the transit time of the pulse to be measured, from which the pulse velocity is calculated. For the present investigation, the pulse velocity measurements were obtained by direct transmission of ultrasonic pulses through the concrete, i.e. by "cross probing" & "Surface probing". For this purpose, the transducers were held on opposite faces of the beam and columns.

The Ultrasonic Pulse Velocity in concrete is mainly related to its density and modulus of elasticity. This in turn depends upon the materials and mix proportions used in making concrete as well as methods of placing, compaction and curing of concrete. If the concrete is not thoroughly compacted, or if there is segregation of concrete during placing or there are internal cracks or flaws, the pulse velocity will be lower, although the same materials and mix proportions are used.

The underlying principle of assessing the quality of concrete from UPV method is that, comparatively higher pulse velocities are obtained when the 'quality' of concrete in terms of density, homogeneity and uniformity is good. In case of concrete of poorer quality, lower velocities are obtained.

On this basis, guidelines have been evolved for characterizing the quality of concrete in structures in terms of ultrasonic pulse velocity. Such guideline reproduced from IS**: 516 (Part V) – 2018.**

3.3 Concrete Core Testing

Concrete cores of 60-mm diameter were extracted from different structural members identified, to estimate equivalent cube compressive strength of the structure. Equivalent cube strength does not indicate 28 days' standard cube strength rather it represents the in-situ cube strength, and is compared vis-à-vis strength used in design calculation with safety of the structure under load in mind.

There are a number of parameters, which influence the measured compressive strengths. Such parameters include size (diameter) of the specimen, length-to-diameter ratio, direction of drilling, method of capping, drilling operations, moisture conditions of cores at the time of testing etc. Many of these parameters have been standardized.

The second set of variables relates to the intrinsic difference that exists between the concrete in structure and in standard laboratory controlled specimens, the core specimens representing the former. Such intrinsic differences are due to inherent differences that may occur in mixing constituents, degree of compaction, extent of curing and temperature condition in two cases. The procedure for sampling, preparing, testing and calculating the equivalent compressive strength with corrections are given in **IS: 516-2018.**

The net effect of all these parameters is that the strength of concrete cores is in general lower than those of laboratory controlled specimens, for this reason **IS: 456-2000** (Code of Practice for Plain and Reinforced Concrete)consider that concrete in the area represented by a core test is adequate if" *the average equivalent cube strength of the cores is equal to at least 85 percent of the specified for the corresponding age and if no single core has strength lower than 75 percent of the specified value".*

3.4 Carbonation Test

Carbonation is the formation of calcium carbonate ($CaCO_3$) by chemical reactions in concrete. When CO_2penetrates into the hardened concrete, it reacts with portlandite [Portlandite is a mineral formed during the curing of concrete, calcium hydroxide Ca $(OH)_2$] in the presence of moisture forming $CaCO_3$. The rate of carbonation depends mainly on the relative humidity, the concentration of CO_2, the penetration pressure and the temperature of the environment where concrete is placed.

As carbon dioxide enters the concrete from the environment, it reacts with calcium hydroxide present in the concrete and depending upon the quality of concrete it reduces the

alkalinity of the pore fluids, depassivating ferric oxide layer on reinforcing bar which in turn initiates the process of corrosion in reinforcement.

To determine the depth of carbonation, concrete is exposed and sprayed with a pH indicator (solutions of 1%phenolphthalein in 70% ethyl alcohol). The demarcation between the region, which turns into magenta (dark pink colour) and the region showing no change in colour indicate the carbonation front.

Carbonation measurements were recorded immediately after the cores specified in col. 3.4 were extracted.

3.5 Half-Cell Potential (HCP) Measurements

This test method covers the estimation of electrical Half Cell Potential of uncoated reinforcing steel, to determine corrosion activity using reference electrode copper; copper sulphate half-cell. It is not possible to expose all the reinforcements in the structural element and observe the extent of corrosion. So, this method has been very convenient to assess the condition of the entire length of a member by exposing a portion of the reinforcement at a suitable location, which measures the half-cell potential on the entire length, by placing the reference electrode on the wet concrete surface.

The Half-Cell Potential measurement is based on the principal of the corrosion, being an electro-chemical process, induces certain voltage to the reinforcement steel that is corroding. The wetting of the concrete is required to make the portion between the concrete surface and the reinforcing bar as electrolytes.

A criterion for assessment for corrosion of steel is given as under **IS: 516 (Part 5, Section 2)-2021** below.

- If potentials over an area are more positive than -200 mV, there is a greater than 90% probability that no reinforcing steel corrosion is occurring in that area at the time of measurement.
- If potentials over an area are in the range of -200 mV to -350 mV, corrosion activity of the reinforcing steel in that area is uncertain.
- If potentials over an area are more negative than -350 mV, there is a greater than 90% probability that reinforcing steel corrosion is occurring in that area at the time of measurement.

Adequate numbers of accessible RCC members were selected from various locations to conduct Half-Cell Potential test.

3.6 Concrete Cover Study

Concrete cover depth to reinforcing bars shall be done by using Ferro Scanner instrument on safe & accessible locations. This instrument detects the reinforcing bars and mesh, to measure their cover depth and determine the bar diameter. The instrument is based on the magnetic technique and is calibrated for different purposes. The cover depth is important from the point of view of estimation of initiation of corrosion of reinforcing bars.

For a longitudinal reinforcing bar in a Column nominal cover shall in any case not be less than 40mm or less than the diameter of such bar as per clause 26.4.2.1 of IS: 456-2000. Nominal cover to meet durability requirement for footing, minimum cover shall be 50mm as per clause 26.4.2.2 of IS: 456-2000.

Minimum values of nominal cover of normal weight aggregate concrete to be provided to all reinforcement including links to meet specified period of fire resistance shall be as per Table 16A of IS:456-2000.

Minimum values for the nominal cover of normal weight aggregate concrete which should be provided all reinforcement including links depending of exposure condition shall be as per the Table 5 of IS: 456-2000.

3.7 Chemical Analysis

Corrosion of reinforcing steel due to chlorides in concrete is one of the most common environmental attacks that lead to deterioration of concrete structures. Whenever there is chloride in concrete there is an increased risk of corrosion of embedded metal. Chloride content is then expressed in kg per cubic meter of concrete and compared with the values of limits of chloride contents of concrete (**Table 7 of IS: 456–2000**).

Sulphates (SO_3) are present in most cements and in some aggregates; excessive amounts of water-soluble sulphate from these or other mix constituents can cause expansion and disruption of concrete. To prevent it, **IS: 456-2000 clause-8.2.5.3** states that the total water-soluble sulphate content of the concrete mix, expressed as SO_3, should not exceed 4 percent by mass of the cement in the mix. The sulphate content should be calculated as the total from the various constituents of the mix.

The pH value of the concrete should be above 11.5 to maintain alkalinity of concrete surrounding the embedded steel. A reduction in the pH value of concrete indicates loss of passive layer around the reinforcement which protects the steel from distress.

For analyzing Chloride content and pH of concrete, concrete powder samples were extracted from 0-25mm, 25-50mm depths at identified locations and then tested as per IS:14959(Part 2) -2001 (Determination of water soluble and acid soluble Chlorides in Mortar and Concrete – Method of Test).

Adequate numbers of accessible RCC members were selected from various locations to extract concrete powders for chemical test.

4.0 RESULTS AND DISCUSSION

4.1. Visual Observations

Visual observations and testing carried out at Different levels of Clariflocators. Distress was found in the form of cracks, Honeycombs and Seepage of Water through concrete surface. Colour deterioration, spalling of Concrete was noticed at few locations of Clariflocators. The visual observations and photographs are shown in Annexure I.

4.2. Rebound Hammer Testing:

Rebound Hammer testing was carried out on various identified RCC (Reinforced Cement Concrete) members of Clariflocators-1, 2 using random sampling technique the results of surface compressive strength obtained by Rebound Hammer testing are given in Table 2 to 17.

Surface Compressive strength results of concrete as obtained on different hardened concrete surfaces of RCC Members are summarized as:

1) Surface compressive strength of concrete obtained Clariflocator-1 East side wall by Rebound Hammer Testing is found with an average surface compressive strength of **31.75 N/mm^2** (Refer Table 2).
2) Surface compressive strength of concrete obtained on Clariflocator-1 West side wall by Rebound Hammer Testing is found with an average surface compressive strength of **34.80 N/mm^2** (Refer Table 3).

3) Surface compressive strength of concrete obtained on Clariflocator-1 South side wall by Rebound Hammer Testing is found with an average surface compressive strength **34.16 N/mm^2** (Refer Table 4).

4) Surface compressive strength of concrete obtained on Clariflocator-1 North side wall by Rebound Hammer Testing is found with an average surface compressive strength of **33.95 N/mm^2** (Refer Table 5).

5) Surface compressive strength of concrete obtained on Clariflocator-1 North East side wall by Rebound Hammer Testing is found with an average surface compressive strength of **36.07 N/mm^2** (Refer Table 6).

6) Surface compressive strength of concrete obtained on Clariflocator-1 South West side wall by Rebound Hammer Testing is found with an average surface compressive strength of **33.66 N/mm^2** (Refer Table 7).

7) Surface compressive strength of concrete obtained on Clariflocator-1 North West side wall by Rebound Hammer Testing is found with an average surface compressive strength of **31.97 N/mm^2** (Refer Table 8).

8) Surface compressive strength of concrete obtained on Clariflocator-1 North West side wall by Rebound Hammer Testing is found with an average surface compressive strength of **35.64 N/mm^2** (Refer Table 9).

9) Surface compressive strength of concrete obtained on Clariflocator-2 North side wall by Rebound Hammer Testing is found with an average surface compressive strength of **32.81 N/mm^2** (Refer Table 10).

10) Surface compressive strength of concrete obtained on Clariflocator-2 South side wall by Rebound Hammer Testing is found with an average surface compressive strength of **33.10 N/mm^2** (Refer Table 11).

11) Surface compressive strength of concrete obtained on Clariflocator-2 East side wall by Rebound Hammer Testing is found with an average surface compressive strength of **33.73 N/mm^2** (Refer Table 12).

12) Surface compressive strength of concrete obtained on Clariflocator-2 West side wall by Rebound Hammer Testing is found with an average surface compressive strength of **32.74 N/mm^2** (Refer Table 13).

13) Surface compressive strength of concrete obtained on Clariflocator-2 North East side wall by Rebound Hammer Testing is found with an average surface compressive strength of **33.03 N/mm^2** (Refer Table 14).

14) Surface compressive strength of concrete obtained on Clariflocator-2 South West side wall by Rebound Hammer Testing is found with an average surface compressive strength of **32.96 N/mm^2** (Refer Table 15).

15) Surface compressive strength of concrete obtained on Clariflocator-2 North West side wall by Rebound Hammer Testing is found with an average surface compressive strength of **33.66 N/mm^2** (Refer Table 16).

16) Surface compressive strength of concrete obtained on Clariflocator-2 North West side wall by Rebound Hammer Testing is found with an average surface compressive strength of **34.09 N/mm^2** (Refer Table 17).

4.3 Ultrasonic Pulse Velocity Testing (UPV):

The Ultrasonic Pulse Velocity testing was conducted on Clariflocators for #1, 2 in the presence of concerned engineering team of NTPC Tanda. The results of the UPV values obtained on various RCC members are as follows:

1) The UPV measurements were taken using Surface probing technique on the Clariflocator-1 East side wall are in the range of **3.77 to 4.6 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018(Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table -19).
2) The UPV measurements were taken using Cross probing technique on the Clariflocator-1 West side wall are in the range of **3.62 to 4.09 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 20).
3) The UPV measurements were taken using Cross probing technique on the Clariflocator-1 South side wall are in the range of **3.64 to 4.27 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 21).
4) The UPV measurements were taken using Cross probing technique on the Clariflocator-1 North side wall are in the range of **3.58 to 4.13 km/sec**. When these values are

compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 22).

5) The UPV measurements were taken using Cross probing technique on the Clariflocator-1 North East side wall are in the range of **3.56 to 4.08 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 23).
6) The UPV measurements were taken using Surface probing technique on the Clariflocator-1 South West side wall are in the range of **3.54 to 3.98 km/sec**. When these values are compared with the velocity criteria of IS:516 (Part V)–2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 24).
7) The UPV measurements were taken using Surface probing technique on the Clariflocator-1 North West side wall are in the range of **3.55 to 3.98 km/sec**. When these values are compared with the velocity criteria of IS:516 (Part V)–2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 25).
8) The UPV measurements were taken using Surface probing technique on the Clariflocator-1 North West side wall are in the range of **3.51 to 3.88 km/sec**. When these values are compared with the velocity criteria of IS:516 (Part V)–2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 26).
9) The UPV measurements were taken using Surface probing technique on the Clariflocator-2 North side wall are in the range of **3.98 to 4.66km/sec**. When these values are compared with the velocity criteria of IS:516 (Part V)–2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 27).
10) The UPV measurements were taken using Cross probing technique on the Clariflocator-2 North side wall are in the range of **3.61 to 4.19 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 28).
11) The UPV measurements were taken using Cross probing technique on the Clariflocator-2 East side wall are in the range of **3.59 to 4.08 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 29).

12) The UPV measurements were taken using Cross probing technique on the Clariflocator-2 West side wall are in the range of **3.64 to 4.02 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 30).

13) The UPV measurements were taken using Cross probing technique on the Clariflocator-2 North East side wall are in the range of **3.73 to 4.08 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 31).

14) The UPV measurements were taken using Surface probing technique on the Clariflocator-2 South West side wall are in the range of **4.06 to 4.41 km/sec**. When these values are compared with the velocity criteria of IS:516 (Part V)–2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 32).

15) The UPV measurements were taken using Surface probing technique on the Clariflocator-2 North West side wall are in the range of **3.86 to 4.26 km/sec**. When these values are compared with the velocity criteria of IS:516 (Part V)–2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 33).

16) The UPV measurements were taken using Surface probing technique on the Clariflocator-2 North West side wall are in the range of **3.89 to 4.22 km/sec**. When these values are compared with the velocity criteria of IS: 516(Part V) – 2018 (Also reproduced in Table 18), the overall quality of concrete is assessed to be **GOOD** (Table - 34).

4.4 Concrete Core Testing:

Corresponding to the 60mm concrete core extracted by random sampling technique covering different locations of Clariflocators- 1, 2 in power plant of NTPC Tanda and tested at NCCBM laboratory Hyderabad, the equivalent cube compressive strength of concrete RCC members are shown in Tables- 40, 41. In total, 28 nos. of concrete cores were extracted from different members of the Clariflocators all are found to be testable either due to short length of the cores.

The test results indicate that the equivalent cube compressive strength values for

Clariflocator-1

1. Clariflocator-1 East side wall is found to be **48.30 N/mm²**
2. Clariflocator-1 West side wall is found to be **64.63 N/mm2**
3. Clariflocator-1 South side wall is found to be **31.00 N/mm2**
4. Clariflocator-1 North side wall is found to be **47.00 N/mm2**
5. Clariflocator-1 North East side wall is found to be **33.41 N/mm2**
6. Clariflocator-1 South West side wall is found to be **39.13 N/mm2**
7. Clariflocator-1 North West side wall is found to be **33.26 N/mm2**
8. Clariflocator-1 North West side wall is found to be **36.80 N/mm2**

Clariflocator-2

1. Clariflocator-2 North side wall is found to be **35.49 N/mm2**
2. Clariflocator-2 South side wall is found to be **31.93 N/mm2**
3. Clariflocator-2 East side wall is found to be **25.53 N/mm2**
4. Clariflocator-2 West side wall is found to be **34.32 N/mm2**
5. Clariflocator-2 North East side wall is found to be **37.92 N/mm2**
6. Clariflocator-2 South West side wall is found to be **35.34 N/mm2**
7. Clariflocator-2 North West side wall is found to be **36.34 N/mm2**
8. Clariflocator-2 North West side wall is found to be **32.87 N/mm2**

In total, 16 nos tested cores all of them found to have equivalent cube compressive strength more than specified characteristic compressive strength of M25 grade concrete (which is produced in Table- 40,41).

4.5 Concrete Cover :

The concrete cover depth to rebars in RCC members is measured with Ferro-scanner and a measuring tape/scale in the places where concrete is exposed and accessible for direct measurement. Nominal cover to reinforcement to meet durability requirement is given in **IS-456: Table 16-clause 26.4.2** (Also reproduced in Table-35), the measured cover to reinforcement steel in the selected RCC members are given in Table 36,37**.**

Clariflocator-1

1. The Concrete cover to Reinforcing bars of Clariflocator-1 East side wall during testing using Ferro scanner meter is found with an average of **50 mm.**

2. The Concrete cover to Reinforcing bars of Clariflocator-1 West side wall during testing using Ferro scanner meter is found with an average of **54 mm.**
3. The Concrete cover to Reinforcing bars of Clariflocator-1 South side wall during testing using Ferro scanner meter is found with an average of **57 mm.**
4. The Concrete cover to Reinforcing bars of Clariflocator-1 North side wall during testing using Ferro scanner meter is found with an average of **56 mm.**
5. The Concrete cover to Reinforcing bars of Clariflocator-1 North East side wall during testing using Ferro scanner meter is found with an average of **52 mm.**
6. The Concrete cover to Reinforcing bars of Clariflocator-1 South West side wall during testing using Ferro scanner meter is found with an average of **53 mm.**
7. The Concrete cover to Reinforcing bars of Clariflocator-1 North West side wall during testing using Ferro scanner meter is found with an average of **57 mm.**
8. The Concrete cover to Reinforcing bars of Clariflocator-1 North West side wall during testing using Ferro scanner meter is found with an average of **54 mm.**

Clariflocator-2

1. The Concrete cover to Reinforcing bars of Clariflocator-2 North side wall during testing using Ferro scanner meter is found with an average of **51 mm.**
2. The Concrete cover to Reinforcing bars of Clariflocator-2 South side wall during testing using Ferro scanner meter is found with an average of **52 mm.**
3. The Concrete cover to Reinforcing bars of Clariflocator-2 East side wall during testing using Ferro scanner meter is found with an average of **58 mm.**
4. The Concrete cover to Reinforcing bars of Clariflocator-2 West side wall during testing using Ferro scanner meter is found with an average of **57 mm.**
5. The Concrete cover to Reinforcing bars of Clariflocator-2 North East side wall during testing using Ferro scanner meter is found with an average of **52 mm.**
6. The Concrete cover to Reinforcing bars of Clariflocator-2 South West side wall during testing using Ferro scanner meter is found with an average of **55 mm.**
7. The Concrete cover to Reinforcing bars of Clariflocator-2 North West side wall during testing using Ferro scanner meter is found with an average of **54 mm.**
8. The Concrete cover to Reinforcing bars of Clariflocator-2 North West side wall during testing using Ferro scanner meter is found with an average of **55 mm.**

The Concrete cover within the specified limits to meet durability requirement as per IS: 456-2000 (Refer Table 16 of IS: 456-2000) which is Reproduced in Table 35.

4.6 Carbonation:

Table-38,39 shows test results of carbonation testing done on 16 nos. of Concrete Cores extracted from various representative concrete samples. The results indicate that the values of depth of carbonation in all different locations of Clariflocators-1, 2 are found to be **0-8**mm, on RCC members.

Based on the above carbonation study carried on different selected RCC members at several locations the carbonation depth is found to be within the concrete cover region.

4.7 Half-Cell Potential Test :

Half-cell potential (HCP) measurements using copper, copper-sulfate half-cell technique as per IS: 516 (Part 5, Section 2)-2021 (Standard test method for corrosion potentials of uncoated reinforcing steel in concrete) were taken at site to ascertain corrosion status of reinforcing bars of various locations of Clariflocators-1, 2 at NTPC TANDA. The measurements were done on different locations randomly selected locations and comprising of representative samples of for the structure.

Test results (refer Table- 43,44) when compared with the corrosion criteria as per ASTM C-876 (Table-42) indicate that probability of corrosion is found to be in “90% Possibility of no corrosion”.

4.8 Chemical Analysis :

The chemical analysis of water and powdered samples extracted from different elements of Clariflocators-1, 2 collecting by random sampling technique. This covered chloride content, sulphate content per cum of concrete as well pH value of powdered samples. The test results as obtained in NCCBM laboratory are shown in Table- 45,46. Analysis of interpretation of test results given as under:

1) Based on the results obtained from laboratory the range of chloride content in the Clariflocators-1 East side wall was found with an average value of **0.09 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3)

content by mass of the cement in mix with an average value of **1.57%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.3** which is within the specified limit to resist the corrosion.

2) Based on the results obtained from laboratory the range of chloride content in the Clariflocators-1 West side wall was found with an average value of **0.13 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.58%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.46** which is within the specified limit specified limit to resist the corrosion.

3) Based on the results obtained from laboratory the range of chloride content in the Clariflocators-1 South side wall was found with an average value of **0.16 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.44%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.52** which is within the specified limit to resist the corrosion.

4) Based on the results obtained from laboratory the range of chloride content in the Clariflocators-1 North side wall was found with an average value of **0.14 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.5%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.54** which is within the specified limit to resist the corrosion.

5) Based on the results obtained from laboratory the range of chloride content in the Clariflocators-1 North East side wall was found with an average value of **0.18 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.5%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of

pH value is found with an average of **11.55** is within the specified limit to resist the corrosion.

6) Based on the results obtained from laboratory the range of chloride content in the Clariflocators-2 North side wall was found with an average value of **0.13 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.62%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.35** which is within the specified limit to resist the corrosion.

7) Based on the results obtained from laboratory the range of chloride content in the Clariflocators-2 South side wall was found with an average value of **0.15 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.58%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.48** which is within the specified limit to resist the corrosion.

8) Based on the results obtained from laboratory the range of chloride content in the Clariflocators-2 East side wall was found with an average value of **0.16 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.44%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.57** is within the specified limit to resist the corrosion.

9) Based on the results obtained from laboratory the range of chloride content in the Clariflocators-2 West side wall was found with an average value of **0.15 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.5%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.58** which is within the specified limit to resist the corrosion.

10) Based on the results obtained from laboratory the range of chloride content in the Clariflocators-2 North East side wall was found with an average value of **0.17 kg/m^3** is

within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix with an average value of **1.47%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found with an average of **11.57** which is within the specified limit to resist the corrosion.

5.0 Conclusions:

The following Conclusions can be broadly made from the testing results Clariflocators-,1,2:

i) Based on visual observations carried out in the Clariflocators-,1,2 locations Distress was found in the form of cracks, Honey combs and Seepage of Water on concrete surface. Colour deterioration, Peeling of Concrete was developing at few locations.

ii) Based on Rebound hammer test surface hardness and likely compressive strength found satisfactory and meeting the required limits as per data furnished by the client.

iii) Based on Ultrasonic Pulse Velocity (random sampling technique) to find quality and homogeneity of concrete on RCC members, the results were found to be good quality of concrete.

iv) The equivalent cube compressive strength of the core samples extracted from the Clariflocators-1, 2 is found meeting more than the required limit for M25 Grade of concrete.

v) Carbonation is found 0-8mm after 30 years 'whereas concrete cover of RCC members is found to vary from 51 – 58 mm and found within the limits of concrete cover region.

vi) Based on the Half-Cell potential measurements done by random sampling technique at various locations and visual observations of Clariflocators-1, 2 given an initiation signal of either in "90% Possibility of no corrosion".

vii) The amount of Acid soluble chloride content and soluble sulphates in the concrete of Clariflocators-1, 2 is within the specified limits for all the samples and pH values for few of tested samples slightly less than 11.5 as per (IS: 456-2000& IS: 3025 -1984).

6.0 Recommendations

The following steps shall be taken to repair the cracks & strengthening of Clariflocators-1, 2 :

i) Chipping:

Cover concrete around the horizontal, vertical cracks & spalling of concrete shall be chipped off to the depth up to 40mm on RCC walls. The chipping in the spalled portion of the Shells and RCC Walls shall be limited up to the cover region. Chipping of loose/hollow sounding concrete can be done by striking the doubtful surfaces with 2 lb. hammer.

ii) Treatment for Cracks:

a. The cracks are to be widened by cutting V-grooves of 10mm x 10mm size and sealed with approved epoxy repair mortar.

b. After the sealing, 12mm dia galvanized steel injection nipples are to be inserted in the crack area and also wherever honeycombing is found by drilling holes of required diameter up to the depth of 30 – 80 mm at required spacing (generally 350 mm staggered spacing). The drilled holes must be made dust free by blowing compressed air and should be sealed after the insertion of the nozzle with approved adhesive and allowed to cure.

c. After the nipples are injected and cured, grouting in the proportion recommended by the manufacturer into the cracks/honeycombed area of concrete/masonry shall be done using suitable gun/pump at required pressure. Once the grouting work is finished, the extruding nipples can be cut-off after the curing period.

iii) Reinforcement Corrosion Treatment:

Wherever reinforcing rebar is found corroded in RCC walls

a) Remove the rust by manually or suitable means to make corroded reinforcing bars rust free.

b) Provide and apply corrosion protection using 2 coats of anticorrosive Zn rich epoxy phenolic rebar protection system of approved brand on the exposed old reinforcement by brush with interval of 24 hours between coats and corrosion protection of exposed old reinforcing bars.

c) Provide and apply concrete penetrating corrosion inhibitor (CPCI) of approved brand over the entire finished surface are obtained after removal of distressed concrete in 2 coats @ of $4m^2$/ltr/coat approximately.

iv) Bond Coat:

After chipping off the concrete cover, provide and apply structural grade two component epoxy bond coat prior to application of any type of mortar conforming to ASTM C - 881 -13 Type - II tested as per ASTM C –882-13 to ensure bond between old and new concrete by brush application. (Material manufacture from SYNORGANIC /BASF/SIKA/FOSRAC/KRISHNA Conchem/Pidilite or equivalent)

v) Making up lost section with Polymer Modified Mortar (PMM):

For repair of patches having, apply average 40mm PMM in 2-3 layers using SBR Latex conforming to ASTM C-1059-13 Type-I in damaged areas (1 Cement-3 part graded cleaned river sand + 20 % latex by weight of cement) with 0.35 w/c ratio, in 10-15 mm thick layers by applying bond coat between successive/each. (Material manufacture either from SYNORGANIC/BASF/SIKA/FOSRAC or equivalent)

vi) Protective coating:

Before applying the protective coating on RCC walls and the outer wall surface shall be cleaned by scrubbing with hard steel brush to remove loose particles, disintegrated concrete, deposited smoke and dust particles etc. The scrubbed surface is cleaned by air blowing and then dries it completely. Apply min. 2 coats of two part high performance moisture compatible corrosion resistant coating material (base and curing agent) of approved manufacturer over prepared surface, using not less than theoretical consumption as per the manufacturer's specification. Total dry film thickness (DFT) including primer will be 300 - 400 microns.

Note:

1. Before taking up any repair work, the dryness of substrate concrete must be ensured for effective application of several repair materials. Remove oil, grease, wax, Cement laitance, loose particles and other contaminants by shot blasting, scarifying or mechanically wire brushing followed by vacuum cleaning from the substrate concrete.
2. During repair works of Clariflocators-1,2 measures should be taken up in accordance with relevant safety standards and safety guidelines of Occupational safety & Health Administration (OSHA) for construction, arrangement like safety nets/platforms should be done.

.....

g. Chemical Analysis to determine Chloride content, Sulphate content and pH value of Concrete Powder Samples in laboratory.

iii) Analysis and interpretation of test results/data obtained in (i) & (ii) above.

iv) Recommendations on remedial measures using indigenously available compatible repair materials. Preparation of BOQ covering selected items for repair including rate analysis & preparation of specifications and methodology for carrying out effective repair shall also be provided.

v) The report covering (i) to (iv) above.

2.0 DATA PROVIDED BY SPONSOR

- Year of Construction of the subject structure was around 1995.

3.0 INVESTIGATION CARRIED OUT BY NCB

3.1 Visual Observations

To collect the data of distress on RCC members of RCC Chimney Unit#1&2 at **NTPC, Tanda, Uttar Pradesh,** Visual observation survey was carried out jointly by NCB team and the concerned NTPC officials during the visits for condition assessment from 26th March to 01st April 2023.

3.2 Rebound Hammer Testing (RHT) As Per IS: 516 (Part V, Sec-IV) – 2020

Rebound hammer testing technique was used for assessing the likely surface compressive strength of concrete. Basic principle of rebound hammer test is given below.

When the plunger of rebound hammer is pressed against the surface of the concrete, the spring-controlled mass rebounds and the extent of such rebound depends upon the surface hardness of concrete. The surface hardness and therefore the rebound are taken to be related to the compressive strength of the concrete. The rebound is read off along a graduated scale and is designated as the rebound number or rebound index. It is also to be noted that rebound indices are indicative of compressive strength of concrete to a limited depth from the surface. If the concrete in a particular member has internal micro cracking, flaws or heterogeneity across the cross-section, rebound hammer indices will not indicate the same. **IS: 516 (Part V, Sec-IV) – 2020 states,** "*As such, the estimation of strength of concrete by rebound hammer method cannot be held to be very accurate and probable accuracy of prediction of concrete strength in a structure is ±25 percent*." However, the test should only be used as indication of the probable compressive strength of concrete.

The test was carried out using a Schmidt's Rebound Hammer on randomly selected accessible RCC Chimney at **NTPC Tanda, Uttar Pradesh.** The members which were tested were made accessible, so the testing done on accessible RCC members. The surfaces at the chosen locations were thoroughly cleaned with carborandum stone/grinding stone and readings were taken around each point. The average of the readings becomes the rebound index at that point of observation.

3.3 Ultrasonic Pulse Velocity (UPV) Method as per as per IS: 516 (Part V, Sec-I) – 2018.

UPV is a non-destructive evaluation method for assessing the quality of concrete; density, homogeneity and uniformity. Basic principle of UPV method is given below.

In this method, an ultrasonic pulse of longitudinal vibrations is produced by an electro-acoustical transducer which is held in contact with one surface of the concrete member under test. After traversing a known path length of the member, the pulse of vibrations is converted into an electric signal by a second electro-acoustical transducer, and an electric timing circuit enables the transit time of the pulse to be measured, from which the pulse velocity is calculated. For the present investigation, the pulse velocity measurements were obtained by direct transmission of ultrasonic pulses through the concrete, i.e. by "cross probing". For this purpose, the transducers were held on opposite faces of the beam and columns.

The Ultrasonic Pulse Velocity in concrete is mainly related to its density and modulus of elasticity. This in turn depends upon the materials and mix proportions used in making concrete as well as methods of placing, compaction and curing of concrete. If the concrete is not thoroughly compacted, or if there is segregation of concrete during placing or there are internal cracks or flaws, the pulse velocity will be lower, although the same materials and mix proportions are used.

The underlying principle of assessing the quality of concrete from UPV method is that, comparatively higher pulse velocities are obtained when the 'quality' of concrete in terms of density, homogeneity and uniformity is good. In case of concrete of poorer quality, lower velocities are obtained.

On this basis, guidelines have been evolved for characterizing the quality of concrete in structures in terms of ultrasonic pulse velocity. Such guideline is given in Table 25, which is reproduced from **IS: 516 (Part V, Sec-I) – 2018.**

3.4 Concrete Core Testing

Concrete cores of 60-mm diameter were extracted from different structural members identified, to estimate equivalent cube compressive strength of the structure. Equivalent cube strength does not indicate 28 days' standard cube strength rather it represents the in-situ cube strength, and is compared vis-à-vis strength used in design calculation with safety of the structure under load in mind.

There are a number of parameters, which influence the measured compressive strengths. Such parameters include size (diameter) of the specimen, length-to-diameter ratio, direction of drilling, method of capping, drilling operations, moisture conditions of cores at the time of testing etc. Many of these parameters have been standardized.

The second set of variables relates to the intrinsic difference that exists between the concrete in structure and in standard laboratory-controlled specimens, the core specimens representing the former. Such intrinsic differences are due to inherent differences that may occur in mixing constituents, degree of compaction, extent of curing and temperature condition in two cases. The procedure for sampling, preparing, testing and calculating the equivalent compressive strength with corrections are given in **IS: 516-2018.**

The net effect of all these parameters is that the strength of concrete cores is in general lower than those of laboratory controlled specimens, for this reason **IS: 456-2000** (Code of Practice for Plain and Reinforced Concrete) consider that concrete in the area represented by a core test is adequate if" *the average equivalent cube strength of the cores is equal to at least 85 percent of the specified for the corresponding age and if no single core has strength lower than 75 percent of the specified value".*

3.5 Carbonation Test

Carbonation is the formation of calcium carbonate ($CaCO_3$) by chemical reactions in concrete. When CO_2 penetrates into the hardened concrete, it reacts with portlandite [Portlandite is a mineral formed during the curing of concrete, calcium hydroxide $Ca(OH)_2$] in the presence of moisture forming $CaCO_3$. The rate of carbonation depends mainly on the relative humidity, the concentration of CO_2, the penetration pressure and the temperature of the environment where concrete is placed.

As carbon dioxide enters the concrete from the environment, it reacts with calcium hydroxide present in the concrete and depending upon the quality of concrete it reduces the alkalinity of the

pore fluids, depassivating ferric oxide layer on reinforcing bar which in turn initiates the process of corrosion in reinforcement.

To determine the depth of carbonation, concrete is exposed and sprayed with a pH indicator (solutions of 1%phenolphthalein in 70%ethyl alcohol). The demarcation between the region, which turns into magenta (dark pink colour) and the region showing no change in colour indicate the carbonation front.

Carbonation measurements were recorded immediately after the cores specified in col. 3.4 were extracted.

3.6 Half-Cell Potential (HCP) Measurements

This test method covers the estimation of electrical Half Cell Potential of uncoated reinforcing steel, to determine corrosion activity using reference electrode copper; copper sulphate half-cell. It is not possible to expose all the reinforcements in the structural element and observe the extent of corrosion. So, this method has been very convenient to assess the condition of the entire length of a member by exposing a portion of the reinforcement at a suitable location, which measures the half-cell potential on the entire length, by placing the reference electrode on the wet concrete surface.

The Half-Cell Potential measurement is based on the principal of the corrosion, being an electro-chemical process, induces certain voltage to the reinforcement steel that is corroding. The wetting of the concrete is required to make the portion between the concrete surface and the reinforcing bar as electrolytes.

A criterion for assessment for corrosion of steel is given as under **ASTM C-876** below.

- If potentials over an area are more positive than -200 mV, there is a greater than 90% probability that no reinforcing steel corrosion is occurring in that area at the time of measurement.
- If potentials over an area are in the range of -200 mV to -350 mV, corrosion activity of the reinforcing steel in that area is uncertain.
- If potentials over an area are more negative than -350 mV, there is a greater than 90% probability that reinforcing steel corrosion is occurring in that area at the time of measurement.

Adequate numbers of accessible RCC members were selected from various locations to conduct Half-Cell Potential test.

3.7 Concrete Cover Study

Concrete cover depth to reinforcing bars shall be done by using Ferro Scanner instrument on safe & accessible locations. This instrument detects the reinforcing bars and mesh, to measure their cover depth and determine the bar diameter. The instrument is based on the magnetic technique and is calibrated for different purposes. The cover depth is important from the point of view of estimation of initiation of corrosion of reinforcing bars.

For a longitudinal reinforcing bar in a Column nominal cover shall in any case not be less than 40mm or less than the diameter of such bar as per clause 26.4.2.1 of IS: 456-2000. Nominal cover to meet durability requirement for footing, minimum cover shall be 50mm as per clause 26.4.2.2 of IS: 456-2000.

Minimum values of nominal cover of normal weight aggregate concrete to be provided to all reinforcement including links to meet specified period of fire resistance shall be as per Table 16A of IS:456-2000.

Minimum values for the nominal cover of normal weight aggregate concrete which should be provided all reinforcement including links depending of exposure condition shall be as per the Table 5 of IS: 456-2000.

3.8 Chemical Analysis

Corrosion of reinforcing steel due to chlorides in concrete is one of the most common environmental attacks that lead to deterioration of concrete structures. Whenever there is chloride in concrete there is an increased risk of corrosion of embedded metal. Chloride content is then expressed in kg per cubic meter of concrete and compared with the values of limits of chloride contents of concrete (**Table 7 of IS: 456–2000**).

Sulphates (SO_3) are present in most cements and in some aggregates; excessive amounts of water-soluble sulphate from these or other mix constituents can cause expansion and disruption of concrete. To prevent it, **IS: 456-2000 clause-8.2.5.3** states that the total water-soluble sulphate content of the concrete mix, expressed as SO_3, should not exceed 4 percent by mass of the cement in the mix. The sulphate content should be calculated as the total from the various constituents of the mix.

The pH value of the concrete should be above 11.5 to maintain alkalinity of concrete surrounding the embedded steel. A reduction in the pH value of concrete indicates loss of passive layer around the reinforcement which protects the steel from distress.

For analyzing Chloride content and pH of concrete, concrete powder samples were extracted from 0-25mm, 25-50mm depths at identified locations and then tested as per IS:14959(Part 2) -2001 (Determination of water soluble and acid soluble Chlorides in Mortar and Concrete – Method of Test).

Adequate numbers of accessible RCC members were selected from various locations to extract concrete powders for chemical test.

4.0 RESULTS AND DISCUSSION

4.1. Visual Observations

The height of the RCC chimney of Unit- is 120m. Visual observations and testing carried out at 1.5m, 10m, 18m, 100m height. Distress, Signs of cracks, spalling of concrete and exposure of reinforcement observed on the chimney at different heights. Distress and Honey comb observed at a few locations of Interior and exterior walls. The visual observations and photographs are shown Annexure 1.

4.2. Rebound Hammer Testing

Rebound Hammer testing was carried out on various identified RCC (Reinforced Cement Concrete) members of Chimney (up to 120 m) using random sampling technique, The results of surface compressive strength obtained by Rebound Hammer testing are given in Table 2 to 21**.** Surface Compressive strength results of concrete as obtained on different hardened concrete surfaces of RCC Members are summarized as:

1) Surface compressive strength of concrete obtained on Chimney wall, S-E, Out Side at 1.5m level by Rebound Hammer Testing is found to vary from **38.26 N/mm^2 to 42.79 N/mm^2** with an average surface compressive strength of **40.81 N/mm^2** (Refer Table 2).
2) Surface compressive strength of concrete obtained on Chimney wall, S-W, Inside at 1.5 m level by Rebound Hammer Testing is found to vary from **39.39 N/mm^2 to 42.79 N/mm^2** with an average surface compressive strength of **40.67 N/mm^2** (Refer Table 3).

3) Surface compressive strength of concrete obtained on Chimney wall, N-W, north, inside at 1.5 m level by Rebound Hammer Testing is found to vary from **36.56 N/mm^2 to 42.22 N/mm^2** with an average surface compressive strength **39.96 N/mm^2** (Refer Table 4).

4) Surface compressive strength of concrete obtained on Chimney wall, N-W, outside at 1.5 m level by Rebound Hammer Testing is found to vary from **38.83 N/mm^2 to 42.79 N/mm^2** with an average surface compressive strength of **41.09 N/mm^2** (Refer Table 5).

5) Surface compressive strength of concrete obtained on Chimney wall, East side Near stack yard, Outside at 1.5 m level by Rebound Hammer Testing is found to vary from **36.56 N/mm^2 to 39.96 N/mm^2** with an average surface compressive strength of **38.97 N/mm^2** (Refer Table 6).

6) Surface compressive strength of concrete obtained on Chimney wall, N-E, outside at 1.5 m level by Rebound Hammer Testing is found to vary from **39.96 N/mm^2 to 42.22 N/mm^2** with an average surface compressive strength of **40.81 N/mm^2** (Refer Table 7).

7) Surface compressive strength of concrete obtained on Chimney wall, South side, outside at 1.5 m level Rebound Hammer Testing is found to vary from **39.39 N/mm^2 to 42.22 N/mm^2** with an average surface compressive strength of **40.67 N/mm^2** (Refer Table 8).

8) Surface compressive strength of concrete obtained on Chimney wall, N-E, outside at 1.5 m level by Rebound Hammer Testing is found to vary from **36.56 N/mm^2 to 42.22 N/mm^2** with an average surface compressive strength of **39.54 N/mm^2** (Refer Table 9).

9) Surface compressive strength of concrete obtained on Chimney wall, North side, outside at 1.5 m level by Rebound Hammer Testing is found to vary from **37.70 N/mm^2 to 41.66N/mm^2** with an average surface compressive strength of **39.68 N/mm^2** (Refer Table 10).

10) Surface compressive strength of concrete obtained on Chimney wall, N-W, Out Side at 1.5 m level by Rebound Hammer Testing is found to vary from **38.26 N/mm^2 to 42.22 N/mm^2** with an average surface compressive strength of **40.24 N/mm^2** (Refer Table 11).

11) Surface compressive strength of concrete obtained on Chimney wall, S-E, outside at 10m level by Rebound Hammer Testing is found to vary from **39.39 N/mm^2 to 42.22 N/mm^2** with an average surface compressive strength of **40.67 N/mm^2** (Refer Table 12).

12) Surface compressive strength of concrete obtained on Chimney wall, N-W, outside at 10 m level by Rebound Hammer Testing is found to vary from **39.39 N/mm^2 to 43.36 N/mm^2** with an average surface compressive strength of **41.23 N/mm^2** (Refer Table 13).

13) Surface compressive strength of concrete obtained on Chimney wall, South side, outside at 10 m level by Rebound Hammer Testing is found to vary from **39.39 N/mm^2 to 41.66 N/mm^2** with an average surface compressive strength of **40.67 N/mm^2** (Refer Table 14).

14) Surface compressive strength of concrete obtained on Chimney wall, North side, outside at 10 m level by Rebound Hammer Testing is found to vary from **37.70 N/mm^2 to 40.53N/mm^2**with an average surface compressive strength of **39.11 N/mm^2** (Refer Table 15).

15) Surface compressive strength of concrete obtained on Chimney wall, S-E, outside at 10 m level by Rebound Hammer Testing is found to vary from **38.83 N/mm^2 to 40.53 N/mm^2** with an average surface compressive strength of **39.68 N/mm^2** (Refer Table 16).

16) Surface compressive strength of concrete obtained on Chimney wall, West side, Outside at 18 m level by Rebound Hammer Testing is found to vary from **38.83 N/mm^2 to 40.53N/mm^2** with an average surface compressive strength of **39.82 N/mm^2** (Refer Table 17).

17) Surface compressive strength of concrete obtained on Chimney wall, South side, outside at 18m level by Rebound Hammer Testing is found to vary from **39.39N/mm^2 to 41.66N/mm^2** with an average surface compressive strength of **40.24 N/mm^2** (Refer Table 18).

18) Surface compressive strength of concrete obtained on Chimney wall, East side, Outside at 18m level by Rebound Hammer Testing is found to vary from **39.39 N/mm^2 to 42.22 N/mm^2** with an average surface compressive strength of **41.09 N/mm^2** (Refer Table 19).

19) Surface compressive strength of concrete obtained on Chimney wall, West side, Outside at 18m level by Rebound Hammer Testing is found to vary from **39.96 N/mm^2 to 41.09 N/mm^2** with an average surface compressive strength of **40.67 N/mm^2** (Refer Table 20).

20) Surface compressive strength of concrete obtained on Chimney wall, N-W, outside at 18m level by Rebound Hammer Testing is found to vary from **38.83 N/mm^2 to 40.53 N/mm^2** with an average surface compressive strength of **39.54 N/mm^2** (Refer Table 21).

4.3 Ultrasonic Pulse Velocity Testing (UPV):

The **Ultrasonic Pulse Velocity** testing was conducted on RCC Chimney in the presence of concerned engineering team of NTPC. The results of the UPV values obtained on various RCC members are as follows:

1) The UPV measurements were taken using Surface probing technique on the Chimney wall, S-E, Out Side at 1.5 m level are in the range of **4.05 to 4.33km/sec**. When these values are

compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 23), the overall quality of concrete is assessed to be **GOOD** (Table - 22).

2) The UPV measurements were taken using surface probing technique on the Chimney wall, S-W, Inside at 1.5 m level are in the range of **4.05 to 4.32km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 24), the overall quality of concrete is assessed to be **GOOD** (Table - 22).
3) The UPV measurements were taken using Surface probing technique on the Chimney wall, N-W, north, inside at 1.5 m level are in the range of **3.89 to 4.34km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 25), the overall quality of concrete is assessed to be **GOOD** (Table - 22).
4) The UPV measurements were taken using cross probing technique on the Chimney wall, Entrance at 1.5 m level are in the range of **3.94 to 4.14km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 26), the overall quality of concrete is assessed to be **GOOD** (Table - 22).
5) The UPV measurements were taken using Surface probing technique on the Chimney wall, East side near stack yard, Outside at 1.5 m level is in the range of **3.96 to 4.31km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table - 22).
6) The UPV measurements were taken using Surface probing technique on the Chimney wall, N-E, Outside at 1.5 m level is in the range of **3.97to 4.26km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 28), the overall quality of concrete is assessed to be **GOOD** (Table - 22).
7) The UPV measurements were taken using Surface probing technique on the Chimney wall, South side, outside at 1.5 m level are in the range of **4.04 to 4.34km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 29), the overall quality of concrete is assessed to be **GOOD** (Table - 22).
8) The UPV measurements were taken using Surface probing technique on the Chimney wall, N-E, Outside at 1.5 m level is in the range of **3.94 to 4.35km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 30), the overall quality of concrete is assessed to be **GOOD** (Table - 22).

9) The UPV measurements were taken using surface probing technique on the Chimney wall, North side, outside at 1.5 m level is in the range of **3.93 to 4.29km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 31), the overall quality of concrete is assessed to be **GOOD** (Table - 22).

10) The UPV measurements were taken using surface probing technique on the Chimney wall, N-W, Out Side at 1.5 m level is in the range of **3.91to 4.06km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 32), the overall quality of concrete is assessed to be **GOOD** (Table - 22).

11) The UPV measurements were taken using surface probing technique on the Chimney wall, S-E, Outside at 10m level are in the range of **3.96 to 4.22km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 33), the overall quality of concrete is assessed to be **GOOD** (Table - 22).

12) The UPV measurements were taken using surface probing technique on the Chimney wall, N-W, Outside at 10m level are in the range of **3.92 to 4.29km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 34), the overall quality of concrete is assessed to be **GOOD** (Table - 22).

13) The UPV measurements were taken using surface probing technique on the Chimney wall, South side, Outside at 10m level are in the range of **4.01to 4.23km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 35), the overall quality of concrete is assessed to be **GOOD** (Table - 22).

14) The UPV measurements were taken using surface probing technique on the Chimney wall, North side, outside at 10m level are in the range of **3.96 to 4.26km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 36), the overall quality of concrete is assessed to be **GOOD** (Table - 22).

15) The UPV measurements were taken using surface probing technique on the Chimney wall, S-E, Outside at 10m level are in the range of **3.94 to 4.26km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 37), the overall quality of concrete is assessed to be **GOOD** (Table - 22).

16) The UPV measurements were taken using surface probing technique on the Chimney wall, West side, Outside at 18 m level are in the range of **4.13 to 4.28km/sec**. When these values

are compared with the velocity criteria of IS: 516(Part V) – 2018 (Also reproduced in Table 38), the overall quality of concrete is assessed to be **GOOD** (Table - 22).

17) The UPV measurements were taken using surface probing technique on the Chimney wall, South side, outside at 18 m level are in the range of **3.94 to 4.25km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 39), the overall quality of concrete is assessed to be **GOOD** (Table - 22).

18) The UPV measurements were taken using surface probing technique on the Chimney wall, East side, Outside at 18 m level are in the range of **4.04 to 4.29km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 40), the overall quality of concrete is assessed to be **GOOD** (Table - 22).

19) The UPV measurements were taken using surface probing technique on the Chimney wall, West side, Outside at 18 m level are in the range of **3.94 to 4.29km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 41), the overall quality of concrete is assessed to be **GOOD** (Table - 22).

20) The UPV measurements were taken using surface probing technique on the Chimney wall, N-W, Outside at 18m level are in the range of **3.97to 4.25km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 42), the overall quality of concrete is assessed to be **GOOD** (Table - 22).

4.4 Concrete Core Testing

Corresponding to the 60mm concrete core extracted by random sampling technique covering different locations of Chimney UNIT #1&2 in NTPC Tanda and tested at NCB laboratory Hyderabad, the equivalent cube compressive strength of concrete of RCC Chimney are shown in Table 46. In total, 15 concrete cores were extracted from different members of the RCC Chimney.

The test results indicate that the equivalent cube compressive strength values for

1. RCC Chimney wall, S-E, Out Side at 1.5 m level is found to 30.65 N/mm^2
2. RCC Chimney wall, S-W, Inside at 1.5 m level is found to 34.08 N/mm^2
3. RCC Chimney wall, N-W, north, inside at 1.5 m level is found to 29.26 N/mm^2
4. RCC Chimney wall, N-W, Outside at 1.5 m level is found to 27.84 N/mm^2
5. RCC Chimney wall, Eastside Near stack yard, Outside at 1.5m level is found to 26.01 N/mm^2
6. RCC Chimney wall, East , N-E, Outside at 1.5 m level is found to 28.83 N/mm^2

7. RCC Chimney wall, North side, Outside at 1.5 m level is found to 25.20 N/mm^2
8. RCC Chimney wall, South side, Outside at 1.5 m level is found to 31.86 N/mm^2
9. RCC Chimney wall, S-E, Outside at 10m level is found to 26.48 N/mm^2
10. RCC Chimney wall, N-W, Outside at 10 m level is found to 21.64 N/mm^2
11. RCC Chimney wall, , South side, Outside at 10 m level is found to 29.01 N/mm^2
12. RCC Chimney wall, North side, outside at 10 m level is found to 30.35 N/mm^2
13. RCC Chimney wall, West side, Outside at 18 m level is found to 27.93 N/mm^2
14. RCC Chimney wall, South side, Outside at 18 m level is found to 27.41 N/mm^2
15. RCC Chimney wall, East side, Outside at 18 m level is found to 29.31 N/mm^2

In total, 15 nos. tested cores all of them found to have equivalent cube compressive strength more than specified characteristic compressive strength of M25 grade concrete (which is reproduced in Table 46).

4.5 Concrete Cover

The concrete cover depth to rebars in RCC members is measured with Ferro-scanner and a measuring tape/scale in the places where concrete is exposed and accessible for direct measurement. Nominal cover to reinforcement to meet durability requirement is given in **IS-456: Table 16-clause 26.4.2**, the measured cover to reinforcement steel in the selected RCC members are given in Table 44**.**

1. The Concrete cover to Reinforcing bars of RCC Chimney wall, S-E, Out Side at 1.5 m level during testing using Ferro scanner meter is found to vary from **68mm–78mm** (average **72 mm**)
2. The Concrete cover to Reinforcing bars of RCC Chimney wall, S-W, Inside at 1.5 m level during testing using Ferro scanner meter is found to vary from **62mm–76mm** (average **70 mm**)
3. The Concrete cover to Reinforcing bars of RCC Chimney wall, N-W, north, inside at 1.5 m level during testing using Ferro scanner meter is found to vary from **66mm–72mm** (average **70 mm**)

4. The Concrete cover to Reinforcing bars of RCC Chimney wall, N-W, Outside at 1.5 m level during testing using Ferro scanner meter is found to vary from **66mm–72mm** (average **69 mm**)
5. The Concrete cover to Reinforcing bars of RCC Chimney wall, East side Near stack yard, Outside at 1.5 m level during testing using Ferro scanner meter is found to vary from **64mm–72mm** (average **68 mm**)
6. The Concrete cover to Reinforcing bars of RCC Chimney wall, N-E, Outside at 1.5 m level during testing using Ferro scanner meter is found to vary from **68mm–74mm** (average **69 mm**)
7. The Concrete cover to Reinforcing bars of RCC Chimney wall, North side, Outside at 1.5 m level during testing using Ferro scanner meter is found to vary from **68mm–74mm** (average **71 mm**)
8. The Concrete cover to Reinforcing bars of RCC Chimney wall, South side, Outside at 1.5 m level during testing using Ferro scanner meter is found to vary from **66mm–74mm** (average **70 mm**)
9. The Concrete cover to Reinforcing bars of RCC Chimney wall, S-E, Outside at 10m level during testing using Ferro scanner meter is found to vary from **66mm–74mm** (average **70 mm**)
10. The Concrete cover to Reinforcing bars of RCC Chimney wall, N-W, Outside at 10 m level during testing using Ferro scanner meter is found to vary from **66mm–72mm** (average **69 mm**)
11. The Concrete cover to Reinforcing bars of RCC Chimney wall, South side, Outside at 10 m level during testing using Ferro scanner meter is found to vary from **70mm–76mm** (average **72 mm**)
12. The Concrete cover to Reinforcing bars of RCC Chimney wall, North side, outside at 10 m level during testing using Ferro scanner meter is found to vary from **68mm–72mm** (average **71 mm**)
13. The Concrete cover to Reinforcing bars of RCC Chimney wall, West side, Outside at 18 m level during testing using Ferro scanner meter is found to vary from **68mm–74mm** (average **71 mm**)

14. The Concrete cover to Reinforcing bars of RCC Chimney wall, South side, Outside at 18 m level during testing using Ferro scanner meter is found to vary from **68mm–74mm** (average **70 mm**)
15. The Concrete cover to Reinforcing bars of RCC Chimney wall, East side, Outside at 18 m level during testing using Ferro scanner meter is found to vary from **68mm–74mm** (average **71 mm**)

The Concrete cover within the specified limits to meet durability requirement as per IS: 456-2000 (Refer Table 16 of IS: 456-2000) which is Reproduced in Table 43

4.6 Carbonation

Table- 45 shows test results of carbonation testing done on 15 no. Concrete Cores extracted from various representative concrete samples. The results indicate that the values of depth of carbonation in all different locations of RCC Chimney are varying from **0-8 mm.**

Based on the above carbonation study carried on different selected RCC members at several locations the carbonation depth is found to be within the concrete cover region.

4.7 Half-Cell Potential Test

Half-cell potential (HCP) measurements using copper, copper-sulfate half-cell technique as per ASTM C-876 (Standard test method for corrosion potentials of uncoated reinforcing steel in concrete) were taken at site to ascertain corrosion status of reinforcing bars of various locations of RCC Chimney unit #1&2 NTPC Tanda. The measurements were done on different locations randomly selected locations and comprising of representative samples for the structure.

Test results (refer Table- 48) when compared with the corrosion criteria as per ASTM C-876 (Table-47) indicate that probability of corrosion is found to be in “Transit State”.

4.8 Chemical Analysis

The chemical analysis of water and powdered samples extracted from different elements of RCC Chimney collecting by random sampling technique. This covered chloride content, sulphate content per cum of concrete as well pH value of powdered samples. The test results as obtained in NCB laboratory are shown in Table- 49. Analysis of interpretation of test results given as under:

1) Based on the results obtained from laboratory the range of chloride content in the Chimney wall, S-E, Out Side at 1.5 m level was found to vary from 0.216 kg/m^3 to 0.192 kg/m^3 with an average value of **0.204 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content is found to be vary from 2.48% to 2.36% by mass of the cement in mix with an average of **2.42%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found to vary from 11.34 to 11.28 with an average of **11.31** which is less than the specified limit to resist the corrosion.

2) Based on the results obtained from laboratory the range of chloride content in the Chimney wall, S-W, Inside at 1.5 m level was found to vary from 0.192 kg/m^3 to 0.216 kg/m^3 with an average value of **0.204 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content is found to be vary from 2.08% to 2.16% by mass of the cement in mix with an average of **2.12%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found to vary from 11.32 to 11.08 with an average of **11.20** which is less than the specified limit to resist the corrosion.

3) Based on the results obtained from laboratory the range of chloride content in the Chimney wall, N-W, north, inside at 1.5 m level was found to vary from 0.192 kg/m^3 to 0.168 kg/m^3 with an average value of **0.18 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content is found to be vary from 2.32% to 2.72% by mass of the cement in mix with an average of **2.52%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found to vary from 11.20 to 11.06 with an average of **11.13** which is less than the specified limit to resist the corrosion.

4) Based on the results obtained from laboratory the range of chloride content in the Chimney wall, N-W, Outside at 1.5 m level was found to vary from 0.192 kg/m^3 to 0.120 kg/m^3 with an average value of **0.156 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content is found to be vary from 2.56% to 2.64% by mass of the cement in mix with an average of **2.60%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found to vary from 11.10 to 11.30 with an average of **11.20** which is less than the specified limit to resist the corrosion.

5) Based on the results obtained from laboratory the range of chloride content in the Chimney wall, East side Near stack yard, Outside at 1.5 m level was found to vary from 0.192 kg/m^3 to 0.144 kg/m^3 with an average value of **0.168 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content is found to be vary from 2.72% to 2.48% by mass of the cement in mix with an average of **2.60%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found to vary from 11.25 to 11.36 with an average of **11.30** which is less than the specified limit to resist the corrosion.

6) Based on the results obtained from laboratory the range of chloride content in the Chimney wall, N-E, Outside at 1.5 m level was found to vary from 0.216 kg/m^3 to 0.192 kg/m^3 with an average value of **0.204 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content is found to be vary from 2.24% to 2.64% by mass of the cement in mix with an average of **2.44%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found to vary from 11.32 to 11.42 with an average of **11.37** which is less than the specified limit to resist the corrosion.

7) Based on the results obtained from laboratory the range of chloride content in the Chimney wall, N-W, Outside at 10 m level was found to vary from 0.192 kg/m^3 to 0.168 kg/m^3 with an average value of **0.180 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content is found to be vary from 2.16% to 2.48% by mass of the cement in mix with an average of **2.32%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found to vary from 11.46 to 11.38 with an average of **11.42** which is less than the specified limit to resist the corrosion.

8) Based on the results obtained from laboratory the range of chloride content in the Chimney wall, South side, Outside at 10 m level was found to vary from 0.216 kg/m^3 to 0.192 kg/m^3 with an average value of **0.204 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content is found to be vary from 2.24% to 2.28% by mass of the cement in mix with an average of **2.26%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found to vary from 11.28 to 11.36 with an average of **11.32** which is less than the specified limit to resist the corrosion.

9) Based on the results obtained from laboratory the range of chloride content in the Chimney wall, West side, Outside at 18m level was found to vary from 0.168 kg/m^3 to 0.216 kg/m^3 with an average value of **0.192 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content is found to be vary from 2.72% to 2.48% by mass of the cement in mix with an average of **2.60%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found to vary from 11.24 to 11.32 with an average of **11.28** which is less than the specified limit to resist the corrosion.

10) Based on the results obtained from laboratory the range of chloride content in the Chimney wall, East side, Outside at 18 m level was found to vary from 0.096 kg/m^3 to 0.168 kg/m^3 with an average value of **0.132 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content is found to be vary from 2.72% to 2.24% by mass of the cement in mix with an average of **2.48%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value is found to vary from 11.06 to 11.20 with an average of **11.13** which is less than the specified limit to resist the corrosion.

5.0 Conclusions:

The following Conclusions can be broadly made from the testing results:

i) Based on Ultrasonic Pulse Velocity, Rebound Hammer testing & Core testing done on representative samples (random sampling technique) on RCC members, the results have given Good quality of concrete. The compressive strength of the samples extracted from the Chimney is found meeting the required limit for M25 Grade of concrete. Also, distress in the form of cracks, spalling of concrete and exposure of reinforcing rebar in some locations of RCC Chimney due to some issues which cannot be overlooked.

ii) Based on the Half-Cell potential measurements done by random sampling technique at various locations and visual observations of RCC Chimney given an initiation signal of corrosion and indicate that probability of corrosion is found to be in “Transit State”. Carbonation is found 0-8 mm after 25 years’ exposure to existing environment where as concrete cover of RCC members are found to vary from 68 – 72 mm.

iii) The amount of Soluble Sulphates in the concrete of RCC members is within the specified limits and chloride content in the concrete is also within the specified limit and pH values are lower than the specified limit in all RCC members.

iv) The chemical test results of water sample shows that the Organic matter, Sulphate content, Chloride content, Inorganic content and pH value are within the permissible limits pH value are lower than the specified limit in all RCC members as per (IS:456-2000& IS: 3025 -1984).

6.0 Recommendations

The following steps shall be taken to repair the cracks & strengthening of RCC Chimney:

Part I: <u>Providing Total Platform system (Scaffolding):</u>

Providing and fixing double scaffolding system (cup lock type) on the exterior side, up to seven story height made with 40 mm diameter M.S. tube 1.5 m centre to centre, horizontal & vertical tubes joining with cup & lock system with M.S. tubes, M.S. tube challies, M.S.clamps and M.S. staircase system in the scaffolding for working platform etc. and maintaining it in a serviceable condition for the required duration as approved and removing it thereafter. The scaffolding system shall be stiffened with bracings, runners, connection with the building etc wherever required for inspection of work at required locations with essential safety features for the workmen etc. complete as per directions and approval of Engineer in- In charge .The elevational area of the scaffolding shall be measured for payment purpose .The payment will be made once irrespective of duration of scaffolding.

Part-II: Repair and Strengthening:

i) <u>Chipping:</u> Cover concrete around the horizontal, vertical cracks & spalling of concrete shall be chipping off to the depth up to 40mm on RCC walls. The chipping in the spalled portion of the Shells and RCC Walls shall be limited up to the cover region. Chipping of loose/hollow sounding concrete can be done by striking the doubtful surfaces with 2 lb hammer**.**

ii) <u>Treatment for Cracks:</u>

- Filling of Cracks: The cracks/voids are to be widened by cutting V-grooves of 10mm x 10mm size and sealed with approved epoxy repair mortar**.**

- After the sealing, 12mm dia galvanized steel injection nipples are to be inserted in the crack area and also wherever honeycombing is found by drilling holes of required diameter up to the depth of 60 – 120 mm at required spacing (generally 350 mm staggered spacing). The drilled holes must be made dust free by blowing compressed air and should be sealed after the insertion of the nozzle with approved adhesive and allowed to cure.
- After the nipples are injected and cured, grouting in the proportion recommended by the manufacturer into the cracks/honeycombed area of concrete/masonry shall be done using suitable gun/pump at required pressure. Once the grouting work is finished, the extruding nipples can be cut-off after the curing period.

iii) <u>Reinforcement Corrosion Treatment:</u> Wherever reinforcing rebar is found corroded in RCC walls

a) Remove the rust by manually or suitable means to make corroded reinforcing bars rust free.

b) Provide and apply corrosion protection using 2 coats of anticorrosive Zn rich epoxy phenolic rebar protection system of approved brand on the exposed old reinforcement by brush with interval of 24 hours between coats and corrosion protection of exposed old reinforcing bars.

c) Provide and apply concrete penetrating corrosion inhibitor (CPCI) of approved brand over the entire finished surface are obtained after removal of distressed concrete in 2 coats @ of $4m^2$/ltr/coat approximately.

iv) <u>Bond Coat:</u> After chipping off the concrete cover, provide and apply structural grade two component epoxy bond coat prior to application of any type of mortar conforming to ASTM C - 881 -13 Type - II tested as per ASTM C –882-13 to ensure bond between old and new concrete by brush application. (Material manufacture from STP/BASF/SIKA/FOSRAC/KRISHNA Conchem/Pidilite or equivalent)

v) <u>Making up lost section with Polymer Modified Mortar (PMM):</u> For repair of patches having, apply average 40mm PMM in 2-3 layers using SBR Latex conforming to ASTM C-1059-13 Type-I in damaged areas (1 Cement-3 part graded cleaned river sand + 20 % latex by weight of cement) with 0.35 w/c ratio, in 10-15 mm thick layers by applying bond coat between successive/each. (Material manufacture either from STP/BASF/SIKA/FOSRAC or equivalent)

vi) <u>Protective coating:</u> Before applying the protective coating on RCC walls and the outer wall surface shall be cleaned by scrubbing with hard steel brush to remove loose particles, disintegrated concrete, deposited smoke and dust particles etc. The scrubbed surface is cleaned by air blowing and then dries it completely. Apply a silane siloxane priming coat as primer compatible to substrate (Cementitious). Over it, applying two or more coats of ready mixed anti carbonation UV resistant acrylic polymer-based water proofing coatings (having minimum 60% solid content) with broad brush or roller over prepared surface, using not less than theoretical Consumption as per the manufacturer's specification and direction of Engineer - In - Charge (time gap between two coats of coating shall be not less than 8 hrs). Total dry film thickness (DFT) including primer will be 225 - 240 microns.

vi) For the top 15m part of the chimney, providing protective coating, in signal red and white bands (2 bands) with contractor's supply of Epoxy-phenolic IP Net paints including priming coat, intermediate coat and polyurethane top coat with paints from approved firms after surface preparation. Total dry film thickness (DFT) including primer will be 185 - 215 microns, all complete as per direction of Engineer-In-Charge.

Note:

1. Before taking up any repair work, the dryness of substrate concrete must be ensured for effective application of several repair materials. Remove oil, grease, wax, Cement laitance, loose particles and other contaminants, scarifying or mechanically wire brushing followed by air jet from the substrate concrete.
2. During repair works of chimney measures should be taken up in accordance with relevant safety standards and safety guidelines of Occupational safety & Health Administration (OSHA) for construction, arrangement like safety nets/platforms should be done.
3. The extraction of concrete cores, chemical analysis samples and other tests shall be carried out up to height wherever safe access is provided as taking the equipment for the extraction of concrete cores at higher reaches would not be possible due to very less width of the platforms available at different heights.

.....

g. Chemical Analysis to determine Chloride content, Sulphate content and pH value of Concrete Powder Samples in laboratory.

iii) Analysis and interpretation of test results/data obtained in (i) & (ii) above.

iv) Recommendations on remedial measures using indigenously available compatible repair materials. Preparation of BOQ covering selected items for repair including rate analysis & preparation of specifications and methodology for carrying out effective repair shall also be provided.

v) The report covering (i) to (iv) above.

2.0 DATA PROVIDED BY SPONSOR

- Year of Construction of the subject structure was around 1988.

3.0 INVESTIGATION CARRIED OUT BY NCB

3.1 Visual Observations

To collect the data of distress on members of TG Unit#1 at NTPC, Tanda. Visual observation survey was carried out jointly by NCB team and the concerned NTPC officials during the visits for condition assessment from 08th May 2023 to 17th May 2023.

3.2 Rebound Hammer Testing (RHT) As Per IS: 516-2020 (Part-V, Sec-IV).

Rebound hammer testing technique was used for assessing the likely surface compressive strength of concrete. Basic principle of rebound hammer test is given below.

When the plunger of rebound hammer is pressed against the surface of the concrete, the spring-controlled mass rebounds and the extent of such rebound depends upon the surface hardness of concrete. The surface hardness and therefore the rebound are taken to be related to the compressive strength of the concrete. The rebound is read off along a graduated scale and is designated as the rebound number or rebound index. It is also to be noted that rebound indices are indicative of compressive strength of concrete to a limited depth from the surface. If the concrete in a particular member has internal micro cracking, flaws or heterogeneity across the cross-section, rebound hammer indices will not indicate the same. **IS: 516(Part 5)-2020 Section 4 states,** "*As such, the estimation of strength of concrete by rebound hammer method cannot be held to be very accurate and probable accuracy of prediction of concrete strength in a structure is ±25 percent*." However, the test should only be used as indication of the probable compressive strength of concrete.

The test was carried out using a Schmidt's Rebound Hammer on randomly selected accessible TG Unit#1 at NTPC, Tanda**.** The members which were tested were made accessible, so the testing done on accessible members. The surfaces at the chosen locations were thoroughly cleaned with carborandum stone/grinding stone and readings were taken around each point. The average of the readings becomes the rebound index at that point of observation.

3.3 Ultrasonic Pulse Velocity (UPV) Method as per IS: 516 (Part V) – 2018.

UPV is a non-destructive evaluation method for assessing the quality of concrete; density, homogeneity and uniformity. Basic principle of UPV method is given below.

In this method, an ultrasonic pulse of longitudinal vibrations is produced by an electro-acoustical transducer which is held in contact with one surface of the concrete member under test. After traversing a known path length of the member, the pulse of vibrations is converted into an electric signal by a second electro-acoustical transducer, and an electric timing circuit enables the transit time of the pulse to be measured, from which the pulse velocity is calculated. For the present investigation, the pulse velocity measurements were obtained by direct transmission of ultrasonic pulses through the concrete, i.e. by "cross probing". For this purpose, the transducers were held on opposite faces of the beam and columns.

The Ultrasonic Pulse Velocity in concrete is mainly related to its density and modulus of elasticity. This in turn depends upon the materials and mix proportions used in making concrete as well as methods of placing, compaction and curing of concrete. If the concrete is not thoroughly compacted, or if there is segregation of concrete during placing or there are internal cracks or flaws, the pulse velocity will be lower, although the same materials and mix proportions are used.

The underlying principle of assessing the quality of concrete from UPV method is that, comparatively higher pulse velocities are obtained when the 'quality' of concrete in terms of density, homogeneity and uniformity is good. In case of concrete of poorer quality, lower velocities are obtained.

On this basis, guidelines have been evolved for characterizing the quality of concrete in structures in terms of ultrasonic pulse velocity. Such guidelines reproduced from **IS: 516 (Part V) – 2018.**

3.4 Concrete Core Testing

Concrete cores of 60-mm diameter were extracted from different structural members identified, to estimate equivalent cube compressive strength of the structure. Equivalent cube strength does not indicate 28 days' standard cube strength rather it represents the in-situ cube strength, and is compared vis-à-vis strength used in design calculation with safety of the structure under load in mind.

There are a number of parameters, which influence the measured compressive strengths. Such parameters include size (diameter) of the specimen, length-to-diameter ratio, direction of drilling, method of capping, drilling operations, moisture conditions of cores at the time of testing etc. Many of these parameters have been standardized.

The second set of variables relates to the intrinsic difference that exists between the concrete in structure and in standard laboratory-controlled specimens, the core specimens representing the former. Such intrinsic differences are due to inherent differences that may occur in mixing constituents, degree of compaction, extent of curing and temperature condition in two cases. The procedure for sampling, preparing, testing and calculating the equivalent compressive strength with corrections are given in **IS: 516-2018.**

The net effect of all these parameters is that the strength of concrete cores is in general lower than those of laboratory controlled specimens, for this reason **IS: 456-2000** (Code of Practice for Plain and Reinforced Concrete) consider that concrete in the area represented by a core test is adequate if" *the average equivalent cube strength of the cores is equal to at least 85 percent of the specified for the corresponding age and if no single core has strength lower than 75 percent of the specified value".*

3.5 Carbonation Test

Carbonation is the formation of calcium carbonate ($CaCO_3$) by chemical reactions in concrete. When CO_2 penetrates into the hardened concrete, it reacts with portlandite [Portlandite is a mineral formed during the curing of concrete, calcium hydroxide $Ca(OH)_2$] in the presence of moisture forming $CaCO_3$. The rate of carbonation depends mainly on the relative humidity, the concentration of CO_2, the penetration pressure and the temperature of the environment where concrete is placed.

As carbon dioxide enters the concrete from the environment, it reacts with calcium hydroxide present in the concrete and depending upon the quality of concrete it reduces the

alkalinity of the pore fluids, depassivating ferric oxide layer on reinforcing bar which in turn initiates the process of corrosion in reinforcement.

To determine the depth of carbonation, concrete is exposed and sprayed with a pH indicator (solutions of 1% phenolphthalein in 70% ethyl alcohol). The demarcation between the region, which turns into magenta (dark pink colour) and the region showing no change in colour indicate the carbonation front.

Carbonation measurements were recorded immediately after the cores specified in col. 3.4 were extracted.

3.6 Half-Cell Potential (HCP) Measurements

This test method covers the estimation of electrical Half Cell Potential of uncoated reinforcing steel, to determine corrosion activity using reference electrode copper; copper sulphate half-cell. It is not possible to expose all the reinforcements in the structural element and observe the extent of corrosion. So, this method has been very convenient to assess the condition of the entire length of a member by exposing a portion of the reinforcement at a suitable location, which measures the half-cell potential on the entire length, by placing the reference electrode on the wet concrete surface.

The Half-Cell Potential measurement is based on the principal of the corrosion, being an electro-chemical process, induces certain voltage to the reinforcement steel that is corroding. The wetting of the concrete is required to make the portion between the concrete surface and the reinforcing bar as electrolytes.

A criterion for assessment for corrosion of steel is given as under **ASTM C-876** below.

- If potentials over an area are more positive than -200 mV, there is a greater than 90% probability that no reinforcing steel corrosion is occurring in that area at the time of measurement.
- If potentials over an area are in the range of -200 mV to -350 mV, corrosion activity of the reinforcing steel in that area is uncertain.
- If potentials over an area are more negative than -350 mV, there is a greater than 90% probability that reinforcing steel corrosion is occurring in that area at the time of measurement.

Adequate numbers of accessible members were selected from various locations to conduct Half-Cell Potential test.

3.7 Concrete Cover Study

Concrete cover depth to reinforcing bars shall be done by using Ferro Scanner instrument on safe & accessible locations. This instrument detects the reinforcing bars and mesh, to measure their cover depth and determine the bar diameter. The instrument is based on the magnetic technique and is calibrated for different purposes. The cover depth is important from the point of view of estimation of initiation of corrosion of reinforcing bars.

For a longitudinal reinforcing bar in a Column nominal cover shall in any case not be less than 40mm or less than the diameter of such bar as per clause 26.4.2.1 of IS: 456-2000. Nominal cover to meet durability requirement for footing, minimum cover shall be 50mm as per clause 26.4.2.2 of IS: 456-2000.

Minimum values of nominal cover of normal weight aggregate concrete to be provided to all reinforcement including links to meet specified period of fire resistance shall be as per Table 16A of IS:456-2000.

Minimum values for the nominal cover of normal weight aggregate concrete which should be provided all reinforcement including links depending of exposure condition shall be as per the Table 5 of IS: 456-2000.

3.8 Chemical Analysis

Corrosion of reinforcing steel due to chlorides in concrete is one of the most common environmental attacks that lead to deterioration of concrete structures. Whenever there is chloride in concrete there is an increased risk of corrosion of embedded metal. Chloride content is then expressed in kg per cubic meter of concrete and compared with the values of limits of chloride contents of concrete (**Table 7 of IS: 456–2000**).

Sulphates (SO_3) are present in most cements and in some aggregates; excessive amounts of water-soluble sulphate from these or other mix constituents can cause expansion and disruption of concrete. To prevent it, **IS: 456-2000 clause-8.2.5.3** states that the total water-soluble sulphate content of the concrete mix, expressed as SO_3, should not exceed 4 percent by mass of the cement in the mix. The sulphate content should be calculated as the total from the various constituents of the mix.

The pH value of the concrete should be above 11.5 to maintain alkalinity of concrete surrounding the embedded steel. A reduction in the pH value of concrete indicates loss of passive layer around the reinforcement which protects the steel from distress.

For analyzing Chloride content and pH of concrete, concrete powder samples were extracted from 0-25mm, 25-50mm depths at identified locations and then tested as per IS:14959(Part 2) -2001 (Determination of water soluble and acid soluble Chlorides in Mortar and Concrete – Method of Test).

Adequate numbers of accessible members were selected from various locations to extract concrete powders for chemical test.

4.0 RESULTS AND DISCUSSION

4.1. Visual Observations

The height of the TG-Unit#1 is 18m. Visual observations and testing carried out at 4m, 8.5m, 18m, and height. Distress, Signs of cracks, surface voids and exposure of steel reinforcement bars observed on the TG-Unit#1 at different heights. Distress and Honeycomb observed at a few locations of Interior and exterior RCC members. The visual observations and photographs are shown **Annexure 1**.

4.2. Rebound Hammer Testing-Completed values

Rebound Hammer testing was carried out on various identified (Reinforced Cement Concrete) members of TG-Unit#1 using random sampling technique. The results of surface compressive strength obtained by Rebound Hammer testing are given in Table 2 to 26**.** Surface Compressive strength results of concrete as obtained on different hardened concrete surfaces of Members are summarized as:

1) Surface compressive strength of concrete obtained on TG-Unit#1, Turbine Pedestal at West side by Rebound Hammer Testing is found to vary from **38.83 N/mm^2 to 41.09 N/mm^2** with an average surface compressive strength of **39.96 N/mm^2** (Refer Table 2).
2) Surface compressive strength of concrete obtained on TG-Unit#1, Turbine Pedestal at East side by Rebound Hammer Testing is found to vary from **38.83 N/mm^2 to 42.22 N/mm^2** with an average surface compressive strength of **39.68 N/mm^2** (Refer Table 3).
3) Surface compressive strength of concrete obtained on TG-Unit#1, Turbine Pedestal at East side by Rebound Hammer Testing is found to vary from **38.83 N/mm^2 to 41.66 N/mm^2** with an average surface compressive strength **40.10 N/mm^2** (Refer Table 4).
4) Surface compressive strength of concrete obtained on TG-Unit#1, Turbine Pedestal at West side by Rebound Hammer Testing is found to vary from **39.39 N/mm^2 to 41.09 N/mm^2** with an average surface compressive strength of **39.68 N/mm^2** (Refer Table 5).

5) Surface compressive strength of concrete obtained on TG-Unit#1, Turbine bottom level at West side by Rebound Hammer Testing is found to vary from **38.83 N/mm^2 to 40.53 N/mm^2** with an average surface compressive strength of **39.82 N/mm^2** (Refer Table 6).

6) Surface compressive strength of concrete obtained on TG-Unit#1, A6 Column by Rebound Hammer Testing is found to vary from **38.26 N/mm^2 to 40.53 N/mm^2** with an average surface compressive strength of **39.68 N/mm^2** (Refer Table 7).

7) Surface compressive strength of concrete obtained on TG-Unit#1, A5 Column @4m by Rebound Hammer Testing is found to vary from **39.39N/mm^2 to 40.53N/mm^2** with an average surface compressive strength of **39.82N/mm^2** (Refer Table 8).

8) Surface compressive strength of concrete obtained on TG-Unit#1, A2 Column by Rebound Hammer Testing is found to vary from **39.39 N/mm^2 to 42.22 N/mm^2** with an average surface compressive strength of **40.24 N/mm^2** (Refer Table 9).

9) Surface compressive strength of concrete obtained on TG-Unit#1, A3 Column @4m by Rebound Hammer Testing is found to vary from **38.83 N/mm^2 to 41.66 N/mm^2** with an average surface compressive strength of **39.96 N/mm^2** (Refer Table 10).

10) Surface compressive strength of concrete obtained on TG-Unit#1, at B5 Column @6m by Rebound Hammer Testing is found to vary from **38.26 N/mm^2 to 41.66 N/mm^2** with an average surface compressive strength of **39.82 N/mm^2** (Refer Table-11).

11) Surface compressive strength of concrete obtained on TG-Unit#1, at B1 Column @6m by Rebound Hammer Testing is found to vary from **39.39 N/mm^2 to 41.09 N/mm^2** with an average surface compressive strength of **40.24 N/mm^2** (Refer Table 12).

12) Surface compressive strength of concrete obtained on TG-Unit#1, at B1 Column @8.5m by Rebound Hammer Testing is found to vary from **38.26 N/mm^2 to 42.22 N/mm^2** with an average surface compressive strength of **40.10 N/mm^2** (Refer Table 13).

13) Surface compressive strength of concrete obtained on TG-Unit#1, at B1 Column @8.5m by Rebound Hammer Testing is found to vary from **39.39 N/mm^2 to 42.22 N/mm^2** with an average surface compressive strength of **40.38 N/mm^2** (Refer Table 14).

14) Surface compressive strength of concrete obtained TG-Unit#1, at A4 Column @4m by Rebound Hammer Testing is found to vary from **37.70 N/mm^2 to 41.66 N/mm^2** with an average surface compressive strength of **39.54 N/mm^2** (Refer Table 15).

15) Surface compressive strength of concrete obtained on TG-Unit#1, A1 Column @8.5m by Rebound Hammer Testing is found to vary from **38.26 N/mm^2 to 42.22 N/mm^2** with an average surface compressive strength of **39.96N/mm^2** (Refer Table 16).

16) Surface compressive strength of concrete obtained on TG-Unit#1, A5 Column @8.5m by Rebound Hammer Testing is found to vary from **38.83 N/mm^2 to 41.09 N/mm^2** with an average surface compressive strength of **39.82 N/mm^2** (Refer Table 17).

17) Surface compressive strength of concrete obtained on TG-Unit#1, A3 Column by Rebound Hammer Testing is found to vary from **38.26 N/mm^2 to 41.66 N/mm^2** with an average surface compressive strength of **39.96 N/mm^2** (Refer Table 18).

18) Surface compressive strength of concrete obtained on TG-Unit#1, A4 Column by Rebound Hammer Testing is found to vary from **38.26 N/mm^2 to 41.09 N/mm^2** with an average surface compressive strength of **39.68 N/mm^2** (Refer Table 19).

19) Surface compressive strength of concrete obtained on TG-Unit#1, B5 Column by Rebound Hammer Testing is found to vary from **37.13 N/mm^2 to 42.79 N/mm^2**with an average surface compressive strength of **39.96 N/mm^2** (Refer Table 20).

20) Surface compressive strength of concrete obtained on TG-Unit#1, A1-B1 Beam 12.5m level by Rebound Hammer Testing is found to vary from **37.13 N/mm^2 to 41.09 N/mm^2** with an average surface compressive strength of **39.82 N/mm^2** (Refer Table 21).

21) Surface compressive strength of concrete obtained on TG-Unit#1, B1 Column 12.5m level by Rebound Hammer Testing is found to vary from **38.83 N/mm^2 to 42.22 N/mm^2** with an average surface compressive strength of **40.10 N/mm^2** (Refer Table 22).

22) Surface compressive strength of concrete obtained on TG-Unit#1, A7-B7 Beam 8.5m level by Rebound Hammer Testing is found to vary from **37.13 N/mm^2 to 42.22 N/mm^2** with an average surface compressive strength of **39.25 N/mm^2** (Refer Table 23).

23) Surface compressive strength of concrete obtained on TG-Unit#1, A1 Column 12.5m level by Rebound Hammer Testing is found to vary from **40.53 N/mm^2 to 41.09 N/mm^2** with an average surface compressive strength of **40.95 N/mm^2** (Refer Table 24).

24) Surface compressive strength of concrete obtained on TG-Unit#1, A6-B6 Beam 12.5m level by Rebound Hammer Testing is found to vary from **38.26 N/mm^2 to 39.96 N/mm^2** with an average surface compressive strength of **39.39 N/mm^2** (Refer Table 25).

25) Surface compressive strength of concrete obtained on TG-Unit#1, A2-B2 Beam 12.5m level by Rebound Hammer Testing is found to vary from **39.39 N/mm^2 to 40.53 N/mm^2** with an average surface compressive strength of **39.96 N/mm^2** (Refer Table 26).

4.3. Ultrasonic Pulse Velocity Testing (UPV):

The **Ultrasonic Pulse Velocity** testing was conducted on TG-Unit#1 in the presence of concerned engineering team of NTPC. The results of the UPV values obtained on various members are as follows:

1) The UPV measurements were taken using cross probing technique on the TG-Unit#1, A1 Column are in the range of **3.86 to 4.38 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018(Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table -28).
2) The UPV measurements were taken using surface probing technique on the TG-Unit#1, A2 Column are in the range of **3.98 to 4.22 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018(Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table - 29).
3) The UPV measurements were taken using surface probing technique on the TG-Unit#1, B3 Column are in the range of **4.03 to 4.26 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018(Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table - 30).
4) The UPV measurements were taken using Surface probing technique on the TG-Unit#1, C1 Column are in the range of **3.94 to 4.19 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018(Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table -31).
5) The UPV measurements were taken using Surface probing technique on the TG-Unit#1, B2 Column @8 m is in the range of **4.03 to 4.22 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018(Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table -32).
6) The UPV measurements were taken using surface probing technique on the TG-Unit#1, A1 Column @8 m is in the range of **4.02 to 4.24km/sec**. When these values are compared

with the velocity criteria of IS: 516 (Part V) – 2018(Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table -33).

7) The UPV measurements were taken using surface probing technique on the TG-Unit#1, C1 Column @8 m is in the range of **3.97 to 4.15 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018(Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table -34).
8) The UPV measurements were taken using Cross probing technique on the TG-Unit#1, C1 Column @8 m is in the range of **3.77 to 3.88 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018(Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table -35).
9) The UPV measurements were taken using Cross probing technique on the TG-Unit#1, B2 Column @8 m is in the range of **3.78 to 3.83 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table -36).
10) The UPV measurements were taken using Cross probing technique on the TG-Unit#1, B2 Column @8 m is in the range of **3.80 to 3.91 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table - 37).
11) The UPV measurements were taken using Cross probing technique on the TG-Unit#1, B1 Column @6m are in the range of **3.81 to 4.16 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table - 38).
12) The UPV measurements were taken using Cross probing technique on the TG-Unit#1, B1 Column @8.5m are in the range of **3.77 to 3.97 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table - 39).
13) The UPV measurements were taken using Surface probing technique on the TG-Unit#1, B1 Column @8.5m are in the range of **3.96 to 4.15 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table - 40).

14) The UPV measurements were taken using cross probing technique on the TG-Unit#1, A4 Column @4m are in the range of **3.85 to 3.92 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table - 41).

15) The UPV measurements were taken using Surface probing technique on the TG-Unit#1, A1 Column @8.5m are in the range of **3.98 to 4.22 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table - 42).

16) The UPV measurements were taken using surface probing technique on the TG-Unit#1, A5 Column @8.5m are in the range of **3.98 to 4.23 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table - 43).

17) The UPV measurements were taken using surface probing technique on the TG-Unit#1, A3 Column are in the range of **3.98 to 4.23 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD (**Table - 44).

18) The UPV measurements were taken using Surface probing technique on the TG-Unit#1, A4 Column are in the range of **3.98 to 4.13 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table - 45).

19) The UPV measurements were taken using surface probing technique on the TG-Unit#1, B5 Column are in the range of **3.98 to 4.22 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table - 46).

20) The UPV measurements were taken using surface probing technique on the TG-Unit#1, A1-B1 Beam 12.5m level are in the range of **3.98 to 4.11 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table - 47).

21) The UPV measurements were taken using Cross probing technique on the TG-Unit#1, B1 Column 12.5m level are in the range of **3.80 to 3.88 km/sec**. When these values are

compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table - 48).

22) The UPV measurements were taken using Cross probing technique on the TG-Unit#1, A7-B7 Beam 8.5m level are in the range of **3.80 to 4.17 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table - 49).

23) The UPV measurements were taken using surface probing technique on the TG-Unit#1, A1 Column 12.5m level are in the range of **3.95 to 4.25 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) – 2018 (Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table - 50).

24) The UPV measurements were taken using surface probing technique on the TG-Unit#1, A6-B6 Beam 12.5m level are in the range of **4.00 to 4.30 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) –2018 (Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table - 51).

25) The UPV measurements were taken using surface probing technique on the TG-Unit#1, A2-B2 Beam 12.5m level are in the range of **4.00 to 4.24 km/sec**. When these values are compared with the velocity criteria of IS: 516 (Part V) –2018 (Also reproduced in Table 27), the overall quality of concrete is assessed to be **GOOD** (Table - 52).

4.4 Concrete Core Testing

Corresponding to the 60mm concrete core extracted by random sampling technique covering different locations of TG-Unit#1 in NTPC Tanda tested at NCB laboratory Hyderabad, the equivalent cube compressive strength of concrete of TG-Unit#1 are shown in Table 56. In total, 12 concrete cores were extracted from different members of the TG-Unit#1 and were tested.

The test results indicate that the equivalent cube compressive strength values for

1. TG-Unit#1, A1 Column is found to be 32.04 N/mm²
2. TG-Unit#1, A2 Column @6m is found to be 31.58 N/mm²
3. TG-Unit#1, B3 Column @4m is found to be 27.30 N/mm²
4. TG-Unit#1, C1 Column @8m is found to be 29.98 N/mm²
5. TG-Unit#1, B2 Column @8m is found to be 25.27 N/mm²
6. TG-Unit#1, A1 Column @8m is found to be 25.75 N/mm²

7. TG-Unit#1, C1 Column @8m is found to be 21.45 N/mm²
8. TG-Unit#1, C1 Column @8 m level is found to be 22.76 N/mm²
9. TG-Unit#1, B2 Column @8m level is found to be 33.60 N/mm²
10. TG-Unit#1, B2 Column @8m level is found to be 22.71 N/mm²
11. TG-Unit#1, A1 Column @12.5m level is found to be 27.88 N/mm²
12. TG-Unit#1, B2 Column @12.5m level is found to be 23.56 N/mm²

In total, 12 nos. tested cores all of them found to have equivalent cube compressive strength more than specified characteristic compressive strength of M25 grade concrete.

4.5 Concrete Cover

The concrete cover depth to rebars in members is measured with Ferro-scanner and a measuring tape/scale in the places where concrete is exposed and accessible for direct measurement. Nominal cover to reinforcement to meet durability requirement is given in **IS-456: Table 16-clause 26.4.2**, the measured cover to reinforcement steel in the selected members are given in Table 54**.**

1. The Concrete cover to Reinforcing bars of TG-Unit#1, A3 Column @4m during testing using Ferro scanner meter is found with an average of **82mm.**
2. The Concrete cover to Reinforcing bars TG-Unit#1, A2 Column @6m during testing using Ferro scanner meter is found with an average of **83mm.**
3. The Concrete cover to Reinforcing bars of TG-Unit#1, B1 Column @4m during testing using Ferro scanner meter is found with an average of **81mm.**
4. The Concrete cover to Reinforcing bars of TG-Unit#1, B2 Column @8.5m during testing using Ferro scanner meter is found with an average of **84mm.**
5. The Concrete cover to Reinforcing bars of TG-Unit#1, A6 Column @8.5m during testing using Ferro scanner meter is found with an average of **83mm.**
6. The Concrete cover to Reinforcing bars of TG-Unit#1, A3 Column @8.5m during testing using Ferro scanner meter is found to with an average of **82mm.**
7. The Concrete cover to Reinforcing bars of TG-Unit#1, B5 Column @8.5m during testing using Ferro scanner meter is found with an average of **81mm.**
8. The Concrete cover to Reinforcing bars of TG-Unit#1, B1 Column 8.5m level during testing using Ferro scanner meter is found with an average of **81mm.**

9. The Concrete cover to Reinforcing bars of TG-Unit#1, A5 Column @8.5m level during testing using Ferro scanner meter is found with an average of **82mm.**
10. The Concrete cover to Reinforcing bars of TG-Unit#1, A3 Column @12.5m level during testing using Ferro scanner meter is found with an average of **83mm.**
11. The Concrete cover to Reinforcing bars of TG-Unit#1, A1 Column 12.5m level during testing using Ferro scanner meter is found with an average of **80mm.**
12. The Concrete cover to Reinforcing bars of TG-Unit#1, B2 Column @12.5m level during testing using Ferro scanner meter is found with an average of **84mm.**

The Concrete cover within the specified limits to meet durability requirement as per IS: 456-2000 (Refer Table 16 of IS: 456-2000) which is Reproduced in Table 53.

4.6 Carbonation

Table-55 shows test results of carbonation testing done on 12 no. Concrete Cores extracted from various representative concrete samples. The results indicate that the values of depth of carbonation in all different locations of TG-Unit#1 were found in between **0-10 mm.**

Based on the above carbonation study carried on different selected members at several locations the carbonation depth is found to be within the concrete cover region.

4.7 Half-Cell Potential Test

Half-cell potential (HCP) measurements using copper, copper-sulfate half-cell technique as per ASTM C-876 (Standard test method for corrosion potentials of uncoated reinforcing steel in concrete) were taken at site to ascertain corrosion status of reinforcing bars of various locations of RCC members in TG-Unit#1 NTPC Tanda. The measurements were done on different locations randomly selected locations and comprising of representative samples for the structure.

Test results (refer Table-58) when compared with the corrosion criteria as per ASTM C-876 (Table-57) indicate that probability of corrosion is found to be in 'Transit State".

4.8 Chemical Analysis

The chemical analysis of water and powdered samples extracted from different elements of RCC members in TG-Unit#1 NTPC Tanda, collecting by random sampling technique. This covered chloride content, sulphate content per cum of concrete as well pH value of powdered

samples. The test results as obtained in NCB laboratory are shown in Table- 59. Analysis of interpretation of test results given as under:

1) Based on the results obtained from laboratory the range of chloride content in the A3 Column @4m of TG-Unit#1 was found to vary from 0.192 kg/m^3 to 0.216 kg/m^3 with an average value of **0.204 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix was found to vary from 2.20 % to 2.48% with an average of **2.34%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value was found to vary from 11.55 to 11.64 with an average of **11.60** which is more than the specified limit to resist the corrosion.
2) Based on the results obtained from laboratory the range of chloride content in the A2 Column @6m of TG-Unit#1 was found to vary from 0.168kg/m^3 to 0.192 kg/m^3 with an average value of **0.18 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix was found to vary from 2.08 % to 2.64% with an average of **2.36%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000).The range of pH value was found to vary from 11.26 to 11.15 with an average of **11.20** which is slightly less than the specified limit to resist the corrosion.
3) Based on the results obtained from laboratory the range of chloride content in the B1 Column @4m of TG-Unit#1 was found to vary from 0.216 kg/m^3 to 0.168 kg/m^3 with an average value of **0.19 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS: 456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix was found to vary from 2.16 % to 2.64% with an average of **2.40%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value was found to vary from 11.45 to 11.14 with an average of **11.30** which is less than the specified limit to resist the corrosion.
4) Based on the results obtained from laboratory the range of chloride content in the B2 Column @8.5m of TG-Unit#1 was found to vary from 0.192 kg/m^3 to 0.168 kg/m^3 with an average value of **0.18 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS:456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix was found to vary from 2.72 % to 2.88% with an average of **2.80%** which is within the permissible limit of 4%

(As per clause-8.2.5.3 of IS: 456-2000). The range of pH value was found to vary from 11.22 to 11.12 with an average of **11.17** which is less than the specified limit to resist the corrosion.

5) Based on the results obtained from laboratory the range of chloride content in the A6 Column @8.5m of TG-Unit#1 was found to vary from 0.192 kg/m^3 to 0.216 kg/m^3 with an average value of **0.20kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS:456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix was found to vary from 2.24% to 2.84% with an average of **2.54%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value was found to vary from 11.25 to 11.09 with an average of **11.17** which is less than the specified limit to resist the corrosion.

6) Based on the results obtained from laboratory the range of chloride content in the A3 Column @8.5m of TG-Unit#1 was found to vary from 0.192 kg/m^3 to 0.168 kg/m^3 with an average value of **0.18kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS:456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix was found to vary from 2.36 % to 2.72% with an average of **2.54%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value was found to vary from 11.34 to 11.14 with an average of **11.24** which is less than the specified limit to resist the corrosion.

7) Based on the results obtained from laboratory the range of chloride content in the B5 Column @8.5m of TG-Unit#1 was found to vary from 0.192 kg/m^3 to 0.216 kg/m^3 with an average value of **0.20 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS:456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix was found to vary from 2.76 % to 2.72% with an average of **2.74%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value was found to vary from 11.28 to 11.06 with an average of **11.17** which is less than the specified limit to resist the corrosion.

8) Based on the results obtained from laboratory the range of chloride content in the A3 Column @12.5m level of TG-Unit#1 was found to vary from 0.168 kg/m^3 to 0.216 kg/m^3 with an average value of **0.19 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS:456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix was found to

vary from 2.28 % to 2.32% with an average of **2.30%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value was found to vary from 11.29 to 11.10 with an average of **11.19** which is less than the specified limit to resist the corrosion.

9) Based on the results obtained from laboratory the range of chloride content in the B2 Column @12.5m level of TG-Unit#1 was found to vary from 0.168 kg/m^3 to 0.192 kg/m^3 with an average value of **0.18 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS:456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix was found to vary from 2.56 % to 2.36% with an average of **2.46%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value was found to vary from 11.41 to 11.21 with an average of **11.31** which is less than the specified limit to resist the corrosion.

10) Based on the results obtained from laboratory the range of chloride content in the A3 Column @12.5m level of TG-unit#5 was found to vary from 0.192 kg/m^3 to 0.144 kg/m^3 with an average value of **0.17 kg/m^3** is within the permissible limit of 0.6 kg/m3 (As per IS:456-2000 Table 7). The range of Sulphate (SO3) content by mass of the cement in mix was found to vary from 2.76 % to 2.80% with an average of **2.78%** which is within the permissible limit of 4% (As per clause-8.2.5.3 of IS: 456-2000). The range of pH value was found to vary from 11.23 to 10.88 with an average of **11.05** which is less than the specified limit to resist the corrosion.

5.0 Conclusions:

The following Conclusions can be broadly made from the testing results:

i) Based on Rebound hammer testing to evaluate the average likely surface hardness on RCC members, the results were found satisfactory and it varies in between 39-40.

ii) Based on Ultrasonic Pulse Velocity to evaluate Quality of concrete on RCC members, the results were found to vary between Good Quality of concrete.

iii) The compressive strength of the concrete core samples extracted from the TG-Unit#1 were found meeting the required compressive strength more than specified characteristic compressive strength of M25 grade concrete.

iv) Carbonation is found 0-10mm after 35years' exposure to existing environment where as concrete cover of members is found to vary from 80 – 84mm.

v) Based on the Half-Cell potential measurements done by random sampling technique at various locations and visual observations of TG-Unit#1 indicate that probability of corrosion is found to be in "Transit State".

vi) The amount of Soluble Sulphates in the concrete of members is within the specified limits and chloride content in the concrete is also within the specified limit and pH values are slightly lower than the specified limit in all members.

vii) Distress and deterioration in the form of minor cracks, Honey combs, surface voids and corrosion of steel reinforcement were noticed visually at few locations of TG-Unit#1.

6.0 Recommendations

The following steps shall be taken to repair the cracks & strengthening of TG-Unit#1:

Part I: Scaffolding:

Providing and fixing double scaffolding system (cup lock type) on the exterior side, up to seven story height made with 40 mm dia M.S. tube 1.5 m centre to centre, horizontal & vertical tubes joining with cup & lock system with M.S. tubes, M.S. tube challis, MS clamps and M.S. staircase system in the scaffolding for working platform etc. and maintaining it in a serviceable condition for the required duration as approved and removing it thereafter .The scaffolding system shall be stiffened with bracings, runners, connection with the building etc wherever required for inspection of work at required locations with essential safety features for the workmen etc. complete as per directions and approval of Engineer in charge. The elevation area of the scaffolding shall be measured for payment purpose.

Part-II: Repair and Strengthening:

i) <u>Chipping:</u>

Cover concrete around the horizontal, vertical cracks shall be chipped off to the depth up to 40mm on RCC members. The chipping in the spalled portion of the columns and beams shall be limited up to the cover region. Chipping of

loose/hollow sounding concrete can be done by striking the doubtful surfaces with 2 lb hammer.

ii) <u>Treatment for Cracks& Honeycombing:</u>

a. The cracks are to be widened by cutting V-grooves of 10mm x 10mm size and sealed with approved epoxy repair mortar.

b. After the sealing, 12mm dia galvanized steel injection nipples are to be inserted in the crack area and also wherever honeycombing is found by drilling holes of required diameter up to the depth of 50 – 120 mm at required spacing (generally 350 mm staggered spacing). The drilled holes must be made dust free by blowing compressed air and should be sealed after the insertion of the nozzle with approved adhesive and allowed to cure.

c. After the nipples are injected and cured, grouting in the proportion recommended by the manufacturer into the cracks/honeycombed area of concrete/masonry shall be done using suitable gun/pump at required pressure. Once the grouting work is finished, the extruding nipples can be cut-off after the curing period.

iii) <u>Reinforcement Corrosion Treatment:</u>

Wherever reinforcing rebar is found corroded in RCC members

a) Remove the rust by manually or suitable means to make corroded reinforcing bars rust free.

b) Provide and apply corrosion protection using 2 coats of anticorrosive Zn rich epoxy phenolic rebar protection system of approved brand on the exposed old reinforcement by brush with interval of 24 hours between coats and corrosion protection of exposed old reinforcing bars.

c) Provide and apply concrete penetrating corrosion inhibitor (CPCI) of approved brand over the entire finished surface are obtained after removal of distressed concrete in 2 coats @ of $4m^2$/ltr/coat approximately.

iv) <u>Bond Coat:</u>

After chipping off the concrete cover, provide and apply structural grade two component epoxy bond coat prior to application of any type of mortar conforming to ASTM C - 881 -13 Type - II tested as per ASTM C –882-13 to ensure bond

between old and new concrete by brush application. (Material manufacture either from Sinorganic/BASF/SIKA/FOSRAC/KRISHNA Conchem/Pidilite or equivalent)

v) **Making up lost section with Polymer Modified Mortar (PMM):**

For repair of patches having, apply average 40mm PMM in 2-3 layers using SBR Latex conforming to ASTM C-1059-13 Type-I in damaged areas (1 Cement-3 part graded cleaned river sand + 15 % latex by weight of cement) with 0.35 w/c ratio, in 15-20 mm thick layers by applying bond coat between successive/each. (Material manufacture either from Sinorganic/BASF/SIKA/FOSRAC or equivalent)

vi) **Protective coating:**

Before applying the protective coating on concrete surface as well as the internal exposed areas all platforms shall be cleaned by scrubbing with hard steel brush to remove loose particles, disintegrated concrete, deposited smoke and dust particles etc. The scrubbed surface is cleaned by air blowing and then dries it completely. Apply min. 2 coats of two-part high-performance moisture compatible corrosion resistant coating material (base and curing agent) of approved manufacturer over prepared surface, using not less than theoretical consumption as per the manufacturer's specification. Total dry film thickness (DFT) including primer will be 300- 400 microns.

Note:

1. Before taking up any repair work, the dryness of substrate concrete must be ensured for effective application of several repair materials. Remove oil, grease, wax, Cement laitance, loose particles and other contaminants, scarifying or mechanically wire brushing followed by air jet from the substrate concrete.
2. During repair works of TG-Unit#1 measures should be taken up in accordance with relevant safety standards and safety guidelines of Occupational safety & Health Administration (OSHA) for construction, arrangement like safety nets/platforms should be done.

.....

I/21918/2022

ANNEXURE-R14

(Computer No. 5220)

भारत सरकार
Government of India
विद्युत मंत्रालय
Ministry of Power
केंद्रीय विद्युत प्राधिकरण
Central Electricity Authority
तापीय अभियांत्रिकी एवं प्रौद्योगिकी विकास प्रभाग
Thermal Engineering & Technology Development

सेवा में / To,

सभी ताप विद्युत उत्पादन संयंत्र / All Thermal Power Generating Plants/Utilities

विषय/Subject: Safety Advisory to all Thermal Power Generating Utilities.

महोदय/महोदया / Sir/Madam,

You may be aware that Hon'ble National Green Tribunal vide its Order dated 22.12.2020 in O.A. No. 108/2020 with O.A. No. 130/2020 had directed that "*Secretaries, Ministry of Power and Coal, Government of India, in coordination with such other Departments/ Institutions, as may be necessary, to undertake Safety Audits of similarly placed thermal power stations throughout the country expeditiously preferably within six months to avoid recurrence of such incidents in future".*

In compliance to the aforesaid order, a Safety Audit Committee under the chairmanship of the undersigned was constituted by Central Electricity Authority (CEA) comprising representatives from Ministry of Coal, Central Boiler Board (CBB), Director General Fire Safety (DGFS), NTPC Ltd., NLC India Limited (NLCIL), Bharat Heavy Electrical Limited (BHEL) and other experts. The above Committee carried out the safety audit of different coal/lignite based Thermal Power plants across the country during the period of August to November 2021.

A safety advisory based on the broad deficiencies observed during above safety audits of the thermal power stations is enclosed at Annexure-I for your kind information and needful actions. However, safety of plant and personnel is not limited to these findings only. Utilities/plants may also continue to take regular safety measures as per the extant Rules and Regulations in this regard.

संलग्नक/Enclosure: यथोपरि/As above

भवदीय/Yours Sincerely,

(धीरज कुमार श्रीवास्तव / Dhiraj Kumar Srivastava)
मुख्य अभियंता / Chief Engineer

सेवा भवन ,आर.के .पुरम – 1, नई दिल्ली – 110066 टेलीफोन: 011-26732977, ईमेल: cetetd-cea@gov.in, वेबसाइट: www.cea.nic.in
Sewa Bhawan, R.K Puram-I, New Delhi -110066, Telephone: 011-26732977, Email: cetetd-cea@gov.in, Website: www.cea.nic.in

Annexure-I

Safety Advisory to all Thermal Power Generating Utilities

(A) General Safety and Fire Safety

1. Implement the requisite provisions of (1) Central Electricity Authority (Safety Requirements for Construction, Operation and Maintenance of Electrical Plants and Electric Lines) Regulations, 2011 (2) Central Electricity Authority (Measures relating to Safety and Electric Supply) Regulations, 2010 (3) Statutory requirement under Factories Act and other related Acts such as Manufacture, Storage, and Import of Hazardous Chemicals (MSIHC) Rules, 1989 – entrusted functions and Response Rules (4) IS:1646 - Code of Practice for Fire safety of buildings (general): Electrical installations (5) IS:3034 - Fire safety of industrial buildings: Electrical generating and Distributing stations - Code of Practice.
2. Internal Safety Audits must be carried out once a year through cross functional teams/ internal trained staff and records must be maintained. Further, External Safety Audit must be carried out through registered Agencies at a regular periodicity of 2 years and Action Taken Report (ATR) must be prepared & monitored to ensure early closing of pending recommendations.
3. Ensure a separate budget head in its overall budget provisions to adequately fund safety related activities. Detailed safety manual complying with the statutory requirements and manufacturers' recommendations must be available with power plant.
4. Safety awareness drives must be conducted amongst plant personnel as well as the employees deployed by the Contractors, periodically for the compliance of provisions of safety manuals and to imbibe the safety culture.
5. The safety officer shall be appointed and safety committee shall be constituted by thermal power plant as per the statutory requirement. Plants shall hold Safety Committee meetings regularly and Head of Plant shall chair these meetings. The output of these Safety Committee meetings should be implemented.
6. Ensure that 'Safety Performance' KPA (Key Performance Area) for employees is linked with Annual Performance Assessment for officers at various levels to instill a safety-compliant behavior.
7. Keep an updated inventory of safety related PPEs and also provide the tasks specific PPE kits to all the workers/ staff.
8. All major/ minor accidents must be properly investigated and analyzed to find the Root Cause of incident/accident.
9. Implement procedures for reporting of accidents by the concerned Power Station to CEA in line with the provisions of the CEA safety regulations.

10. Emergency Response Disaster Management Plan (ERDMP) both On-site & Off-site shall be prepared by all power plants.
11. Ensure that a functional proper Public Address system is in place and also 'Walkie/ Talkie' should be mandatorily adopted in the power plants.
12. Plants must be compliant/ certified as per ISO: 45001 'Occupational Health & Safety Management System'.
13. Ensure that all fire safety procedures are followed and fire-fighting system, its operation, installations are well maintained and upkeep of various sub-components is reviewed at regular intervals to make sure their proper response during emergencies. These shall include but not be limited to the following:
    i. Fire Water pump house must be maintained in proper healthy condition. There should be no obstructions in the pathways and approaches to equipment should be hindrance free.
    ii. All fire hydrant pumps and jockey pumps must be maintained in healthy condition. The Fire Hydrant pumps need to be operated in 'AUTO MODE' & Sequential starting system should be in place. The reliability & availability of the Pumps are to be checked at frequent intervals and recorded.
    iii. Fire-fighting crew along with some identified regular employees must go through hands-on firefighting training including rescue and disaster handling to enhance effectiveness of firefighting & safety crew.
    iv. Manual call points (MCPs) must be provided at all the strategic locations of the power stations and must be integrated with the Fire Control Room for effective monitoring and to ensure timely & quick response from fire-fighting crew.
    v. Mock drills should be conducted at regular intervals and also at odd hours for various emergencies scenarios & debriefing session should be conducted after each mock drill. The gaps observed are to be analyzed and mitigation measures need to be taken. These details should be recorded in a register.
    vi. Fire Marshalls/ firefighting crew should be trained for actual emergencies scenarios.
    vii. Each Power Station shall have a Fire Emergency Plan formulated so as to facilitate organized actions (in case of fire) by employees at various levels, during day as well as night and shall also contain the instructions on fire prevention measures and the firefighting organization.
    viii. Fireboxes with hose reels at fire hydrant points must be available.
    ix. Non-sparking tools and flame-proof electric fittings should be mandatorily used at all places where flammable materials like coal gases are stored/ are in use. Also, static electric charge dissipate shou

be provided at the entry gate of such systems which are prone to catch fire easily.

14. Emergency exit path marking should be made available for safe evacuation of working personnel during emergency conditions. Emergency telephone numbers must be prominently displayed at prominent locations in the plant, such as at TG floor, Unit Control Room & emergency exit points etc. Display of DO's & DON'Ts should be done in large fonts for better visibility. All such Display Boards should have a DC backlit display.
15. Lock Out & Tag Out (LOTO) system for maintenance management should be fully implemented for safe operation of the power plants and a proper Permit to Work (PTW) system must be followed and there should be seamless integration between LOTO & PTW System (and also to ERP system, if available). Proper Job Safety Analysis (JSA) should be carried out before issuance of each PTW.
16. Accumulated and unwanted scrap/ dismantled machinery etc. should be removed from working areas such as boiler structure, TG floor etc. and stored at designated places. Measures should be taken to remove wild vegetation growth in switchyard.
17. Excessive accumulation of coal/ lignite dust in some of the vulnerable areas like Crusher house, transfer points, coal/ lignite Bunker house, etc. must be avoided.
18. Preventive measures such as anti-corrosion painting and regular maintenance should be done for support structures and various equipment.
19. Rotating parts of various equipment should be covered with proper guards.
20. SOPs for various plant equipment to be prepared and made available to working personnel.

(B) Boiler, Turbine and Generator (BTG) Safety

1. As per IBR Regulations, periodic Remnant Life Assessment (RLA) should be carried out.
2. Annual overhauling, Capital overhauling and Renovation & Modernization works must be done on time as these prevent equipment failures. Overhauling work should be monitored comprehensively.
3. The boilers must be operated by Boiler Operating Engineers (BOEs) in compliance with the provisions of IBR. Utilities with shortage of BOEs are advised to take immediate and urgent steps to ensure that sufficient number of engineers should be qualified BOEs.
4. Boilers having box type column-beam structure are prone to accumulation of coal/ash dust if there are openings in the boiler structure. Coal dust accumulated in such confined structure may lead to fire/explosion. All such openings in such kind of structure must be closed. Also, cleaning must ensured before closure.

5. Thermal insulation of Boiler, Turbine, associated sub-systems and all other critical equipment & lines must be ensured and maintained in good health. Regular thermal survey for surface temperature should be done. It is recommended to do insulation of.
6. Pulverized fuel leakage in mills, pipes, joints etc., if any, should be arrested on immediate basis.
7. The closeness of steam lines with other components/structure of Boiler or adjacent civil structure must be avoided.
8. All Boiler expansion indicators must be fitted properly to measure vertical movement as well as horizontal movement.
9. Mandatorily carry-out tool tagging to have effective inventory management and thus ensure timely availability of all tools & tackles. Tagging and marking date of last load testing of all O&M tools & tackles must be ensured.
10. Illumination measurement should be carried out as per IS:6665 and it needs to be improved in the plants wherever necessary.
11. Take measures to ensure that ambient noise levels around equipment like Turbine-Generator, Boiler etc. auxiliaries are in desired limits.
12. Regular ash level monitoring in ESP hoppers must be done by providing Ash Level Indicators (ALI). Timely steps must be taken for regular evacuation of ash. Also, ensure that ash hopper heaters are in healthy condition so that fluidity of ash is not hampered.
13. Safety Valves and Electromatic Relief Valves (ERVs) must be maintained in healthy condition and operative.
14. Vibration levels of machines such as TG set, fans, pumps, etc. must be monitored on regular basis and machines should not run beyond the recommended vibration limits prescribed by OEM.
15. Compulsorily carry out turbine over speeding test as per OEM recommendations.
16. Regularly perform checks for functionality of all the Protection & Interlocks (P&I) for various equipment and system.

(C) Balance of Plant (BoP) Safety

1. Chlorine leak sensor probes must be provided for all chlorine cylinder bays at proper locations. Water sprinkler system need to be installed in chlorination plant to neutralize chlorine leak in addition to the extant system.
2. Dust suppression system must be in operating condition to prevent coal/ lignite dust accumulation in areas such as coal/ lignite yard, Crusher house, transfer junctions/ points, coal/ lignite conveyor, coal/ lignite Bunker etc.
3. Battery Room is to be properly lined with 'Acid resistance tiles' up to the h[illegible] of 'Battery Bank'. It is suggested to provide Flame-proof lighting in the Batte[illegible]

room. It is also to be ensured that the Eye-wash system is located at a place nearby to the Battery Room.

4. Cable gallery/ racks must be maintained in healthy conditions with proper illumination levels, exhaust system and the cable dressing in the racks should be done properly. All entry & exit of cables must be sealed properly for preventing progression of fire and toxic gases to adjacent rooms.
5. Insulating floor or mat conforming to IS:15652 of appropriate voltage level shall be provided in front of the panels for the safety of operating personnel.
6. Regularly measure and maintain proper records of Resistance value of Earth pits and monitor Tan-Delta value of current transformers (CT) and all other oil-filled electrical equipment.
7. Oil soak pits of transformers should be kept free of waste material.
8. Manuals and Standard Operating Procedures (SOPs) for Ash Bund/ Dyke Maintenance should be prepared by Power Plant. Emergency Plan should be prepared to deal situations of Ash Dyke breach and should be made available to the Site engineers.

****

ANNEXURE-R15

दूरभाष Tel.- 26967840 / 42 / 45, 26967990, 26868681
ई-मेल e-mail : nrpccomml@yahoo.com
वैबसाइट Website : www.nrpc.gov.in
फैक्स Fax : 26865206

भारत सरकार
उत्तरी क्षेत्रीय विद्युत समिति
18-ए, शहीद जीत सिंह मार्ग, कटवारिया सराय, नई दिल्ली-110016.
Government of India
NORTHERN REGIONAL POWER COMMITTEE
18-A, Shaheed Jeet Singh Marg, Katwaria Sarai, New Delhi-110016.

पत्रांक : उक्षेविस/अधी.अभि.(वाणि)/12-क्षे.वि.स/09/1272-135/ दिनाँक :06 -05-2009
No. NRPC / SE(C) /12-RPC / 09 / Dated : -05-2009

सेवा में,
To,

उत्तरी क्षेत्रीय विद्युत समिति तथा तकनीकी समन्वय उप-समिति के सदस्य
(संलग्न सूची के अनुसार)
Members of Northern Regional Power Committee and TCC
(As per list attached)

विषय : तकनीकी समन्वय उप-समिति की 11वीं बैठक तथा उत्तरी क्षेत्रीय विद्युत समिति की 12 वीं बैठक का कार्यवृत्त।
Subject : 11th meeting of TCC and 12th meeting of Northern Regional Power Committee - Minutes.

महोदय,
Sir,

तकनीकी समन्वय उप-समिति की 11वीं बैठक तथा उत्तरी क्षेत्रीय विद्युत समिति की 12वीं बैठक क्रमशः 21 अप्रैल , 2009 व 22 अप्रैल , 2009 को चंडीगढ में आयोजित की गयी थीं। इन बैठकों के कार्यवृत्त की एक प्रति आपकी सूचना व आवश्यक कार्यवाही हेतु इस पत्र के साथ संलग्न है।

The 11th meeting of TCC and 12th meeting of Northern Regional Power Committee were held on 21st April, 2009 and 22nd April, 2009 respectively at Chandigarh. A copy of the summary record of discussions of the meetings is enclosed herewith for favour of information and necessary action.

संलग्नक : यथोपरि ।
Encl. : As above.

भवदीय,
Yours faithfully,

अशोक अग्रवाल 06/05/2009

(अशोक कुमार अग्रवाल)
(A. K. Aggarwal)
सदस्य सचिव
Member Secretary

NORTHERN REGIONAL POWER COMMITTEE

SUMMARY RECORD OF DISCUSSIONS

OF

11th MEETING OF TECHNICAL COORDINATION SUB-COMMITTEE

&

12th MEETING OF NORTHERN REGIONAL POWER COMMITTEE

The 11th meeting of Technical Coordination Sub-committee (TCC) and 12th meeting of Northern Regional Power Committee (NRPC) were held on 21st & 22nd April, 2009 respectively at Chandigarh. The lists of participants at the TCC and NRPC meetings are enclosed at Annexure-I & II respectively.

PROCEEDINGS OF 11th MEETING OF TCC

Shri Sanjay Kumar, Secretary (Power), UT of Chandigarh welcomed all the members of Technical Co-ordination Committee and other delegates. He congratulated NRPC in establishing such platform where the regional level technical problems relating to power are being discussed and resolved. He stated that a healthy power sector is a prime mover of development of economy of any country. Many countries in the past had been able to restructure their economies through reforming their power sector. He gave example of China in this regard. Unfortunately the power sector in India had been still beset with the problems like poor quality, high T&D losses. However, Chandigarh had been fulfilling the vision of Ministry of Power to provide reliable, affordable and quality power for all by 2012. By taking various measures, Chandigarh Administration had been able to reduce T&D losses to around 16.5%.

He further mentioned that Chandigarh had no source of own power generation and totally dependent on allocation from Central generating stations. Chandigarh had peaking shortages of 50 MW and being the Capital of two States they could not afford to impose power cuts. He stated that this small gap could be easily bridged with increase in allocation out of unallocated quota from Central generating stations.

He thanked Member Secretary, NRPC for giving them the opportunity to host the meeting.

Shri A.K. Aggarwal, Member Secretary, NRPC, welcomed TCC Members & other participants. He also welcomed Shri R.K.Seli, Development Commissioner, PDD, J&K on taking over the charge of Chairman, TCC w.e.f.1st April, 2009. He expressed hope that his presence would help TCC resolve the issues amicably. He

thanked Shri Sanjay Kumar, Secretary (Power), UT of Chandigarh, Sh. Surinder Pal, Chief Engineer, and their team of officers for hosting the meeting and making an excellent arrangements for the same as well as for comfortable stay of the participants at Chandigarh. He briefly mentioned the issues to be deliberated in the TCC meeting. Thereafter, he requested Shri R.K.Seli, Chairman, TCC to address the Sub-Committee.

Shri R.K.Seli, Chairman, TCC welcomed the TCC Members & other delegates. In the opening remarks, he appreciated the efforts by the POWERGRID and State TRANSCOs which had carried out insulator cleaning before/during the winter season due to which there were not much tripping of lines due to fog unlike last winter season. He requested all the constituents to take suitable measures to meet the demand in this summer months. He briefly mentioned about the CERC's new regulations on Unscheduled Interchange charges and also the amendments to Indian Electricity Grid Code (IEGC) applicable w.e.f. 1.4.2009 and requested all the members to follow the regulations of CERC strictly. He stressed the need for installation of shunt capacitors by the State utilities, which had been resulting into low voltage problems at certain locations in all the States. Regarding the generation planned during the year 2009-10, he requested generating companies to take all necessary steps to see that there is no slippage in meeting the target.

He thanked Shri Sanjay Kumar, Secretary (Power), UT of Chandigarh, Sh. Surinder Pal, Chief Engineer, and their team of officers for hosting the meeting at Chandigarh and making excellent arrangements for comfortable stay of the participants.

He then requested Member Secretary, NRPC to take up the agenda for discussions.

A. CONFIRMATION OF MINUTES (TCC)

A.1 MINUTES OF 10th MEETING OF TCC OF NRPC

Member Secretary, NRPC stated that as no request for amendment to the minutes had been received, the minutes of 10th TCC could be confirmed.

The members confirmed the minutes of 10th meeting of TCC.

PROCEEDINGS OF 12th MEETING OF NRPC

Shri Sanjay Kumar, Secretary (Power), UT of Chandigarh welcomed Chairman, NRPC, Shri R.K.Seli, Chairman, TCC, Member (GO&D), CEA, Member

Secretary, NRPC, and distinguished members of NRPC and other delegates in the meeting. He expressed that as discussed during the TCC meeting, we should continue the discussion to achieve outcome in the NRPC meeting. He stated that we all should endeavor to achieve what had been mandated not only in this meeting but otherwise also.

Shri A.K. Aggarwal, Member Secretary, NRPC welcomed members of Northern Regional Power Committee and other delegates to the meeting. He especially welcomed Shri Sundeep K Nayak, Commissioner and Secretary, PDD, J&K who took over charge of Chairman, Northern Regional Power Committee on 1.4.2009 on relinquishment of charge by Shri R.K.Jain , Chairman, HPSEB as Chairman, NRPC. He further stated during his tenure as Chairman, NRPC, Shri Jain had played an important role in resolving a number of operational, commercial & administrative issues. He had been a source of inspiration and provided continuous guidance. On behalf of NRPC, Member Secretary, NRPC thanked Shri Jain for his valuable contribution during his tenure.

The Committee passed the following resolution in appreciation of the services rendered by Shri R.K.Jain, Chairman, HPSEB during his tenure as Chairman, NRPC:

"Northern Regional Power Committee places on record its deep appreciation of the outstanding service rendered by Shri R.K.Jain , Chairman, HPSEB during his tenure as Chairman, NRPC. Shri Jain provided able guidance in various technical, commercial & administrative matters and made valuable contribution as Chairman of the Committee."

Member Secretary, NRPC also welcomed Shri Sudhansh Pant, CMD, RVPNL, Shri T.Panda, MD, PTCUL and Shri J.M.Lal, MD, UPCL who were attending the meeting for the first time. On behalf of NRPC, he also congratulated Shri H.S. Brar, who had taken over as Chairman, PSEB.

He thanked Shri Sanjay Kumar, Secretary (Power), UT of Chandigarh, Sh. Surinder Pal, Chief Engineer, and their team of officers for hosting the meeting and making an excellent arrangements for the same as well as for comfortable stay of the participants at Chandigarh. He requested Shri Sundeep K Nayak, Chairman, NRPC to address the Committee.

Shri Sundeep K Nayak, Chairman, NRPC welcomed the Members of the Northern Regional Power Committee and other delegates to the meeting.

He stated that during this winter season there had not been much line tripping due to foggy weather as a result of timely action taken by POWERGRID and State TRANSCOs in cleaning of insulators. POWERGRID had particularly done this with the help of Helicopter successfully for the first time in the country. On Behalf of NRPC, he appreciated the efforts by the POWERGRID and State TRANSCOs in minimizing the instances of line tripping due to fog and saving the grid. He also

requested all concerned to continue the work on replacement of porcelain insulators of line with polymers/Anti-fog as per the plan.

Referring to the anticipated power shortages in the coming summer, he requested all the constituents to manage the shortages by arranging bi-lateral assistance from outside region and maximization of generation as well as suitable demand management measures and statutory / notified load restrictions.

He also informed to the Committee about the new regulations on Unscheduled Interchange charges for electricity grid operations and also the amendments to Indian Electricity Grid Code (IEGC) notified by CERC and applicable w.e.f. 1.4.2009. He stated that CERC had narrowed down the operating frequency band from 49.0 -50.5 Hz to 49.2 to 50.3 Hz. In addition to UI Rate corresponding to frequency of 49.2 Hz, an Additional Unscheduled Interchange Charge at the rate of 40% of the UI Rate corresponding to frequency of 49.2 Hz had been introduced for over-drawal or under-injection of electricity below this frequency. He requested all the members to follow the regulations of CERC other wise CERC could consider penal action under sections 142 and 149 of the Electricity Act, 2003 for contravention of the overdrawl and under generation limit specified in the regulations.

He mentioned that certain locations of almost every States had been experiencing low voltage problems due to inadequate shunt compensation provided by the states. He expressed deep concern about poor progress in installation of shunt capacitors by the State utilities. He requested all the State to expedite the installation of capacitors in the State system to control the low voltage problems.

With regard to generation addition programme during this financial year, he requested the generating companies to take all necessary steps to see that there is no slippage in meeting the generation targets planned during the year 2009-10.

Finally, he thanked Shri Sanjay Kumar, Secretary (Power), UT of Chandigarh, and his team of officers for hosting and making an excellent arrangement for the meeting as well as for stay of the participants at this beautiful city of Chandigarh. Thereafter, he requested Member Secretary, NRPC to take up the agenda for discussions.

A. CONFIRMATION OF MINUTES(NRPC)

A.2 MINUTES OF 11th MEETING OF NRPC

Member Secretary, NRPC stated that as no request for amendment to the minutes had been received, the minutes of 11th NRPC meeting could be confirmed.

The members confirmed the minutes of 11th meeting of NRPC.

B. ITEMS FOR TCC ONLY

FOLLOW-UP ACTION

B.1 STATUS OF SPECIAL PROTECTION SCHEME (SPS) TO TAKE CARE OF TRIPPING OF RIHAND-DADRI HVDC BIPOLE

TCC Deliberation

M.S, NRPC, while briefing the progress made in implementing the SPS scheme on Rihand-Dadri HVDC Bipole line stated that the Special Protection Scheme (SPS) had been declared on commercial operation w.e.f. 1st August, 2008 .

NTPC/POWERGRID informed that circuit modifications as well as testing works had been completed at Rihand and Singrauli STPS. Mock testing of complete scheme would be undertaken in next 15 days.

POWERGRID intimated that after January, 2009 there had been no report of any 'Mal Operation' in the SPS.

B.2 REPLACEMENT OF OBSOLETE ELECTRO MAGNETIC TYPE PROTECTION RELAYS IN NORTHERN REGION WITH STATE-OF-ART NUMERICAL RELAYS.

TCC Deliberation

MS, NRPC briefed the members about the decision of Protection sub committee meeting held on 24/03/09 on the issue and requested all the constituents to replace obsolete electro magnetic type protection relays with numerical relays in the region. He stated that the BBMB, POWERGRID and DTL had already taken action in this regard. Some constituents like UPPCL and PSEB were lagging behind, so they were requested to take immediate action to replace the obsolete relays on critical lines in their systems and replacement of remaining relays by March 2010.

PTCUL stated that they had already replaced the obsolete relays with numerical relays in their system.

HPSEB stated that studies were being conducted by them on the functionality of existing relays. They assured that top priority would be given for replacing the relays in their 220 kV system in the first instance. However, all the relays in their system would be of numerical type by March, 2010.

RRVPNL stated that they had undertaken Renovation, Modernization and Up-gradation (RMU) programme on this issue.

HVPNL stated that they had received 49 numbers of numerical relays from M/s ABB Limited and additional 64 numbers such relays from M/s Areva Limited, which would be replaced soon.

MS, NRPC emphasized that due to limited shut down of lines and more time needed for procurement action, the programme of replacement of relays by constituents need to be coordinated by various constituents. The month wise targets for replacement of obsolete electro magnetic type protection relays in northern region should be fixed in coordination with NRLDC/SLDCs.

TCC decided that all the constituents would complete the process of installation of numerical relays by March, 2010.

NRPC Deliberation

NRPC accepted the recommendations of TCC and decided that all the constituents would complete the process of installation of numerical relays in their systems by March, 2010.

B.3 COORDINATION OF RELAY SETTINGS FOR PROTECTION OF TRANSMISSION LINE IN NORTHERN REGION.

TCC Deliberation

MS, NRPC informed the TCC that the Uniform philosophy for protection of lines to avoid indiscriminate tripping under fault conditions as agreed to in various Protection Sub-Committee Meetings had been widely circulated and it needs to be implemented by all the constituents.

NRPC Deliberation

NRPC noted the information.

B.4 BUS-BAR PROTECTION AT 400 kV AND 220 kV SUB STATIONS

TCC Deliberation

MS, NRPC, requested all the constituents to brief the current status of the bus bar protection on their 400 kV and 220 kV sub stations.

PTCUL stated that they had bus bar protection at all their sub stations.

UPPTCL stated that they had 14 numbers 400 kV sub stations and busbar protection had been provided in these substations. However, at six substations, the bus bar protection was out of order and action was being taken to rectify the same.

ANNEXURE-R16

दूरभाष Tel.- 26967842, 26868681
फैक्स Fax : 26865206
वैबसाइट Website : www.nrpc.gov.in

भारत सरकार
उत्तर क्षेत्रीय विद्युत समिति
18-ए, शहीद जीत सिंह मार्ग, कटवारिया सराय, नई दिल्ली – 110016
Government of India
Northern Regional Power Committee
18-A, Shaheed Jeet Singh Marg, Katwaria Sarai, New Delhi-110016

पत्रांक: उक्षेविस/अधी. अभि.(वा.)/22-क्षे.वि.स./11/ 1685-1754 दिनांक : 05 अगस्त, 2011
No. NRPC / SE(C)/22-RPC /11/ Dated : 05th August, 2011

सेवा में,
To,

उत्तरी क्षेत्रीय विद्युत समिति तथा तकनीकी समंवय उप-समिति के सदस्य

(संलग्न सूची के अनुसार)

Members of Northern Regional Power Committee and TCC
(As per list attached)

विषय : तकनीकी समंवय उप - समिति की 20 वीं बैठक तथा उत्तरी क्षेत्रीय विद्युत समिति की 22 वीं बैठक काकार्यवृत ।

Subject : 20th meeting of TCC and 22nd meeting of Northern Regional Power Committee – Minutes.

महोदय,
Sir,

तकनीकी समंवय उप-समिति की 20 वीं बैठक तथा उत्तरी क्षेत्रीय विद्युत समिति की 22 वीं बैठक क्रमश: 28 व 29 जुलाई, 2011 को होटल होलीडे इनन, जेम पार्क, ऊटी (तमिलनाडु) में आयोजित की गयी थी। इन बैठकों के कार्यवृत की एक प्रति आपकी सूचना व आवश्यक कार्यवाही हेतु इस पत्र के साथ संलग्न है।

The 20th meeting of TCC and 22nd meeting of Northern Regional Power Committee were held on 28th & 29th July, 2011 respectively at Hotel Holiday Inn, Gem Park, Ooty (Tamilnadu). A copy of the summary record of discussions of the meetings is enclosed herewith for favour of information and necessary action.

संलग्नक: यथोपरि ।
Encl: As above

भवदीय,
Yours faithfully,

अग्रवाल 05/08/2011

(अशोक कुमार अग्रवाल)
(A. K. Aggarwal)
सदस्य सचिव
Member Secretary

Signature Not Verified
Digitally signed by PARIMAL PIYUSH
Date: 2024.11.25 22:55:12 IST
Reason: AGM(Commercial)
Location: NTPC Limited

5.14 CONTROL, METERING AND PROTECTION

Following shall be included in the scope of the bidder:

i) Complete control, operation and metering requirements for the following :

- Generator, generator transformer, unit auxiliary transformers and associated circuit breakers
- 11kV incomers, tie feeders and outgoing transformer, supply feeders of unit and station switchgears
- 3.3kV incomers, bus-coupler feeders and outgoing transformer, supply feeders of unit switchgears and incomers of station switchgears
- 415V incomers and bus-coupler feeders of unit and station switchgears
- Diesel Generator sets

ii) Protection and relay panels for generator, generator transformer and UATs including relay test kit

5.14.1 Codes and Standards

IEEE: Std. C37.111	Standard common format for transient data exchange (COMTRADE) for power systems
IEEE Std. C37.90.2	Standard for withstanding capability of relay systems to radiated electromagnetic interference from transceivers
ANSI/ IEEE C37.90	Relays and relay systems standard associated withelectric power apparatus
ANSI/ IEEE C37.93	Power system protective relay applications of audio tones over telephone channels
IS: 3231	Electrical relays for power system protection
IS: 8686	Specification for static protective relays

5.14.2 Control Requirements

i) Operators work station (OWS) along with thin film transistor (TFT) and keyboard etc. shall be located in unit control room and shall be provided for operation, control and interlocking of the following :

- Generator, generator transformer, unit auxiliary transformers and associated circuit breakers
- 11kV incomers, tie feeders and outgoing transformer, supply feeders of unit and station switchgears
- 3.3kV incomers, bus-coupler feeders and outgoing transformer, supply feeders of unit switchgears and incomers of station switchgears
- 415V incomers and bus-coupler feeders of unit and station switchgears
- Diesel Generator sets

ii) General Technical Description

a) Generator

The generator and auxiliary systems shall be controlled from OWS located in unit control room through DDCMIS. All necessary control, interlock, indication, metering and annunciation shall be provided. These controls shall be in addition to local control panels for generator auxiliary systems.

The synchronization of the 400kV Generator transformer circuit breaker shall be performed through auto-synchronizer in DDCMIS. The manual synchronizing shall also be provided in the generator metering panel.

b) Auxiliary power distribution system

The control, monitoring, metering as required for the electrical auxiliary power distribution system comprising of 11kV, 3.3kV, 415V circuit breakers and unit auxiliary transformers, 11kV/3.3kV, 3.3kV/415V auxiliary service transformers within the power block including ESP switchgear shall be performed.

c) Diesel Generator set

The remote control of DG set shall be provided in addition to those provided in associated automatic mains failure (AMF) panels.

5.14.3 Metering

i) Generator

The ammeters, voltmeters, MW meter, MVAR meter, frequency meter, power-factor meter, energy meter (MWH) meter, MVARH meter, exciter field voltage and exciter field current meters including necessary transducers shall be provided in the generator metering panel located in unit control room.

The energy meters mentioned above shall be used for energy accounting and audit purposes and shall be located at a point after the generator stator terminals and before the tap-off to UATs and shall comply with the requirements of CEA regulations on Metering.

The digital indication for the above meters shall also be provided.

ii) 11kV, 3.3kV incomers, tie feeders and outgoing transformer, outgoing supply feeders.

The digital indication of Ammeter, kW meter and kWH meter located on the respective switchgears and bus voltages shall be provided.

iii) 415V Incomer and bus-coupler feeders and Diesel Generator sets

The digital indication of Ammeter, kW meter and kWH meter located on the respective switchgears and bus voltages shall be provided.

5.14.4 Protection and Relay Panels

5.14.4.1 General requirements

i) Panels

a) The panels shall be free standing, floor mounting type and completely metal enclosed. Cable entries shall be from bottom.

b) The panels shall have removable gland plates with glands made of brass and suitable for armoured cables

c) All equipment mounted on front and rear side of the panels shall have individual name plates with equipment designation engraved. Each panel shall also have circuit/ feeder designation name plate.

d) Each panel shall be provided with a 240V AC fluorescent lighting fixture controlled by door switch as well as a 5A, 240V AC switch-socket unit.

e) Voltage circuits for protection and metering shall be protected by fuses. Suitable fuse failure relays shall be provided to give an alarm for voltage circuits of protection/metering. Voltage selection scheme based on relays shall be provided for meters wherever possible.

f) The DC supplies at the individual relay and protection panels shall be monitored by suitable relays and failure of DC supplies shall be annunciated.

ii) Relays

a) The protective relays shall be numerical type. All relays, auxiliary relays and devices shall be of reputed make and types proven for the application and shall be subject to purchaser approval. The relays and timers shall have appropriate setting ranges, accuracy, resetting ratio, transient over-reach and other characteristics to provide required sensitivity to the satisfaction of the owner.

b) Relays shall be suitable for efficient and reliable operation of the protection scheme. Necessary auxiliary relays, timers, trip relays, etc. required for complete scheme, interlocking, alarm, logging, etc. shall be provided. No control relay, which shall trip the circuit breaker when relay is de-energized, shall be employed in the circuits.

c) Relays shall be flush mounted on the front with connections at the rear shall be draw-out or plug-in type/ modular case with proper testing facilities. Provision shall be made for easy isolation of trip circuits for testing and maintenance.

d) Relays shall be provided with self reset contacts except the trip, lockout relays and interlocking (contact multiplication) relays which shall be manual reset type

e) Auxiliary relays shall be provided in the trip circuits of protections located outside the board, such as buchholz relay, temperature indicators, fire protection, etc.

f) Suitable measures shall be provided to ensure that transients present in CT and VT connections due to extraneous sources in 400kV system do not cause damage to static circuit.

g) Only DC/ DC converters shall be provided in the relays, wherever necessary to provide a stable auxiliary supply for relay operation

h) All relays shall have hand-reset flags or other means for ready visual indication of their operation and also of the faulty phase.

i) The numerical relays shall have continuous self-monitoring and cyclical test facilities. The internal clock of the system shall be synchronized through the GPS Time Synchronizing System.

j) Each numerical relay shall have a serial interface on the front for local communication to a PC and Printer. Facilities shall be provided to access each discrete protection function including modification in relay settings and monitoring of the relay from a HMI or a separate protection. The printout of all settings, scheme logic, event records etc. shall be accessible through the HMI. The display of various measured parameters during normal as well as fault conditions on a segregated phase basis shall be provided. LEDs and a backlit LCD screen shall be provided for visual indication and display of messages related to major trips/ alarms. Necessary multilevel password protection shall be provided.

k) The sampling rate of analog inputs, the processing speed and processing cycle of digital values shall be selected to achieve the operating times of various protection functions specified. In case all protection functions specified do not have as a part of the standard numerical relay, separate discrete numerical relays can be provided.

l) The numerical relays shall be provided with built-in disturbance recording facility. The output shall be available in IEEE/ COMTRADE format and shall be compatible with the dynamic relay test kit.

m) The manufacturer of the numerical protection system shall carry out the complete engineering, testing and commissioning on site of the protection equipment including the associated relays and protection panels. The testing and commissioning protocols for the numerical protection systems offered shall be approved by the purchaser before commissioning on site.

n) The numerical relays offered shall have self-diagnostic features to reduce the down time of the relay and to provide useful diagnostic information upon detection of an internal fault so as to speed up the maintenance. The necessary support documentation explaining in detail the self-diagnostic features of the numerical relays shall be furnished for the purchaser's use.

5.14.4.2 Protection

1) Protection Philosophy

- The protection and control equipment and circuitry, shall be provided with two independent channels with reliable protection systems with separate DC supplies, separate CT/ VT cores and separate cables and hand-reset trip relays to obtain 100% reliability. The DC supplies to these protections shall be monitored.

- Associated trip relays of the two systems shall be separate having sufficient number of contacts for all the functions.

- Each protection system shall energize both trip coils of the circuit breaker.

- The total critical fault clearance time from fault initiation in any part of the system shall be 80ms for phase to phase fault in the generator-transformer unit and for phase to phase and phase to earth faults in the 400kV system inter-connection.

- Protective relay system shall be provided to protect the Electrical equipments from faults, overloading and abnormal operating conditions.

2) Each generator, generator transformer and unit auxiliary transformer etc. shall be provided with microprocessor based protection system comprising of the following protections :

i) Generator

a) Differential current protection (87)

b) Inter-turn fault protection (where split winding in stator is provided) if six neutral terminals are available (87TG)

c) 100% stator earth fault protection (64G)

d) Loss of field protection (40) (to be duplicated)

e) Back-up impedance protection (21)

f) Negative sequence current protection (46)

g) Reverse power protection (32) (preferably of 3-phase power relay)

h) Low forward power interlock (37) (preferably of 3-ph. power relay)

i) Rotor earth fault Protection:
- First stage (alarm) (64F1)
- Second stage (trip) (64F2)

j) Over voltage protection (59)

k) Generator pole slipping protection (98)

l) Synchro-check relay (25)

m) Under-frequency protection (based on manufacturer's recommendations, under-frequency relays with timers set at prescribed values connected to alarm and trip (81).

n) Stand by stator earth protection (64G2)

o) Overload (51)

p) Overheating (windings and/ or bearings) (49)(annunciation only)

q) Over fluxing protection in addition to all aforecited protections (99) (to be duplicated)

r) Accidental back energisation protection

s) Voltage balance scheme for blocking voltage dependent protection, in case of VT-fuse failure (60)

In case digital multifunctional generator protection system (MGPS) is provided, the protections shall be duplicated. Each MGPS shall be preferably provided with individual inputs from CTs and VTs and connected to the independent set of hand-reset trip relays, such that one set is always available in case of testing and mal-operation of other set. Any protection, which is not a part of MGPS, separate discrete protection shall be provided as per the above table. The MGPS shall preferably have continuous self-monitoring and testing facilities.

ii) Generator Transformer

a) Overall differential current protection covering the Generator zone also (87OA)

b) Time graded IDMT type back up non-directional over current protection in all phases on HV side (51)

c) Restricted earth fault protection (87NT)

d) Over- fluxing protection (99) (to be duplicated)

e) Neutral over-current protection against sustained external system earth faults (51 NT)

f) Buchholz protection (annunciation and trip) (63)

g) Winding temperature high for annunciation and trip (49T)

h) Oil temperature high (annunciation and trip) (49Q)

i) Pressure relief valve trip (PRV)

j) Generator Transformer differential protection for single phase bank (87T)

k) Overhead line connection differential protection(87L) (For 3 single phase banks, if 87L includes HV winding, separate 87NT is not mandatory)

l) Pole discrepancy protection of the breaker if single pole breakers are used (162)

m) Breaker (HV) back–up protection (protection against breaker failure) (50Z)

iii) Unit Auxiliary Transformer

a) Differential current protection (87)

b) Restricted earth fault protection for LV winding in case of low resistance grounding (87N)

c) Back-up over- current protection on primary side (51)

d) Back-up earth fault protection for low/ high resistance grounding (LV side)

e) Winding temperature high (annunciation and trip LV side breaker) (49T)

f) Oil temperature high (annunciation and trip the LV side breaker) (49Q)

g) Buchholz protection (annunciation and trip) (63)

h) Pressure relief valve trip (PRV)

5.14.5 Generator Disturbance Recorder (DR)

a. One no. microprocessor based Disturbance Recorder (DR) shall be provided for each generator to record graphic form of instantaneous values of voltage and current in all three phases and neutral, open and closed positions of relay contacts and breaker during disturbances.

b. It shall have the facility for slow and fast scan to record transient and dynamic performance of the system.

c. Both slow and fast scan facility shall have atleast 8 analog and 16 digital inputs.

d. The slow scan facility shall be provide with the following minimum features

- The input shall be MW, MVAR, field voltage, frequency and generator terminal voltage etc. Any transducers, if required for interfacing, shall be provided.

- It shall be suitable to record the frequency excursions and response of generator field and governor control on system fluctuations.

- It shall have options to select the scan rate in the range having a min. of 10Hz suitable to facilitate capture of low frequency waveforms in the range of 0.5 - 3Hz.

- The non-volatile memory shall be suitable for recording for a minimum of 15 minute at scan rate corresponding to selected pre-fault zone of recording.

e. The fast scan facility shall be provide with the following minimum features

- The input shall be voltages and current etc. Any transducers, if required for interfacing, shall be provided.

- It shall have scan rate of 1000Hz or better for sampling each of the analog channel having fundamental frequency of 50Hz. The frequency response for these channels shall be DC on the lower side to 500Hz or better on the upper side. Any interposing devices provided shall be suitable for this frequency response.

- The pre and post fault recording time shall be atleast 200 ms and 5s respectively.

f. All external and internal faults in the DR equipment such as power supply fail, printer faults, paper exhausting, processor failure, memory failure etc. are to be indicated by means of light emitting diodes on the front of the panel of restitution unit. The DR shall be provided with a MMI (man machine interface) through a PC with VDU, keyboard and printer.

g. The internal clock of the system shall be synchronized through the GPS. The output shall be in IEEE/ COMTRADE format. The format shall be compatible for dynamic protection Relay Test Kit Necessary interfacing and software for analysis shall also be provided.

h. The amplitude resolution of the analog channels shall not be less than 16 bit and event resolution for digital channels shall be 1ms or better.

5.14.6 Electrical Control Board :

a. One no. 'Electrical Control Board' (ECB) shall also be provided in the Central Control Room with minimum control and indication facilities for various equipments described below, as a back-up to Operator Work Station/ CRT keyboard (OWS) for both units and station supply. ECB shall be Simplex panel in mosaic grid configuration.

b. Semaphore indicators shall be provided for isolators, earth-switches of 400kV system associated with generators. Further, control and indication of the important but not limited to the followings breakers shall also be provided:

i. Generator Transformer breaker (at 400kV), field breaker for both units including manual synchronizing facilities, governor and excitation control.

ii. Incoming and Tie breakers of 11kV, 3.3kV and 415V Unit Switchgears including Unit Emergency Switchgears of both units.

iii. Incoming and Tie breakers of 11kV, 3.3kV and 415V Station Switchgears.

iv. Emergency Diesel Generator sets

c. Relevant Mimic shall be provided to cover the above 400kV, 11kV, 3.3kV and 415V system. Mimic shall be atleast 3 mm thick and 10 mm width and colour coded.

d. The analogue meters for the following shall also be provided on ECB:

i. Generator current, voltage, MW, MVAR, power-factor, frequency, field current, field voltage, etc.

ii. Bus voltages for 400kV, 11kV, 3.3kV and 415V system

NORTHERN REGIONAL POWER COMMITTEE

SUMMARY RECORD OF DISCUSSIONS
OF
20th MEETING OF TECHNICAL COORDINATION SUB-COMMITTEE
&
22nd MEETING OF NORTHERN REGIONAL POWER COMMITTEE

The 20th meeting of Technical Coordination Sub-committee (TCC) and 22nd meeting of Northern Regional Power Committee (NRPC) were held on 28th and 29th June, 2011 respectively at Ooty (Tamilnadu). The list of participants at the TCC and NRPC meetings is enclosed at Annexure- I & II respectively.

PROCEEDINGS OF 20th MEETING OF TCC

AGM, Commercial, NTPC Shri C.K.Mondal welcomed the TCC Members & other participants to the 20th TCC meeting. He gave brief background of NTPC Ltd. and its future plans.

Shri A.K. Aggarwal, Member Secretary, NRPC, welcomed TCC Members & other participants. He informed that as per decision taken in last NRPC meeting, an interactive workshop was organised successfully to clarify the issues related to implementation of POC transmission charges. He also stated that CERC regulation on PoC charges & losses has come into force from 01/07/2011. The Commission vide its order dated 29.06.2011 have approved three slab rates for POC transmission charges. The Commission has also approved POC losses in percentage and its applicable slab.

He emphasized the need for adequate protection Systems its upkeep by carrying out regular protection audit to avoid multiple tripping of transmission lines and other system elements. He also stressed the need to expedite System Protection Scheme as recommended by inquiry committee to minimise the impact of incidents in the grid.

MS, NRPC mentioned that the NR met highest demand of 38000 MW. Peak power shortage was around 6% and average energy shortage was about 4% in July. The average grid frequency was also around 49.9 HZ during this period. He touched upon the instances of heavy overdrawal by some States, huge reactive power drawal causing low voltages and TTC violations.
He expressed concern on extremely slow progress of installation of requisite quantum of shunt capacitors and associated low voltage problem. He requested States utilities, particularly those having paddy crops, to take up revival of defective capacitors and installation of new capacitors on war footing apart from maintaining their distribution system.
He requested for cooperation of all concerned in resolving long pending issues such as Installation of adequate Capacitors & revival of defective Capacitors, AMRs for Interface

meters, Pollution Mapping, Third party Protection Audit, Replacement of obsolete protection relays with Numerical Relays.
With regard to capacity building he informed that 9 training programmes are being organised on reactive power management during the FY 2011-12 to enhance the capacity building of system operators and field staff.
He thanked Shri I.J.Kapoor, Director(commercial), NTPC, Shri Naresh Anand, AGM, NTPC and their team of officers for hosting and making excellent arrangements for the meeting as well as for stay of the participants at Ooty.

Shri Y.Raizada, Director (Tech.), RVPNL and Chairman, TCC welcomed the TCC Members & other delegates. Referring to the grid operation he expressed that the Power Supply Position during the period from April 2011- June 2011 was quite comfortable. The shortages were manageable. The grid frequency was for most of the time within the frequency band as stipulated in IEGC. In addition to the need for installation of Capacitors he emphasized the need for installation of reactors in view of the high voltages being faced in certain pockets.

Finally, he thanked Shri I.J.Kapoor, Director (commercial), NTPC and their team of officers for hosting and making excellent arrangements for the meeting as well as for stay of the participants at Ooty.

He then requested Member Secretary, NRPC to take up the agenda for discussions.

C O N F I R M A T I O N O F M I N U T E S (T C C)

A.1 Minutes of 19th Meeting of TCC of NRPC

MS, NRPC stated that the minutes of 19th meeting of TCC held at Parwanoo, on 1st June, 2011, were circulated vide letter No. NRPC / SE(C) / 21-RPC / 11/1038-1108 dated 27th June, 2011. As no comments had been received on TCC minutes, he proposed for confirmation of minutes.

TCC confirmed the minutes of meeting.

P R O C E E D I N G S O F 2 2 n d M E E T I N G O F N R P C

Shri I.J.Kapoor, Director(commercial), NTPC welcomed the NRPC Members & other participants to the 22nd NRPC meeting. He briefly explained the future plans of NTPC Ltd. As Shri A.K.Aggarwal, Member Secretary, NRPC is superannuating in August 2011, he appreciated the services rendered and hard work in resolving the important technical & commercial issues by Shri A.K.Aggarwal, Member Secretary, NRPC during his tenure as Member Secretary NRPC.

Shri A.K. Aggarwal, Member Secretary, NRPC welcomed members of Northern Regional Power Committee and other delegates to the meeting. He especially welcomed Shri Anurag Agarwal Ex-Chairman NRPC and CMD, Punjab State Transmission Corporation Ltd. During his tenure many visionary decisions taken with consensus in NRPC. He also welcomed Sh I.J.Kapoor, Director (Commercial) NTPC, Shri K. D. Chaudhary CMD, Punjab State Power Corporation Ltd, Sh A.K.Jain MD, Uttrakhand Power Trans. Co Ltd who are attending the meeting for the first time.

He informed that during the TCC meeting 30 agenda items covering technical, commercial and operational issues were discussed. He briefly explained the important issues such as Installation of adequate Capacitors & Revival of defective Capacitors, AMRs for Interface meters, Pollution Mapping, Third Party Protection Audit, Bus Bar Protection and implementation of System Protection Scheme as recommended by inquiry committee.

He further stated that as suggested by Chairman NRPC in last meeting, the matter had been taken up with CEA to establish a forum of all RPCs. This will bring uniformity on various common issues like certifying of additional generation due to re-scheduling of the planned maintenance programme, Non-ISTS lines, protection Co-ordination and Audit apart from sharing of best practices of each RPC.

He thanked Shri I.J.Kapoor, Director(commercial), NTPC, Shri Naresh Anand, AGM, NTPC and their team of officers for hosting and making excellent arrangements for the meeting as well as for stay of the participants at Ooty.

Shri Shailendra Agarwal , Chairman, NRPC welcomed members of Northern Regional Power Committee and other delegates to the meeting. He informed that the power supply during the April to June 2011 quarter was quite comfortable. He expressed concern over heavy overdrawal of power from the grid by many States. Some of the constituents sell power through power exchange and at the same time overdraw power from the grid endangering the grid security. He also stated that the overdrawal of power is not in the interest of safe and secure operation of grid. He expressed that only policy frame work would take care of such issues. He proposed that Heads of the power utilities needs to be informed in this regard.

He further stated that same agenda items had been repeating from last many of the meetings. He stressed the need for action from the utilities so that these issues get resolved.

He expressed happiness that the issue of formation of RPC forum at national level as decided in the last NRPC meeting was being examined in CEA.

Finally, he thanked Shri I.J.Kapoor, Director (commercial), NTPC and their dedicated team of officers for hosting and making excellent arrangements for the meeting.

He then requested Member Secretary, NRPC to take up the agenda for discussions.

C O N F I R M A T I O N O F M I N U T E S (N R P C)

A.2 Minutes of 20th Meeting of NRPC

MS, NRPC stated that the minutes of 20th meeting of NRPC held at Dehradun, on 1st March. , 2011, were circulated vide letter No. NRPC / SE(C) / 21-RPC / 11/1038-1108 dated 27th June, 2011. BBMB had requested for amendment in the minutes as given below:

"BBMB stated that the Board may recommend adoption of average YTC for BBMB to which no Constituent objected. Chairman, TCC also stated that there was no objection to the proposal of BBMB. The proposal of BBMB and its acceptance by the TCC may be intimated to concerned agencies for adoption."

The members confirmed the minutes of 20th meeting of NRPC with the above amendments.

I T E M S F O R T C C A N D N R P C

O P E R A T I O N A L I S S U E S

B.1 Status of Major Decisions of NRPC.

The deliberations in the TCC and NRPC meeting are given at **Annexure- III**.

B.2 Status of Implementation of action plan for partial Grid Disturbance on 2nd January, 2010.

TCC Deliberations.

MS,NRPC stated that Northern Region had experienced a partial gird disturbance on 2nd January 2010 in which power supply in Punjab, North Haryana, Himachal Pradesh, J&K and UT Chandigarh sub system was affected. Central Electricity Authority had constituted a Committee under the Chairmanship of Member (GO&D), CEA, to inquire into the grid incident and ascertain the cause of grid disturbance and suggest remedial measures to avoid recurrence of such incident. The committee had submitted its Report along with recommendations to the Authority in May 2010. He added that the recommendations along with progress of implementation is being regularly monitored in OCC meetings. Further, he mentioned that presently the focus is on implementation of three major recommendations.

Annex-III

Major Decisions in earlier NRPC Meetings

Sr. No	Issues Discussed	Decisions Taken/discussions in the subsequent meetings.	20th TCC Deliberations	22nd NRPC Deliberations
1.	**12th NRPC meeting held on 22nd April, 2009 in Chandigarh**			
1.1	Replacement of obsolete protection relays with State of numerical relays	All the constituents agreed to complete the process of installation of numerical relays in their system by March 2010. Not Much progress has been achieved; NRPC had referred the matter to Protection Sub Committee for early implementation of NRPC decision. The matter was discussed in 14th PSC meeting, wherein it was suggested that since the cost of replacing all relays would involve huge investments, so numerical relays must be provided in new system elements and for old system elements, the relay would be replaced in a phased manner. Utilities had also agreed to submit time line for replacement of obsolete protection relays to NRPC Secretariat. In UP, all new S/s are being provided with numerical relays. In addition, 446 numerical relays have been procured & out of these, 311 relays have been replaced.	To size the problem, NRPC Secretariat would prepare a format for capturing the information. Constituents would submit the information before next Protection Sub-Committee meeting.	Members noted the deliberation of TCC.
2	**13th NRPC meeting held on 24th June, 2009 at Lucknow**			
2.1	Automatic Meter Reading(AMR) for SEMs	The proposal for implementation of AMR through POWERGRID was approved by NRPC. In **21st NRPC meeting,** POWERGRID had informed that the investment has been approved on 30.05.2011 and the work would be awarded in 3 months and would be implemented in 1 year thereafter. While implementing, priority shall be accorded to locations from where data is getting delayed at present POWERGRID was requested to take timely actions to meet the time line.	NIT issued. Bids are to be opened in August 2011.	Members noted the deliberation of TCC.
3	**In 14th meeting held on 9th September 2009 at Surajkund**			
3.1	Procurement	Procurement of 315 MVA, 400/220 kV	Delivery for 315 MVA's	noted