ISO 9001 : 2008

TEC

टी ई सी संचारिका
NEWSLETTER

Vol. 20 AUGUST 2016 ISSUE 3

Secretary(T) addressing a meeting in TEC

Shri J. S. Deepak, Secretary (T), DoT visited TEC on 09-05-2016. Secretary(T) was welcomed by Sr. DDG, TEC and a meeting with all DDsG of TEC was held. In this meeting, DDG (R) gave a presentation about TEC and the current activities being undertaken by TEC. Secretary(T) in his address talked about vision & Mission of DoT and the role of TEC in the current telecom scenario of India. He emphasized to make the testing activities/procedure of TEC more user friendly so that industry does not face difficulty in this regard.

ISO 9001:2008

TELECOMMUNICATION ENGINEERING CENTRE

IN THIS ISSUE

"Smart Grid Security"

1.0 Introduction

In recent decades the application and use of Information and Communication Technologies (ICT) in Critical Infrastructures, like drinking water systems, energy grids, financial and communication infrastructures have increased enormously. These systems have opened an unforeseen amount of opportunities and have been beneficial for society. The growing dependency on ICT also means that new threats have to be met. The disruption or destruction of electricity grids would have a serious impact on economic and societal functions. In order to keep our infrastructures resilient, we have to invest in secure and resilient architectures. In this newsletter, introduction of Smart Grid architecture along with its functional domains and security of respective functional domains are discussed.

2.0 Smart Grid

A smart electrical grid is defined as an electrical grid, which can integrate the behaviour and actions of all connected users in a cost effective way including producer, consumer and actors, which are both producer and consumer to ensure a resource-saving and economically efficient electrical network with less losses, high quality, great security of supply and high technical safety.

Smart grids provide electricity demand from the centralized and distributed generation stations to the customers through transmission and distribution systems. The grid is operated, controlled and monitored using ICT. These technologies enable energy companies to seamlessly control the power demand and allow for an efficient and reliable power delivery at reduced cost via digital two-way communications between consumers and electric power companies, the smart grid system provides the most efficient electric network operations based on the received consumer's information.

3.0 Smart Grid Architecture

Smart grid architecture may be defined in two ways (on service area domain basis & functional basis);

3.1 Smart Grid Domains:

As per ITU-T Smart Grid architecture consist of five domains 1 to 5 domains and are viewed in three service areas: smart grid service/applications, communications and physical equipment.

i. Grid Domain:
The grid domain provides the bulk generation/transmission/distribution function. Components in the grid domain are classified as the 'smart meter infrastructure' and the 'distribution grid management'.

ii. Customer Domain:
Customer Domain comprises of customer related equipment such as Smart Appliances, Plug in electric Vehicles, heating, ventilating & air conditioning (HVAC) etc.

iii. Service provider Domain:
This domain basically performs application functions & comprises of operators, service providers & governed by market scenarios.

iv. Smart Metering:
This mainly performs metering related functions such as meter reading function, meter control and maintenance function. This domain also deals with fault monitoring and protection.

v. Communication Network:
Mainly performs communication related functions between different domains using telecommunication infrastructure including IP based infrastructure functions.

3.2 Functional Basis:

Smart grid architecture is mainly divided into 6 functional components so as to identify & address the security issues, failure scenarios, threats and vulnerabilities.

3.2.1 Advanced Metering Infrastructure (AMI):

Smart metering infrastructure comprising smart meters at the customer's premises, data concentrators, an AMI headend system and an MDM (Meter Data Management) System. The smart meter is typically located in the customer premises. It has multiple communication interfaces: the uplink employs a proprietary PLC (Programmable Logic Controller) system, which, according to the manufacturer, uses state-of-the-art encryption technologies. Besides the PLC communication interface, there is an optical interface for the configuration and maintenance of the smart meter. Access to the optical interface is protected with a strong password.

The utility uses the same service password for all smart meters. The smart meter firmware is proprietary and can be considered as a black box system to the utility. Additionally, the smart meter contains a remote controllable breaker unit. The data concentrator is the PLC endpoint for the smart meters. Apart from the PLC interface, it has an Ethernet uplink that is connected to the headend system over a fibre optic link secured via VPN. The data concentrators are all situated in physically secure locations such as substations or transformer stations operated by the utility. The headend system is located at the utility and comprises a proprietary manufacturer software implementation that is executed on an off the shelf server system. The system is connected to a metering VLAN to communicate with the data concentrators.

3.2.2 Wide Area Monitoring, Protection, and Control (WAMPAC):

Systems that support wide area applications, related mainly to synchro phasor technology and the devices that generate, receive, and utilise synchro phasor data. WAMPAC is one of most critical component in smart

grid landscape and hence few precautions have been taken by utility for preventing potential attacks. The solutions consist of various combinations of common design elements: Intelligent Electronic Devices (IEDs) capable of collecting samples of input waveforms and calculating phasors, sources for a high precision time synchronization reference, various phasor data concentrators, communications, applications, and visualization tools for data presentation

The system is physically separated from other communication networks. Maintenance operations can only be performed by temporarily enabling access to the maintenance functionalities. From the utility to the field, mostly fibre links are employed that are located at the top of high voltage power poles. Directional radio links are used for a small number of devices in rural areas.

3.2.3 Distribution Grid Management (DGM):

A utility has a wide ranging DGM system in place that ranges from primary and secondary substations to plug-in electric vehicles (PEVs), low voltage generation, or smart buildings. In this utility leverage manufactures in device VPN implementation as mentioned above so that any communication outside the device is cryptographically protected. The configuration is thus comparable to the WAMPAC case study as mentioned above, with the difference that the number of devices which are more easily accessible to attackers is higher.

3.2.4 Demand Response:

The primary focus on the Demand Response (DR) is to provide the customers with pricing information so that the customers or the energy management and control system (EMCS) at the customer's sites may respond based on the demands for electricity and electricity prices during some period of time. For instance, the customer may decrease demand (or shed load) during higher priced time periods or increase demand (or shift load) during lower priced time periods.

3.2.5 Supervisory Control and Data Acquisition (SCADA) System:

SCADA systems are widely deployed in Critical Infrastructure industries where they provide remote supervisory and control. In the Smart Grid, SCADA systems are used in automation. SCADA is a collection of systems that measure, report, and change in real time

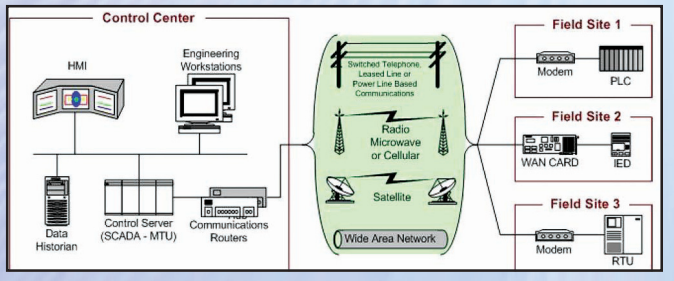

Fig. 1. SCADA general layout

both local and geographically remote distributed processes.

The fundamental components in the above figure are the control centre usually computer based, referred to as MTU (Master Terminal Unit), RTU (Remote Terminal Unit) or also called as field site, and the communication link between them. The MTU issues commands to distant facilities and gathers data from them, interacts with other systems in the corporate intranet for administrative purposes and interfaces with human operators. An operator can interface with a MTU through an interface device consisting in a video display unit, a keyboard, etc. Control commands sent by a MTU to distant facilities are triggered by programs in that MTU which are executed either manually or through a programmable built in scheduler. The SCADA system is a control system which was originally designed to operate in an isolated environment.

3.3 Smart Grid Component:

The Grid can be viewed as having mainly two types of components; System component and Network component.

3.3.1. System Component:

The major system components in smart grid are Smart meter, Electrical household appliances, Renewable energy sources, Electric utility providers and Service Providers.

3.3.2. Network Component:

Smart grid incorporates two types of communication networks: Home Area Network (HAN) and Wide Area Network (WAN). A HAN connects the in-house smart devices across the home with the smart meter. The HAN can communicate using Zigbee, wired or wireless Ethernet, or Bluetooth. A WAN, on the other hand, is a bigger network that connects the smart meters, service providers, and electric utility.

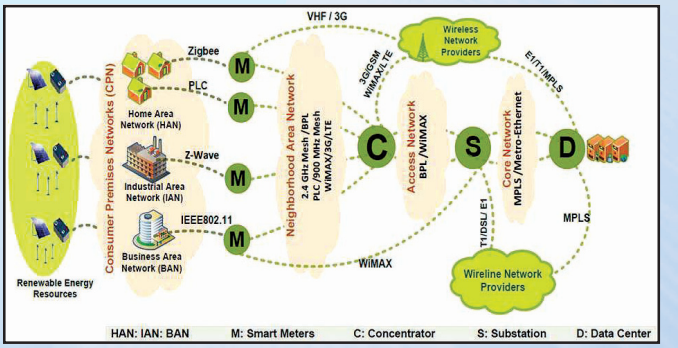

Fig. 2. Basic Network Architecture

The WAN can communicate using WiMAX, 3G/GSM/ LTE, or fibre optics. The smart meter acts as a gateway between the in-house devices and the external parties to provide the needed information. The electric utility manages the power distribution within the smart grid,

collects sub-hourly power usage from smart meters, and sends notifications to smart meters once required. The smart meter receives messages from devices within HAN and sends them to the appropriate service provider.

4.0 Smart Grid Threat Landscape

On basis of functional domains specified, various threat scenarios are as below:

4.1 Advance Metering Infrastructure:

The smart meter is a critical device due to its physical location & can be easily accessed by attackers and subject to physical attacks which are in general more powerful than typical network attacks. In comparison, physical access to the data concentrator becomes less likely for external attackers, whilst systems hosted at the utility (i.e. the headend and the MDM system) are very unlikely to be physically accessible to external attackers. Considering external attackers following threat scenarios on a smart meter are conceivable:

i. Unauthorised use of the optical communication interface: The attacker may able to break the configured password first and might then be able to re configure the smart meter or exploit a software vulnerability.
ii. Physical attacks on the smart meter device: This would allow an attacker to deconstruct the smart meter device and potentially read out the firmware, the system configuration, as well as system credentials and key material. This information could be used to gain access to remote systems over the PLC network.
iii. Unauthorised communication over the PLC network: As a consequence, an attacker could potentially control remote devices & may affect the network.
For PLC data concentrators possible threats are:
iv. Remote attacks over PLC: If an attacker has figured out how the PLC communication works, remote attacks could be used against the data concentrator.
v. Remote attacks over the uplink connection: Although more critical systems are available over the uplink connection, an attacker might still consider attacking the data concentrator due to the potential to control large amounts of smart meter devices.
vi. Physical attacks on the data concentrator: This is the most powerful type of attack. Similar to smart meter devices, an attacker could use physical attacks to extract the firmware, key material, credentials, and other critical information from the data concentrator. Using the collected information, the potential to conduct remote attacks on other data concentrators, smart meters, or even headed system rises.

4.2 Wide Area Monitoring, Protection, and Control (WAMPAC):

Since WAMPAC systems can be easily physically accessed by attackers, the utility employs components that have the full VPN functionality built into the devices by the manufacturer. As a result, any communication to or from these devices is VPN protected.

4.2.1 For the physically well protected systems at the utility's premises, the following threats are conceivable:

i. Denial of Service (DoS) attacks on the network, VPN and NTP (Network time Protocol) infrastructure: To mount this attack, the attacker needs to have access to the WAN. The VPN tunnel effectively protects the inner systems if credentials and key material are not available to the attacker.
ii. DoS attacks on the wireless infrastructure: Due to easy accessibility, an attacker manages to jam or flood wireless links with erroneous messages.
iii. Software vulnerabilities: The systems at the utility contain software Vulnerabilities that are exploited by an attacker. However, the VPN tunnel provides protection unless the attacker gains knowledge of credentials and key material.

4.2.2 For the physically less protected systems in secondary substations or low voltage generation stations, the attack vectors:

i. Physical attacks on WAMPAC devices: An attacker utilises powerful physical attacks on accessible devices allowing him, for instance, to read out the firmware, configuration, credentials, or key material, potentially providing the attacker with the information necessary to access the VPN network.
ii. Injection of bogus measurement data: An attacker compromises the local authentication at a WAMPAC device and injects bogus measurement data to destabilise the grid.

4.2.3 Considering the present attack vectors, viable attack scenarios could be:

i. Physical attacks on WAMPAC devices in secondary substations
ii. DDoS attack on wireless WAMPAC communication links

4.3 Distribution Grid Management (DGM):

Considering physically more easily accessible systems, viable threats considering external attackers are:

i. Physical attacks on in field DGM devices: An attacker could utilise powerful physical attacks on accessible devices allowing him, for instance, to read out the firmware, the configuration, the credentials or the key material from those devices. These attacks could provide the attacker with the necessary information to access the VPN network. Subsequently, the attacker might leverage this information to compromise the DMS system through the VPN uplink channel.
ii.Attacks on the wireless infrastructure: As wireless links are physically easy to access, an attacker might jam these links, flood the wireless links with messages,

or target the implementation of the wireless routers. Access to the DMS traffic is however protected by the VPN.

iii. DoS attacks on the DMS uplink: By levering these attack vectors, the attacker can potentially impact the physically well protected DGM systems in the utility's premises.

4.4. Demand Response:

4.4.1 Demand Response at Residential Sites and Security issues

Demand response events arrive at the residential site from the utility to adjust the electricity price. During peak hours the price of the electricity rises; through demand response the customers can adjust their residential temperature on the basis of the demand response event received. During normal conditions the broadcast messages consisting of price signals are sent to residential whereas during emergency control signals are issued. The Programmable Communicating Thermostat (PCT) would be used in order to reduce the electric power at the residential site. Broadcast messages which will be sent out to the thermostat which causes the thermostat to update the power consumption. The PCT will communicate with the utility through a meter. The PCT allows the customer to set the temperature for heating as well as cooling.

Possible attacks in PCT:

i. An attacker may attempt to shut down the A/C, prevent the load reduction, and manipulate the scheduling of events received.
ii. An attacker tries to tamper with the incoming signals or PCT system. The attacker carries out the attacks by carrying out masquerading and man in the middle attack by shutting or turning down the A/C units in order to cause the grid instability.
iii. An attacker blocks the incoming broadcast signal by carrying out denial of service attack. Replay attacks can be carried out in order to manipulate the incoming demand response signal.
iv. An attacker could manipulate the system by disabling the PCT antenna or changing the PCT local time.

4.5 Supervisory Control and Data Acquisition (SCADA) System Security Issues:

Security issues of SCADA is mentioned below:

4.5.1 Platform configuration vulnerabilities:

i. OS and application security patches are not maintained.
ii. Inadequate Access controls: Poorly specified access controls can result in giving an SCADA user too many or too few privileges.

4.5.2. Platform Software Vulnerabilities:

i. Denial of service (DoS): SCADA software could be vulnerable to DoS attacks, resulting in the prevention of authorized access to a system resource or delaying system operations and functions. They could proactively exploit software bugs and other vulnerabilities in various systems, either in the corporate network or the SCADA network, to gain unauthorized access to places such as control centre networks, SCADA systems, interconnections, and access links.
ii. Intrusion detection/prevention software not installed: Incidents can result in loss of system availability; the capture, modification, and deletion of data; and incorrect execution of control commands. IDS/IPS software may stop or prevent various types of attacks, including DoS attacks, and also identify attacked internal hosts, such as those infected with worms.
iii. Malware protection software not installed definitions not current, implemented without exhaustive testing: Malicious software can result in performance degradation, loss of system availability, and the capture, modification, or deletion of data. Malware protection software, such as antivirus software, is needed to prevent systems from being infected by malicious software.

4.5.3. Network parameter vulnerabilities:

i. Network leak vulnerabilities: TCP/IP networks by their very nature promote open communications between systems and networks, unless network security measures are implemented. Improper network configuration often leads to inbound and outbound network leaks between SCADA networks, corporate networks, business partners, regulators and outsourcers and even the Internet which pose a significant threat to network reliability. Network leaks can allow worms, viruses or hackers direct visibility to vulnerable SCADA systems.
ii. Insecure connections exacerbate Vulnerabilities: Potential vulnerabilities in control systems are exacerbated by insecure connections. Organizations often leave access link such as dial up modems to equipment and control information open for remote diagnostic SCADA, maintenance, and examination of system status. Such links may not be protected with authentication or encryption, which increases the risk that hackers could use these insecure connections to break into remotely controlled systems. Control system often use wireless communications systems, which are vulnerable to attack or leased lines that pass through commercial telecommunications facilities.
iii. Firewalls non-existent or improperly configured: A lack of properly configured firewalls could permit unnecessary data to pass between networks such as control and corporate networks. This could cause several problems, including allowing attacks and malware to spread between networks, making sensitive data

susceptible to monitoring/eavesdropping on the other network, and providing individuals with unauthorized access to systems.

4.5.4 Network Communication Vulnerabilities:

The SCADA systems are built using public or proprietary communication protocols which are used for communicating between an MTU and one or more RTUs. The SCADA protocols provide transmission specifications to interconnect substation computers, RTUs, IEDs, and the master station. The most common protocol is DNP3 (Distributed Network Protocol Version 3.3). It was developed to achieve interoperability among systems in the electric utility.

i. Destination Address Alteration: By changing the destination address field, an attacker can reroute requests or replies to other devices causing unexpected results. An attacker can also use the broadcast address 0xFFFF to send erroneous requests to all the outstation devices; this attack is difficult to detect because (by default) no result messages are returned to a broadcast request.

ii. Rogue Interloper: An attacker installs a "man in the middle" device between the master and outstations that can read modify and fabricate DNP3 messages and/or network traffic.

4.5.5 Securing Serial SCADA Communications:

Many substations and distribution communication systems still employ slow serial links for various purposes including SCADA communications with control centres and distribution field equipment. Furthermore, many of the serial protocols currently in use does not offer any mechanism to protect the integrity or confidentiality of messages, i.e., messages are transmitted in clear text form. Solutions that simply wrap a serial link message into protocols like SSL or IPSEC over PPP will suffer from the overhead imposed by such protocols (both in message payload size and computational requirements) and would unduly impact latency and bandwidth of communications on such connections. A solution is needed to address the security and bandwidth constraints of this environment.

4.6. Generic Security Issues in Smart GRID:

These Security issues are not uniquely associated with specific smart grid "logical" component but are critical and affect any smart grid component.

4.6.1 Authenticating and Authorizing Users (People) to Substation IEDs: IEDs stand for Intelligent Electronic devices. This device may be accessed locally i.e. user may be physically present in substation & access the IED from front panel or access remotely from different physical connection. Hence the problem to authenticate and authorize different users arises so as to access is granted specifically to a user, authentication information (e.g. password) is specific to each user (i.e. not shared between users), and control of authentication and authorization can be centrally managed across all IEDs in the substation and across all substations belonging to the utility and updated reasonably promptly to ensure only intended users can authenticate to intended devices and perform authorized functions.

4.6.2 Authenticating and Authorizing Maintenance Personnel to Smart Meters: The Security problem in Smart meters is similar to IEDs. Access to these may be local through the optical port of meter or through the AMI infrastructure, or remote through the HAN gateway. In this, password is shared between users and the same passwords is used across entire meter deployment and hence problem arises for authenticating and authorizing Smart meters.

4.6.3 Side Channel Attacks on Smart Grid Field Equipment: These attacks are based on physical accessibility (Substation, Pole Top, Smart Meters, Collectors, etc.). A side channel attack is based on information gained from the physical implementation of a cryptosystem. Tempest attacks similarly can extract data by analysis of various types of electromagnetic radiation emitted by a CPU, display, keyboard, etc. Tempest attacks are nearly impossible to detect. Syringe attacks use a syringe needle as a probe to tap extremely fine wire traces on printed circuit boards. Smart grid devices that are deployed in the field, such as substation equipment, pole top equipment, smart meters and collectors, and in home devices, are at risk of side channel attack due to their accessibility. Extraction of encryption keys by side channel attacks from smart grid equipment could lead to compromise of usage information, personal information, passwords, etc. Extraction of authentication keys by side channel attacks could allow an attacker to impersonate smart grid devices and/or personnel, and potentially gain administrative access to smart grid systems.

4.6.4 Patch Management: Specific devices such as IEDs, PLCs, Smart Meters, etc. will be deployed in a variety of environments and critical systems. Their accessibility for software upgrades or patches maybe a complex activity to undertake. Also there are many unforeseen consequences that can arise from changing firmware in a device that is part of a larger engineered system. Control systems require considerable testing and qualification to maintain reliability factors.

The patch, test and deploy lifecycle is fundamentally different in the electrical sector. It can take a year or more (for good reason) to go through a qualification of a patch or upgrade. Thus there are unique challenges to be addressed in how security upgrades to firmware needs to be managed.

5.0 Challenges for New Security Solutions

Security solutions developed for traditional IT networks are not effective in grid networks because of the major

differences between them. Their security objectives are different in the sense that security in IT networks aims to enforce the three security principles (confidentiality, integrity and availability), while the security in automation (grid) networks aims to provide human safety, equipment and power lines protection, and system operation. Moreover, the security architecture of IT networks is different than that of the Grid network since security in IT networks is achieved by providing more protection at the centre of the network (where the data resides), while the protection in automation networks is done at the network centre and edge. Their underlying topology is also different where IT networks use a well-defined set of operating systems (OSs) and protocols, while automation networks use multiple propriety OSs and protocols specific to vendors. Finally, their Quality of Service (QoS) metrics are different in the sense that it is acceptable in IT networks to reboot devices in case of failure or upgrade, while this is not acceptable in automation networks since services must be available at all times.

These major differences between the IT and grid network security objectives necessitate the need for new security solutions specific for the smart grid network.

6.0 Conclusion

Smart Grid is identified as one of main components of Critical Infrastructure group. Smart grid integrates the traditional electrical power grid with ICT. Such integration empowers the electrical utilities providers and consumers. This improves the efficiency and the availability of the power system while constantly monitoring, controlling and managing the demands of customers. Wider expansion of smart grid and its communication capabilities make it more prone to cyber-attacks. Since the smart grid is considered a critical infrastructure, all vulnerabilities should be identified and sufficient solutions must be implemented to reduce the risks to an acceptable secure level.

Mumbai Visit of Sr. DDG, TEC on 27.07.2016

Sr. DDG, TEC along with senior officers of RTEC WR

Activities at NTIPRIT (Apr.-June 2016)

1. In-service training courses for DoT Officers were conducted at NTIPRIT on the following topics:
   - **i.** Work Shop on 'Greening the Telecom for Sustainable Growth' (18-19 April) [04 Participants]
   - **ii.** In-service training courses for DoT Officers on 'Unified License-An Overview', (18-19 May) [11 Participants]
   - **iii.** In-service training courses for DoT Officers on 'NGN Basics', (01-03 June) [11 Participants]
   - **iv.** In-service training courses for DoT Officers on 'Energy Management in Telecom', (09-10 June) [06 Participants]
2. Induction Training of ITS-2014 Batch (17 officers) and JTO-2014 Batch (8 officers). Technical Modules of the ITS / BWS and JTO induction courses as per training calendar were conducted during this period.
3. Fifteen Weeks Foundation course for 25 Officer Trainees of ITS/BWS 2010, 2012 & 2013 batches were successfully conducted at IIPA, New Delhi from 21st March 2016 to 01st July 2016. The objective of the course was to provide understanding of basic principles of Public Administration, comprehend the legal provisions relevant to administrative functioning, financial management, project management etc.

fgUnh dk;'kkyk

दूरसंचार अभियांत्रिकी केंद्र, नई दिल्ली में दिनांक 23.06.2016 को एक हिंदी कार्यशाला का आयोजन किया गया। इस कार्यशाला में कुल 25 अधिकारियों/कर्मचारियों ने भाग लिया। इस कार्यशाला के अतिथि वक्ता श्री केवल कृष्ण, वरिष्ठ तकनीकी निदेशक, राजभाषा विभाग द्वारा यूनिकोड इन्स्टाल करने, गूगल–ट्रांसलेशन, गूगल वॉइस टाइपिंग, मोबाइल फोन पर गूगल वॉइस टाइपिंग, क्रोम ब्राउज़र का प्रयोग करके हिंदी/अंग्रेजी में डिक्टेशन देने और एंडरॉइड फोन में गूगल डॉकयुमेंट पर कार्य करने के बारे में विस्तार से बताया गया।

Approvals from Apr. 2016 to June 2016

S. No.	Name of the Company /Name of Product & Modal No.
A	*M/s NEC India Pvt. Ltd.*
1	PABX with Interface ISDN, SV9300
B	*M/s Team Engineers Advance Technologies India Pvt Ltd*
2	High Speed Line driver, Teamlink 3002 SHDSL
3	Ethernet to E1 converter, Teamlink 3104/08/16
C	*M/s MRO-TEK Ltd*
4	High Speed Line driver, WL/E1/S/2W/AC/DC
D	*M/s ECI Telecom India Pvt Ltd*
5	Interchange of Digital Signals at 2/8/34/45/140 Mbps Ports/ STM64, XDM 1000
6	Interchange of digital signals at 2/8/34/45/140 Mbps Ports/ STM1, BG 20B
7	Interchange of Digital Signals at 2/8/34/45/140 Mbps Ports/ STM64, XDM 300
8	Interchange of Digital Signals at 2/8/34/45/140 Mbps Ports/ STM1, BG 40
9	Interchange of Digital Signals at 2/8/34/45/140 Ports/STM1, XDM 100
10	Interchange of STM-1/4/16/64/256 signals between different networks/ STM1, XDM 1000
11	Interchange of STM-1/4/16/64/256 signals between different networks/STM64, XDM 300

Important Activities of TEC during APR 16 to JUN 16

Revised GRs/IRs issued

- IR on Audio Conference Facility Device
- IR on Multi Line Telephone System
- IR on Executive Telephone System
- IR on Point of Sales (POS) Terminal with PSTN/ CDMA/ GSM/GPRS/3G/4G Interface

DCC Sub Committee Meeting conducted

- GR on SPV based Hybrid Power Supply for Wi-Fi terminals & similar other terminal equipment
- GR on SPV Power Supply for telecom equipment
- SD on Electromagnetic Compatibility Standard for Telecom Equipment

Representation of TEC in Training/Seminar Meetings

- ITU-T SG-12 & 16 meetings at Geneva
- ITU-D SG-2 meeting at Geneva
- 3rd meeting of APT Preparatory Group for WTSA-16 at Kathmandu
- Meeting of working group on "Synergy among various organisation" held in DoT
- One-week training on Public Procurement at NIFM, Faridabad
- 8th LTE India 2016 International conference at New Delhi
- Smart city Exhibitions and Conference at New Delhi
- IPR & Competition issues Conference at New Delhi
- International Conference on Electromagnetic Emissions in Mobile Telephony and its Health impact at IIT Delhi
- Workshop on 'M2M & IoT Forum-2016 towards Smarter India' and 'Accelerating Digital Growth & ease of doing business' at New Delhi

ISO : 9001-2008

Certifications issued by TEC

Type Approval (TA)

Interface Approval (IA)

Certificate of Approval (CoA)

Visit

www.tec.gov.in

Regional TEC Contact :

Eastern Region	:	033-23570008
Western Region	:	022-26610900
Northern Region	:	011-23329464
Southern Region	:	080-26642900

Other Activities

- National Working Group 12 meeting held in TEC in May 2016
- One Contribution was submitted regarding ITU-T SG-12 on work item 'G.Poicong'
- Testing of Cisco Router 3945 completed
- IPv6 Ready Logo Certificate was awarded for CDoT DWDM based on the testing done in NGN Lab TEC.

Approvals issued by TEC during the period from Apr. 2016 to June 2016

Interface Approvals.....10

Type Approvals 01

Certificate of Approval.....00

Vh bl lh lpkfjdk % nwjlapkj vfHk;kf=dh dUnz
vxLr 2016 % [k'khn yky Hkou
Hkkx 20 % tuiFk
vad 3 % ubl fnYyh&110001

Editor : Sunil Purohit, DDG (NGS) Phone : 23329354 Fax : 23318724 E-mail : ddgs.tec@gov.in

Printed at : Yugantar Prakashan Pvt. Ltd., New Delhi; M: 9811349619