Additional Agenda -1 for TeST Sub-Committee Meeting
dated 07.08.2019

2.9   OPGW Connectivity at Bhadla Pooling Stations (Agenda by NRLDC)

2.9.1   Bhadla Pooling Station was first time charged in the month of March 2019. The SCADA data of Bhadla was to be integrated on OPGW through 765 KV Bhadla-Bikaner Line. But due to non-commissioning of the 765kV Bhadla-Bikaner line, data was transferred to NRLDC over GPRS which is highly intermittent.

2.9.2   Further, this is to inform you that many Solar Power Plants are getting connected at Bhadla PG. As per Connectivity agreement data of these solar plants has to be integrated with OPGW at Bhadla PG.

2.9.3   Due to unavailability of OPGW at Bhadla PG data transmission from these sub-stations is also getting affected as they are also integrating through GPRS Network.

2.9.4   At Present approximately 700 MW {Adani Power (250MW), Saurya Urja (200MW), and Mahoba Solar (250MW)} has already been integrated in the grid and non-availability of data from these sub-stations is causing constraint in smooth grid operation. Further, 580 MW {Azure (130 MW), Tata Power (150 MW) & Clean Solar (300 MW)} is likely to be connected in near future.

2.9.5   As you are aware there is evacuation constraint at Bhadla Pooling Station and proper visualization of data from these Solar Power Parks is very essential for smooth monitoring and reliable grid operation.

2.9.6   Due to non-availability of OPGW at Bhadla PG we are facing following issues at NRLDC.

a)   High intermittency of RTU data from Bhadla (85%), Adani Power (94%) and Saurya Urja (79%).

b)   Non availability of PMU data from these sub-stations

c)   Non availability of dedicated Voice communication with Solar Power Parks.

2.9.7   It is learnt that alternate arrangement of fiber connectivity to Bhadla PG has been done by PGCIL, PGCIL may confirm the same and arrangements may be made for shifting of data at the earliest.

PGCIL to update the status.

2.10 Signing of side letters of MoU for AMC (Agenda by POWERGRID)

2.10.1 Side letter of MoU for maintenance of RTUs, OPGW, Wideband was send to respective constituents long back. However, side letters for MoUs are yet to be signed by following Constituents and payment got stuck

a) PTCUL – RTU (Long pending)

b) J&K PDD – OPGW and Wideband

c) UPPTCL – all (OPGW, wideband, APS,etc).

2.10.2 It is once again requested to expedite the signing of side letter to MoUs immediately otherwise it is difficult to carry out the AMC works without MOU in place.

2.11 Non-issuance of PTW (Agenda by POWERGRID)

2.11.1 Non-issuance of PTW / auto relay setting code for OPGW works in 400kV Dadri-Maharanibagh and Dadri-Mandola under Reliable communication package, permission for change in relay setting from Auto to non-auto mode got repetitively (since April'2019) cancelled due to perceived grid security in respective OCC meetings and work will be delayed.

2.12 Implementation of Multisite Configuration between BBMB SLDC Chandigarh and SLDC Patiala. (Agenda by BBMB)

2.11.2 The following Multisite Configurations are yet to be implemented by M/s SIEMENS:
a) Scheduling and UI rate calculations to be implemented between Backup Control Centre and NRLDC.
b) Flow of BBMB ICCP data between Backup Control Centre and NRLDC.

2.11.3 Further, the following SIEMENS make RTUs are yet to be configured for multisite due to non-availability/provision of communication links between RTU and PSTCL Patiala.
- Bhakra Left
- Bhakra Right
- Pong
- Dehar
- Bhiwani
- Chandigarh

M/s SIEMENS is to implement the pending Multisite Configuration without further delay.

M/s PGCIL to provide communication links for multisite configuration of the left out RTUs.

Cyber Security of SCADA/EMS System

3.4 Cyber Security of SCADA/EMS System (Agenda by BBMB)

As per Govt. of India, Ministry of Power Office Memorandum dated 2nd August 2017 (**Annexure-3.4**) regarding steps to be taken to prevent cyber incidents due to malware, under the heading "Important and immediate steps need to be taken by the Power Sector Companies" (point (iv)), it has been mentioned that:

"No use of Word processing software Power Point, Excel sheets on ICT systems deployed *in the operational network".*

In this regard, preparation of Control Room Reports and extraction of history data from SCADA/EMS System installed under ULDC Phase-2 is being done by using MS Excel

Members may discuss please.

5.2 PMUs installed under URTDSM Scheme at 400 kV Substations / Power Houses of BBMB. (Agenda by BBMB)

5.2.1 Due to phase mismatch of 400 kV viz-a-viz 220 kV system at 400 kV Substations / Power Houses of BBMB, phasor mismatch is being observed in the PMUs installed under URTDSM Scheme. POWERGRID is requested to impart necessary instructions to M/s GE to alter the phase sequence wiring in PMUs installed at Dehar Power House, Bhiwani & Panipat substations of BBMB, so as to rectify the discrepancy in the phasor mismatch being observed in the PMUs installed under URTDSM Scheme.

6.8 Delay in Payment (Agenda by POWERGRID)

6.8.1 POWERGRID is providing consultancy services on RTU/APS/Wideband/OPGW maintenance to constituents on overhead charges basis as per MOU signed with respective Constituents. Constituents are paying on quarterly or yearly basis with advance payment, however even advance payments are being released on delay of 5-6 months and in some cases the delay is of up to one and more years which is not acceptable and POWERGRID have no other option to deduct the overhead charges from advance 1% deposited with us and cancellation of AMC with immediate effects.

6.8.2 Outstanding payment:

DTL – approx. Rs. 5 Lacs (RTU)

J&K PDD – Approx. Rs 13 Lac (APS, OPGW, RTU, wideband & Insurance)

PTCUL – approx. Rs 5 Lac (RTU, APS, OPGW & short payments)

UPPTCL – approx. Rs 50 Lac (APS, RTU, OPGW, wideband)

HPSEBL- approx. Rs 5 Lac (RTU, OPGW, wideband & APS)

6.8.3 Above outstanding amounts are pending since long and POWERGRID is regularly pursuing the case with respective Constituents however settlement of payment issue was not closed till date even repeated reminders. Now POWERGRID is going to stop AMC works for UPPTCL, PTCUL and J&K PDD where payment has not been released since long and total outstanding is also very huge.

6.9   Pending TDS (Agenda by POWERGRID)

6.9.1 All Constituents are requested to submit Quarterly TDS certificate in time against payment made to POWERGRID for Consultancy / AMC services which is required to match the books of Accounts.

6.9.2 In view of non-payment of insurance charges, all constituents are requested to do their insurance at their own. POWERGRID is not taking may overhead charges, audit has also objected several times for this type of works without any overhead charges and delay in payment.

Annexure-3.4

SECRET

F No 1/6/2011/IT-Pt VIII (238324)
Government of India
Ministry of Power

Shram Shakti Bhawan, Rafi Marg
New Delhi, dated 2nd August, 2017

OFFICE MEMORANDUM

Subject : Steps to be taken to prevent cyber incidents due to malware.

The undersigned is directed to inform that a highly suspicious communication is being observed on the Internet in the country. An advance software script (malware), is associated in such suspicious communication. The said software script is targeted specifically for the Energy sector to infect devices to steal information/ steal password to get foothold in the ICT Networks deployed in power generation, distribution and transmission sector and pass over to the adversaries outside the country. The software script also has the capability to encrypt entire information on the computer system. In some cases, the data hosted or stored on the computer terminals may be lost permanently. The software script connects to a malicious domain, the location of which keeps on changing in Germany and Russia. However, the structure of data which is communicating the stolen information to outside the country is in different format.

2.   The cyber incidents involving energy and power sector are on increase worldwide. The ICT infrastructure, especially, that of power grid is under cyber threat. The Eastern Regional Load Dispatch Centre (ERLDC), wholly subsidiary of Power Grid Corporation of India has been in severe attack in the recent past. Their infrastructure has been found to be infected and compromised with software script which has the capability to destroy some functionality of the ICT system

3.   In view of above it is requested to take specific steps as listed in Annexure to prevent cyber incidents which may take place due to the suspicious communication flowing on the Internet.

4.   This issues with the approval of competent authority.

Encl: As above.

(Praveen Kumar)
Under Secretary to Government of India
it-mop@nic in

To,

1. Chairperson, CEA, R.K. Puram, New Delhi
2. CMDs of NTPC, NHPC, NEEPCO, SJVNL, THDC, REC, PGCIL, PFC
3. Chairman of DVC, BBMB, POSOCO
4. Director General BEE, NPTI,CPRI
5. Registrar ATE.
6. Secretary, CERC
7. MD, EESL
8. CERT-Thermal/Hydro/Trans/Distribution
9. CISO MoP/CE(IT)CEA

ANNEXURE I

I. Mechanism by which the Malicious Software Script impact the Power Sector

(i) Exploitation of vulnerabilities in the old versions of Microsoft Windows OS and Microsoft Office products (Excel, Word and PPT) used in the ICT system

(ii) Network components and network products which are not upgraded with the latest upgrades with respect to cyber security

(iii) Sending Phishing mails

(iv) Removable media like Pen drives

(v) Lack of update antivirus, firewall etc.

II. Important and immediate steps need to be taken by the Power Sector companies

(i) The organizations must audit their ICT network and systems with respect to the upgrades and updates of anti-virus, operating system and other software and apply upgrades and updates immediately

(ii) Review security policies for email distribution, screening and usage by all users of power sector companies

(iii) Business Network (with email access) and Operational Network should be fully isolated. The Control System of Power Plant and other vital plant components are not connected to Business Network or the Internet

(iv) No use of Word processing software, Power Point, Excel sheets on ICT systems deployed in the operational network.

(v) All Desktop systems connected on the operational and business network be reviewed with respect to the need for pen drives and other removable media. The pen drives in the operational network should mandatorily be disabled

(vi) All Desktop systems/devices to be audited for latest software updates for new version of MS windows. Discontinue use of Window XP or older versions. SMB or other similar functions need to be disabled to reduce the cyber incidents

(vii) Organization must analyse all outgoing and incoming communication traffic to the operational and business network. Deep Packet Inspection System and Netflow system be installed

Analysis of communication traffic to identify suspicious and to minimize the impact of already compromised systems or systems with existing backdoors

Sandbox – the use of Microsoft Word, Power Point and Excel to minimize their phishing

Organization must disable execution of scripts and internet cookies

The organization must create white listing of authorized applications for network use and disallow all other applications from using the network

The application white listing will ensure that malware, ransomware etc. are made ineffective in operational and business networks

No upgrade/update be downloaded and applied directly on the devices connected on the Operational Network. The updates and upgrades be downloaded on separate computer systems examine its behavior and thereafter applied on the computing devices connected on both Operational and Business Network