File No.CEA-PS-17-13/2/2021-PCD Division/ 481

आज़ादी का अमृत महोत्सव

भारत सरकार
Government of India
विद्युत मंत्रालय
Ministry of Power
केन्द्रीय विद्युत प्राधिकरण
Central Electricity Authority
विद्युत संचार विकास प्रभाग
Power Communication Development Division
****

विषय - विद्युत प्रणाली संचालन में संचार योजना के नियमावली – के संबंध में

प्राधिकरण ने विद्युत प्रणाली संचालन में संचार योजना के नियमावली को दिनांक 31.03.2022 को प्रकाशित किया है| सेंट्रल ट्रांसमिशन यूटिलिटी ने मैनुअल के कुछ खंडों पर स्पष्टीकरण मांगा है।

इस संबंध में खंड-वार स्पष्टीकरण (अनुलग्नक) जारी किए जाते हैं।

संलग्न:- उपरोक्त अनुसार

— sd —

मुख्य अभियंता

To:-
1. COO, CTU
2. MDs/CMDs, STUs
3. CMD, POSOCO
4. CMD, POWERGRID

Copy for kind information to:-
1. Chairperson, Central Electricity Authority
2. Chairperson, Central Electricity Regulatory Commission
3. Member (Power System), Central Electricity Authority
4. Joint Secretary (Trans), Ministry of Power

Annexure

Clarification sought by CTU on certain clauses of "Manual of Communication Planning in Power System Operation"

S. No.	Clause	Clarification sought by CTU	Clarification Issued
1	**Clause 3.2**: While the Cross Border, National, Regional and intra-state ISTS communication systems are to be planned by CTU, the State Communication systems are to be planned by respective STUs up to their interface point with DISCOMs.	"intra-state ISTS communication systems" need more clarity. To be discussed	"intra-state ISTS communication system" refers to communication system on those non ISTS lines which are being used/are part of ISTS communication.
2	**Clause 3.4:** Cyber security is to be ensured by the respective nodal agencies while planning interfaces between two networks of two different entities like DISCOMs, STUs and ISTS licensees and while connecting a new user to the existing communication system.	Clear identification of nodal agency at such points and how will the nodal agency ensure the specific cyber security planning.	Nodal agencies for different level of communication systems have already been defined in the manual. For planning of cyber security, clause 6 of the manual may be referred.
3	**Clause 3.6:** The communication planning process starts with first phase, involving assessment of requirement for expansion of nodes, upgradation of existing network, new connectivity requirements etc. Second phase considers design for the functional level for services like tele-protection, SCADA, video-surveillance, PMU, tele-metering, voice, automated metering application, IT requirement etc. and technologies like switching, routing, etc. Finally, the network design and planning are performed taking physical media, equipment, security risks, protocols, interfacing requirements, management aspects etc. into consideration.	IT requirement needs to be clarified.	IT requirement referred in the Manual are used by some utilities with proper isolation of IT and OT networks to run different applications in Power Sector.
4	**Clause 4.1.2:** To ensure redundancy with route diversity, each communication	To be discussed for MSP, SNCP and route diversity.	For maintaining route diversity the working path and protection path

Annexure

Clarification sought by CTU on certain clauses of "Manual of Communication Planning in Power System Operation"

	channel (working path) planned for the Users shall be provided with alternate channel (protection path) in different routes, i.e., the working path and protection path should be resource disjoint. For last mile connectivity to load dispatch center, additional redundancy in different route may be considered. In case of failure of the working path, the protection path shall be available for the required communication services.		should be resource disjoint i.e. there should be no common intervening path between the working path and protection path.
5	**Clause 4.1.12:** The requirements of the applicant(s) shall be examined by the concerned nodal agency before allowing the connectivity to the existing communication system. Any augmentation/expansion of the existing communication system shall be planned by the nodal agency to ensure redundancy with route diversity of the allocated communication system. However, in case of radial connectivity to the existing node, the applicant(s) shall develop their own redundant communication system up to the existing wideband node.	In case RE generators or private generators connecting to ISTS node on single dedicated transmission line, how to ensure redundant communication. Whether it should be over leased line or GPRS etc. For new generators CTU may mention redundant path in their ST-II intimations. Same for other radial lines which are coming new.	For new Gencos with availability of one dedicated line only, protection path may be provided by Gencos on diverse communication media like leased line, GPRS etc. Further, Gencos pooling station to ISTS DCP point, a link may also be planned with redundant path as per service requirement and availability of communication media.
6	**Clause 4.4.2:** Following measures, as applicable, may be considered for ensuring reliability of Communication System in case of a link or node failure: (a) Duplicated equipment; (b) Equipment with redundant modules (Power supply, CPU, service cards, access ports, etc.);	Methodology to ensure the reliability as these are in the purview of TSP for their implementation. CTU provides technical inputs to the RfPs.	Nodal agency, while planning the communication system, may incorporate these measures as per applicability for ensuring reliability of Communication System in case of a link or node failure.

Annexure

Clarification sought by CTU on certain clauses of "Manual of Communication Planning in Power System Operation"

	(c) Physically independent communication media (wired or wireless); (d) Different communication technologies (SDH, MPLS, PLCC, Cellular, RF, VSAT etc); (e) Alternate network routes; (f) Distributed processing systems		
7	**Clause 6.4:** Services and applications like PMU, SCADA, protection, AGC, AMR, video surveillance, voice etc may be segregated into different security zones based on risk and impact assessment. Restrictive control over data exchange between different security zones may be done according to the security policy (e.g. firewalls). Consequent to partitioning the services and applications into separate security zones, partitioning of aggregate communication traffic is required which may be achieved by a combination of physical separation (e.g. equipment/link) and virtual separation (e.g. VPNs)	For the cybersecurity of Power sector, CEA has issued (Cyber Security in Power Sector) Guidelines, 2021. CTU has proposed perimeter cybersecurity, to start with, for TBCB projects by implementation of firewalls at the upcoming substations. This firewall proposal was included in the RfP. CEA/CSIRT-Power shall also review the above said firewall proposal and specify additional cybersecurity measures to be taken up in the planning of (new & existing) ISTS communication systems of the ISTS schemes. Guideline for existing substations/ generators to be clarified by CEA/CSIRT-Power.	Specific cyber security measures are not part of the manual.
8	**Clause 6.6:** In case of radial connectivity to the existing node, the user(s) developing their own redundant communication system up to the existing wideband node should follow the cyber security guidelines in practice.	Shall CTU ask Genco/RE Genco/Private/Genco to provide leased line/other communication media network for redundant communication alongwith cyber security measures to provide connectivity to the ISTS communication system.	In case of radial connectivity, a redundant communication system up to the nearest wideband node needs to be developed by the user by ensuring the cybersecurity for such network as per cyber security guidelines in practice.