भाग 24 / अंक 2 अप्रैल 2020 त्रैमासिक पत्रिका (JAN-MAR, 2020)

ISO 9001 : 2015

TEC

दूरसंचार अभियांत्रिकी केन्द्र
TELECOMMUNICATION ENGINEERING CENTRE

टी ई सी संचारिका NEWSLETTER

Telecom News : At a Glance

1. Shri Ravi Shankar Prasad, Hon'ble Minister of Communications inaugurated the "Chennai-Andaman & Nicobar Islands (CANI) Submarine Cable laying work" at Chennai on 09 Jan 2020 in presence of the Islands territory Lt Governor Admiral DK Joshi. Work of laying of more than 2,300 Kms of under sea cable is funded by DoT and executed by BSNL. It will provide high speed Internet connectivity to entire cluster of islands in Andaman and Nicobar.

2. Shri Ravi Shankar Prasad, Hon'ble Minister of Communications inaugurated a regional workshop on 'Digital Infrastructure Readiness & Review of implementation of Govt schemes' in Patna on 14 March 2020. Secretary(T), Senior Officers of DoT & State Govts were present during the event.

Hon'ble Minister during inauguration at Chennai

Hon'ble Minister & Secretary(T) during inauguration of regional workshop at Patna

Telecom News: At a Glance.....continue

3. Shri Sanjay Dhotre, Hon'ble Minister of State for Communications inaugurated India Telecom 2020, a global ICT business expo in New Delhi on 11 Feb 2020.

Hon'ble Minister inaugurating the event

4. In view of Covid19 pandemic situation in country, DoT issued certain exemptions on 13 March 2020 to facilitate Indian IT companies/ OSPs to offer work from home to their employees. During the lockdown, a number of meetings were held at DoT HQ on policy and technology actions to fight COVID 19 led by senior management including Secretary (T), Member (T), Member (F), AS(T), Adviser (TEC), Adviser (F).

5. Shri Anshu Prakash, Secretary(Telecom) & Chairman, Digital Communications Commission, met Mr. Ajit Pai, Chairman, FCC, USA in Sanchar Bhawan, New Delhi on 24 Feb 2020 and discussed various issues ranging from spectrum to 5G.

6. MoU between the Ministry of Communications, Government of India and the Ministry of Transport & Communications of Myanmar on cooperation in the field of communication was exchanged between Shri Anshu Prakash, Secretary(T) and H.E Moe Kyaw Aung, Ambassador of Myanmar in New Delhi on 27 Feb 2020 in august presence of Shri Narendra Modi, Hon'ble PM and H.E. U Win Myint, President of Myanmar.

7. On 21 Feb 2020, DoT launched '5G Hackathon' in association with various stakeholders including academia, industry & government organizations to identify and promote applications relevant to India in the 5G realm. More information is available on website 'www.5ghackathon.in'.

CYDER training program for GoI officers

As part of DoT's effort to develop skilled manpower equipped with relevant skill-sets to handle any cyber security breach, a two day hands-on training program titled 'Cyber Defence Exercise with recurrence (CYDER)' was organised under the ambit of the Joint Working Group on ICT between Department of Telecommunications, Govt. of India and Ministry of Internal Affairs & Communications, Govt. of Japan in Telecommunication Engineering Center on 4th & 5th March, 2019.

With the growing utilization of ICT, the existence of a safe and secure global and interdependent information communication technology infrastructure becomes imperative, Hence this training program was designed to equip the participants with the relevant skill-sets to handle the existing & emerging cyber security threats, and mitigating them. The training program was attended by representatives of Ministry of Home Affairs, Airport Authority of India, Reserve Bank of India, ISRO, DRDO, NCCS, MeitY, NCIIPC, Income Tax & C-DoT besides participants from DoT HQ and DoT Field units. The training provided an opportunity to gain hands-on experience in handling a Cyber Security breach and mitigation efforts.

Senior officers during inauguration of training program

Participants from various organizations

Mandatory Testing and Certification of Telecom Equipment (MTCTE)

Mandatory Testing and Certification of Telecom Equipment (MTCTE) for 13 telecom equipment, covered under Phase-I was made mandatory w.e.f. 1st Oct, 2019. 60 companies/firms have registered on MTCTE portal for certification of their telecom equipment. Total 83 applications have been registered, so far, for certification of telecom equipment covered under Phase-I. Out of these 83 registered applications, 67 certificates have been issued till Mar-20. 15 certificates were issued during quarter i.e. Jan-20 to Mar-20, while remaining applications are under process at different stages.

A meeting with Industry Associations was held on 4th Mar, 2020 under chairmanship of Additional Secretary (T) in Sanchar Bhawan to discuss the issues related to the implementation of Phase-I. More than 20 representatives of Industry Associations participated in the meeting. During meeting, most of the issues were addressed to streamline the MTCTE process.

The total Designated CABs (Conformity Assessment Bodies) reaches to 54 and 2 CABs certificate were also renewed during Jan-Mar, 2020 for testing purpose under MTCTE. List of all designated labs is available at TEC website "*http://www.tec.gov.in/list-of-cabs-designated-by-india/*".

Technical Paper on 'EMBEDDED SYSTEM SECURITY'

1.0 Introduction

We are moving towards the age of full automation where not only routine, repetitive but also sophisticated task will be done without much human intervention with extreme precision in a very short time. This has been made possible by increasing use of embedded systems in all domains. From cars to cell phones, video equipment to mp3 players and dishwasher to home thermostats, embedded systems increasingly permeate our lives [1]. These systems are the driving force for technological development in every sphere of our life. Embedded systems started as iPod, mp3 player, Bluetooth headset, PlayStation and now they have emerged at a very large scale as being used in washing machines, smart phones, self-driven cars, banking, military, space, research and defence sections. Embedded systems are the driving force for technological development in many domains such as automation products, industrial monitoring, control systems, etc. As more and more computational and networked devices are integrated into all aspects of our lives in a pervasive and "invisible" way, security becomes critical for the dependability of all smart or intelligent systems built upon these embedded systems. With the growing popularity of embedded systems, concerns about security and privacy of these systems have risen dramatically in a short period of time. This article explains some of the security risks and threats associated with embedded systems, challenges in their security along with some of proposed countermeasures.

2.0 Embedded System

It is an application specific computer system built into a larger mechanical or electrical system which does a particular task repeatedly as per the given instructions [2]. It consists of combination of software and hardware and mechanical parts if required. An embedded system thus refers to a system that is controlled by a computer that resides within the system. The type of software used in embedded systems are fixed and has limited flexibility to allow user to program run. Embedded systems are used in different applications according to the requirement but their structure and principle of working is same in terms of system hardware and design methodology. The application like mechanical and chemical plants may requires extra hardware implementation like standard input and output devices but it's not compulsory for all the plants and other devices. Embedded systems are usually based on microcontroller in which the memory, timer, input output ports, counters all are integrated on the CPU which do not require extra memory. According to their usage these can be categorised into three categories as small, medium and large. Embedded systems are not standalone but these are used within a complex device.

3.0 Application of Embedded System

Table 1- Few applications of embedded systems

Area of usage	Applications
Household usage	Washing machines, mobile phones, dishwasher, ACs, microwave oven, TV remote, DVD player, video recorder, digital camera, etc.
Industrial usage	Fax machine, printer, scanner, industrial robot, scanner, hazard detector, load vehicles etc
Banking usage	ATM, card readers, currency counter, bar code reader, finger print scanner etc.
Communication usage	Cell phones, routers, web camera, modem etc.
Medical usage	CT scanner, glucose monitor, BP monitor, x ray machines etc.
Aerospace usage	GPS system, RADAR, space robotics, rocket launching devices etc.
Gaming usage	Play Station, video games etc.

Artificial intelligence and machine learning is the new and very broad example of embedded system in which a robot or an artificial assistant like JARVIS produced by Facebook's CEO Mark Zuckerberg is able to follow every instruction given by him by the voice recognition.

4.0 Security Threats of Embedded System

In the year 2010, STUXNET became the first malware with ability to break into industrial infrastructure and allow an attacker to take control of critical system [4]. Since most of the embedded systems are Internet enabled devices which has its own utility in day to day operations but the problem arises when it starts interfering with personal information and exposing the same to unauthenticated agents.

As with any internet enabled technologies, the common cause of security threat is the connectivity to the internet. Secondly the embedded systems are cost sensitive. The cost sensitivity leads the manufacture to use slower computational processors which results in weak cryptography making the device less secure. Programming errors in the software is also a big cause of the security threat. Embedded systems perform task that are time limited, and any minute delay can cause lot of disruption and loss of details. Some embedded systems are produced to perform tasks in critical environment i.e. high temperature, humidity and even radiation to meet their requirement. In addition to above, the main threats associated with Embedded systems are as follows: [3]

4.1 Side-Channel Analysis (SCA) Attacks in Embedded System Devices

Side-channel analysis attacks exploit a device under attack hardware characteristics leakage (power dissipation, computation time, electromagnetic emission etc.) to extract information about the processed data and use them to deduce sensitive information (cryptographic keys, messages etc.). An attacker does not tamper with the device under attack in any way and needs only make appropriate observations to mount a successful attack. Such observation can be done remotely or physically through appropriate tools. Depending on the observed leakage, the most widely used SCAs are micro architectural/cache, timing, power dissipation, electromagnetic emission attacks.

4.2 Network attacks

A network attack can be defined as any method, process, or means used to maliciously attempt to compromise network security. Though field deployed systems are subject to new threats, all the existing battery of network attacks still apply. Ideally, all network communication is authenticated and encrypted using well-established protocols such as Transport Layer Security (TLS). A public key infrastructure (PKI) can be used by both remote endpoint devices (clients) and servers to ensure that only communications from properly enrolled systems are accepted by the parties to the communication. A strong hardware root of trust can provide this secure "identity" for the system, providing unique-per-device keys linked to the hardware and certified in the user's PKI.

4.3 Software Attacks

Today majority of software attacks comprise of code injection attacks. The malicious code can be introduced remotely via the network. Cryptographic attacks exploit the weakness in the cryptographic protocol information to perform security attacks, such as breaking into a system by guessing the password. The number of malicious attacks always increases with the amount of software code. Some of the attacks include stack-based buffer overflows, heap-based buffer overflows, exploitation of double-free vulnerability, integer errors, and the exploitation of format string vulnerabilities.

4.4 Control hijacking attacks

This type of attacks divert the normal control flow of the programs running on the embedded device, which typically results in executing code injected by the attacker.

4.5 Reverse engineering

Often, an attacker can obtain sensitive information (e.g., an access credential) by analysing the software (firmware or application) in an embedded device. This process is called reverse engineering. By using reverse engineering techniques, the attacker can find vulnerabilities in the code (e.g., input parsing errors) that may be exploited by other attack methods.

4.6 Malware

An attacker can try to infect an embedded device with a malicious software (malware). There are different types of malware. A common characteristic is that they all have unwanted, potentially harmful functionality that they add to the infected system. A malware that infects an embedded device may modify the behaviour of the device, which may have consequences beyond the cyber domain.

4.7 Memory and bus attacks

If the hardware is physically available and insufficiently protected, it may be possible just to read the contents of memory directly from an external programmable read- only memory (PROM) or external random access memory (RAM) chip, or by probing the connecting bus. It is generally good practice, and not that difficult, to encrypt and authenticate all static data such as firmware stored in PROMs.

4.8 Cold Boot Attack

It is a memory attack where the memory [a bank of dynamic random-access memory (DRAM) chips, for example], is chilled, quickly removed, and read on another system controlled by the attacker. The cold chips hold remnants of the data even during the short interval where they are unpowered. Thus, it is best not to store critical secrets such as cryptographic keys in off-chip memory. In cases where higher levels of security are justified, external volatile memory may be encrypted.

4.9 Injecting crafted packets or input

Injection of crafted packets is an attack method against protocols used by embedded devices. A similar type of attack is the manipulation of the input to a program running on an embedded device. Both packet and input crafting attacks exploit parsing vulnerabilities in protocol implementations or other programs. In addition, replaying previously observed packets or packet fragments can be considered as a special form of packet crafting, which can be an effective method to cause protocol failures.

4.10 Eavesdropping

While packet crafting is an active attack, eavesdropping (or sniffing) is a passive attack method whereby an attacker only observes the messages sent and received by an embedded device. Those messages may contain sensitive information that is weakly protected or not protected at all by cryptographic means. In addition, eavesdropped information can be used in packet crafting attacks (e.g. in replay type of attacks)

4.11 Brute-force search attacks

Weak cryptography and weak authentication methods can be broken by brute force search attacks. Those involve exhaustive key search attacks against cryptographic algorithms such as ciphers and MAC functions, and dictionary attacks against password-based authentication schemes. In both cases, brute force attacks are feasible only if the search space is sufficiently small Normal use: This refers to the attack that exploit an unprotected device or protocol through normal usage.

5.0 Effect of Attacks

5.1 Denial-of-Service

Many Common Vulnerabilities and Exposures (CVE) records identify potential attacks that lead to denial of-service conditions such as malfunctioning or completely halting the device.

5.2 Code execution

Another large part of the analysed CVE records identifies execution of attacker supplied code on the embedded device as the effect of potential attacks. This also includes web scripts and SQL injections in addition to the native code of the device.

5.3 Integrity violation

A commonly observable effect of potential attacks is the integrity violation of some data or code on the device. This includes modification of files and configuration settings, as well as the illegitimate update of the firmware or some applications on the device. This not only includes the cases when an attacker, who otherwise has no access to the device,

manages to logically break into it, but also cases when the attacker has already some access, but he gains more privileges (i.e., privilege escalation).

5.4 Financial loss

Certain attacks enable the attacker to cause financial loss to the victim e.g. by making calls from a smart phone. Actually, most attacks can lead to financial loss in a general sense, so a criterion is used to represent only those attacks whose primary goal is to cause financial loss. A typical example would be an attack which aims at sending an SMS or making a call to a premium number from a compromised smart phone

5.5 Degraded level of protection

In some cases, potential attack results in a lower level of protection than expected. An example would be when a device is tricked into using weaker algorithms or security policies than those that it actually supports.

6.0 Challenges in Security of Embedded Systems

Security of embedded systems will only be ensured by implementing security at both Hardware and Software level. The implementation of security policies in these systems have its own challenges. Some of the challenges are as follows: [5] –

6.1 Irregular software update

Most of the embedded systems are not upgraded regularly for security updates. Once embedded systems are installed, they keep working for years and years without the influence of humans, if the device needs a software update, they should be employed a self-updating program in it that ensures embedded security so that they could be updated automatically with security.

6.2 Attack reproductivity

As the embedded systems are produced in mass production their interior structure and properties are same. If any attacker gets successful in attacking one device, he can attack other identical devices as well.

6.3 Rules and regulations

There are no fixed rules and regulations exists for ensuring the security of these systems. Therefore, sometimes for the commercial purposes the industries compromise its security with the set rules and regulations laid by the authority.

7.0 Counter Measures

Embedded systems, like the computers, are vulnerable to security threats from several different vectors. It is important to implement multiple kinds of security in layers that keep attackers from penetrating the devices and manipulating them for nefarious purposes.

Systems-Engineering Security, implementing security features at the systems-engineering level is an effective means of preventing hackers from interacting with software. This includes applications like firewalls, secure network communication protocols, proper authentication of data sources, and data encryption. These measures regulate interaction between the software and the outside environment, making it more difficult for attackers to access the system. They are especially important for devices that connect to the internet and could potentially be accessed remotely. Security requirement can vary according the type of embedded system being used. The type of attack may also vary for users, service providers, manufacturers etc. Intelligent and secure encoding techniques provide strong resistance against the conventional attacks.

Security in the architectural level should also be improved in which the mapping of adopted algorithms and protocols are considered more efficiently. The languages such as Java and ML are capable of preventing some of the vulnerabilities discussed here. Operating system based counter measures will also be another best counter. The memory within the OS are segmented into two parts i.e. data and code memory block so by swapping the data and code memory it will make harder for the attacker to inject any malware.

Public Key encryption have been severely attacked using Simple Power Analysis (SPA), mainly because of the conditional branching in the encryption. Such vulnerabilities in the program can be prevented by modifying the implementation or replacing with a better new algorithm to perform the same task. Countermeasures which can be used for prevention of attacks on embedded system security are as follows [4]:

7.1 Conducting end to end threat analysis

The security of an embedded device can be improved by starting with identifying the potential threats. These threats must be evaluated in the context of the device manufacturer, operators (if the device is provisioned in such a way, and end users, including their usage). The attacks can be done in terms of wired Ethernet connection with the device used for communication, and common services such as web

(HTTP). A complete product life cycle analysis needs to be performed.

7.2 A risk matrix needs to be built

Because of the vast number of combinations possible, a risk assessment needs to be performed by the government. The key matrix should be made more complex so that it become harder for the attacker to attack.

7.3 Select an Appropriate Run-Time Platform

Restricting use of common platform govt. should ensure that organisations should select an appropriate commercial run-time platform for an embedded system and make it mandatory for use. Implementing a system with components that have COTS (Commercial off the shelf) security can increase the security and reduce the cost of development of the overall platform.

7.4 Certification

The government should assure that standards for the security are made and tested to meet the standard and provide certification to all the products being launched in the market.

7.5 Design and test for security

Security vulnerabilities are a class of software requirement deficiencies in design or implementation and earlier they are caught in the product development life cycle, the less costly it is to fix them and harden a system against attack. Security testing must involve defining the boundaries of a system and determining methods of exploiting weak defences along these boundaries

7.6 Security Testing

Source Code Analysis is an important technique used to avoid attacks. It is automated testing of source code for the purpose of debugging a computer program or application before it is distributed or sold. Source code analysis can be either static or dynamic.

In static analysis, debugging is done by examining the code without actually executing the program. In most cases the analysis is performed on the source code and in the other cases on some form of the object code. This can reveal errors at an early stage in program development, often eliminating the need for multiple revisions later. After static analysis has been done, dynamic analysis is performed in an effort to uncover more subtle defects or vulnerabilities. Dynamic analysis consists of real-time program testing. Performing dynamic code analysis is more accurate than static analysis (more information of the execution is available at runtime compared to compile-time), dynamic code checking might miss some errors as they may not fall on the execution path while being analysed.

7.7 Secure the Applications

Same as the products should be tested first the application should also be tested first. Standards should be made and tested and then only permit the apps to get launch.

7.8 Create a security response team

Government should make a team to address vulnerabilities, draft responses, communicate internally and externally, plan for potential product updates, and manage the delivery of those changes. A security response team is usually cross-functional, for example, including software and hardware development, software quality assurance, customer support, product management, and technical publications.

8.0 Conclusion

Embedded system based devices have made our life easier and comfortable by meeting almost all the real-time constraints but at the same time as they are so useful, they also have a threat on its security.

There is an increasing number of security threats over embedded systems and various hacker attacks that jeopardize the commercial viability of new products or that can endanger the correct operation of existing ones. As 100% security does not exist, an attacker having enough time, resources and motivation could always break into any system. For this reason, manufacturers must secure their products against specific threats trying to achieve a balance between the cost of security implementation and the benefits obtained. In order to improve security, concentration on cryptography, tamper-resistance techniques, advanced microcontroller and algorithms can make the embedded devices secure enough. At the same time, it is also important for the government to ensure that design and implementation of the whole embedded system must be done with much more security concern.

9.0 References

[1] P. Koopman, “Embedded system security,” IEEE, pp. 95-97, 12 July 2004.

[2] M. Rouse, “whatIs.com,” IoT Agenda, [Online]. Available: https://internetofthingsagenda.techtarget.com/ definition/embedded-system.

[3] R. Newell, The Biggest Security Threats Facing Embedded Designers, Electronic Design, May 23, 2016
[4] Five Steps to Improving Security, wind river.
[5] R. SAVJANI, "6 Critical Challenges Facing the Embedded Systems Security," 20 AUGUST 2018. [Online]. Available: https://www.einfochips.com /blog/6-critical-challenges-facing-the-embedded-systems-security/.
[6] Z. M. L. B. Dorottya Papp, "Embedded Systems Security: Threats," in Thirteenth Annual Conference on Privacy, Security and Trust, 2015, p. 151.
[7] A. Grua, "Security Requirements for Embedded Devices – What is Really Needed?" Icon Labs, [Online]. Available: https://www.iconlabs.com/ prod/security-requirements-embedded-devices-%E2%80%93-what-really-needed.
[8] D. J. W. B. R. N. D. M. U. Michael Vai, "Secure Embedded Systems," [Online]. Available: https://www.ll.mit.edu/sites/default/files/page/doc/2018-05/22_1_9_Vai.pdf.
[9] M. M. H. A. Anik Barua, "Embedded Systems: Security Threats and Solutions," American Journal of Engineering Research (AJER), 2014.

[Contributed by TS division, TEC]

Adoption of International Standards/ specifications as National Standard

1. **Adoption of oneM2M Rel 2 specifications, transposed by TSDSI, as National Standard:** A two layered Committee was constituted by Sr. DDG TEC in Feb 2019 for this work. Consultative Committee chaired by DDG (IoT), TEC is having members from industries, Government and standardisation bodies, including C-DOT and TSDSI. After a no. of meetings and training programmes, Consultative Committee finalized its report and submitted to Telecom Standards Advisory Committee in Dec 2019, which has been agreed in Telecom Standards Advisory Committee (TSAC) meeting held on 17th Jan 2020. Approval is awaited from the competent authority.

2. **Adoption of 3GPP standards, transposed by TSDSI, as National Standard:** In the Consultative Committee meeting held on 14 Feb 2020, recommendation was given for adoption of 402 3GPP standards, transposed by TSDSI, as national standards.

TEC Contributions submitted to ITU-T & other Standardization bodies

1. Following two contributions against Q16 (for Study period 2017-2020) were discussed and presented in SG-15 meeting held during 27 Jan - 07 Feb 2020 at Geneva, Switzerland.
   i. Contribution on draft new recommendation ITU-T. L.oha "Optical fibre cables for in-home applications" - Proposal to add Appendix V as Indian Experience was agreed and accepted by SG-15.
   ii. Contribution as a new proposal for draft new Rec. L.font "Requirement for a combined Fibre Optical Network Termination Box: FONT was agreed and accepted as a new work item which will be further discussed in next SG-15 meeting.
2. One contribution regarding Proposal for modification in baseline text for TD1026 ITU-T draft Recommendation Q.39_FW_Test_ID_IoT "The framework of testing of identification systems used in IoT" against Q12/SG-11 of ITU-T was finalized and will be submitted in the forthcoming meeting of ITU-T.
3. A contribution for updating 'draft Recommendation ITU-T Y.OBF_Trust' was finalized in the NWG-13 meeting held on 6th Feb, 2020 in TEC. The contribution was remotely presented in the ITU-T SG-13 meeting held on 4th & 11th Mar, 2020 & was unanimously accepted by SG-13. Accordingly, the 'draft Recommendation Y.OBF_Trust ' was updated.

Various Presentations by TEC officers

1. DDG(IoT), TEC Shri Sushil Kumar
   - delivered a talk on "Modern Communication Technologies", in Faculty development programme in A K Garg Engineering College, Ghaziabad on 14th Jan 2020.
   - delivered a talk on "IOT/ M2M: Technology, Policy & Standards Overview", to ADET in NTIPRIT Ghaziabad on 26th Feb 2020.
   - chaired and moderated the panel discussion on PLC technology, in a conference organised by IEEE in New Delhi on 2nd Mar 2020.
2. Dir(FA), TEC Shri Abdul Kayum gave two Presentations on the topics "5G Transport" and "Next Generation Transmission Equipment" in NTIPRIT Ghaziabad in Jan-20 & Mar-20 respectively.

3. DDG RTEC (SR) Shri K. Hanumanth Rao delivered the special address at the inaugural function of "IoT Centre of Excellence" and new EMC and Wireless Laboratory organised by M/s UL India Pvt. Ltd. on 12th March 2020 in Bangalore.

Inauguration of IoT Centre of Excellence in Bengaluru

Workshops conducted

1. A Technical workshop was held at Bengaluru in ITI premises on 12.02.2020 in association with M/s ITI Ltd. and M/s C-PRAV to brief manufacturers, traders and Test labs about the new MTCTE scheme. Shri K. Hanumanth Rao, DDG RTEC (SR) delivered the key note address and guided the audience about MTCTE scheme, CAB designation, online application, evaluation and approval process.

DDG RTEC (SR) addressing the workshop

2. Future Network Division of TEC in association with M/s Ericsson India organized a workshop on "Artificial Intelligence and Machine Learning (AI/ ML) in Telecom" on 30th January 2020. Mr. Thirumaran Ekambaram, Director of Data Science at Ericsson's Global AI Accelerator group and Mr. M J Prasath Senior Manager Data Science in Global Artificial were speakers of ibid workshop. Important topics presented and discussed were: AI/ML benefits (AI Enabled Network Design, Network Deployment, Service Assurance, Customer Care, Security); AI/ML Platforms and Infrastructure; AI/ML Use Cases Already Implemented; AI/ML Use Cases Under Development.; AI/ML - 5G, IoT and beyond; and AI/ML - Global Trends. It was very interactive and well received workshop.

MoU of TEC/NTIPRIT with other organizations

1. **Between TEC and CSIR-CEERI:** An MoU was signed between TEC and CSIR-Central Electronics Engineering Research Institute (CSIR-CEERI Pilani) on 08.01.2019. This MoU aims to act as an umbrella agreement defining the broader aspects and scope of collaboration between TEC and CSIR-CEERI. Under this MoU broad scope of engagement of TEC with CSIR-CEERI includes Future Telecom & ICT technologies with focus on but not limited to 5G, IoT AI, Big data, mm-wave technology, Edge automation platforms, C-V2X, Machine learning technologies and Standards/ specifications etc.

   First Meeting between two organization took place on 7.11.2019. Going forward Future Network Division of TEC arranged an e-meeting between TEC and CSIR-Central on 13th March 2020. Senior Officers from TEC and Senior Scientists from CSIR-CEERI Pilani attended the meeting. Some important areas for future collaboration have been identified as : a) Joint study for utilization of millimeter waves and other identified radio frequency bands for 5G, b)Study of possibilities of Specific Absorption Rate (SAR) measurement in 5G frequencies, c) Development of IoT use cases and specific IoT applications (e.g. for healthcare, smart city applications),d) Development of India specific Artificial Intelligence (AI) standards, e) Development of Explainable Artificial Intelligence (XAI) framework, f) Designing a framework for End to End product cycle management of IoT devices, g) AI for Health (CEERI is already working with Samsung, ITI and other industry partners. In addition , possibility of accreditation of CEERI labs for EMF Safety and Security of telecom equipment under DoT's MTCTE regime and participation of CEERI scientists in National Working Groups (NWGs) corresponding to ITU-T standardization, steered by TEC, were also discussed and agreed.

2. **Between NTIPRIT and GSMA:** National Telecommunications Institute for Policy Research, Innovation & Training (NTIPRIT) - a training institute of Department of Telecommunications located in

Ghaziabad and the GSM Association (GSMA) agreed to build cooperation by signing a Memorandum of Understanding to diversify and strengthen the Capacity Building programme of NTIPRIT. The MoU was signed by Sh. S. P. Rai, Sr. DDG on behalf of NTIPRIT, on February 14, 2020 (Friday) at New Delhi. The MoU further aims at the exchange of information and consultation for strengthening effective and practical cooperation in relevant areas.

MoU signing between NTIPRIT and GSMA

Activities in 'National Telecommunications Institute for Policy Research, Innovations & Training Institute'

1. Induction Training of ITS-2018 Batch probationers

NTIPRIT is conducting ITS-2018 batch induction training from September 16, 2019. Different modules on several subjects were conducted during January 2020 to March 2020. As part of curriculum, course on Disaster Management was conducted in the first week of March. Trainees also underwent two days of training at NIDM, New Delhi. During the module, trainees interacted with faculties of NIDM and senior officers of National Disaster Management Authority, New Delhi.

ITS-2018 probationers and Course Director Sh. Deepak Sharma, Director (FT), NTIPRIT with faculties of NIDM, New Delhi

2. ITEC (Indian Technical and Economic Cooperation) Course on 'EMF Radiation in Telecom Services' (20.01.2020 to 24.01.2020)

One-week course on 'EMF Radiation in Telecom Services' was conducted by NTIPRIT at CDTI, Ghaziabad. Total 07 participants were attended the course. The objective of the Course was to familiarize the participants with the Electromagnetic Radiation in view of tremendous growth of mobile and wireless communication and importance of measurement of Electromagnetic Radiations from the point of view of public health and safety.

The course covered the concepts of EMF radiation, Specific Absorption Rate (SAR), testing, measurement and regulatory aspects of EMF radiation related to telecom. The participants also visited Delhi as part of cultural / heritage Visit.

Group photo of participants of "EMF Radiation in Telecom Services" course

3. Seminar on 'Artificial Intelligence' (18.02.2020)

One days Seminar on 'Artificial Intelligence' was conducted by NTIPRIT at Hotel Fortune Inn, Ghaziabad. The seminar was started with welcome speech and inauguration by Shri S. P. Rai, Sr. DDG, NTIPRIT. Thereafter, various lectures were delivered by the experts of subject matter from various DoT field units and private organizations. This seminar was attended by 30 officers from different units of Department of Telecommunications.

ITS-2016 and P&T BWS 2016 batch with faculties of NTIPRIT on the occasion of Valedictory Programme

4. ITEC Course on 'ICT Policy Planning' (17.02.2020 to 28.02.2020)

NTIPRIT conducted 5th ITEC course in the month of February, 2020. Total 22 participants participated in the course. The objective of the Course was to familiarize the participants with the concepts, evolution and different aspects of Policy Familiarization, especially in ICT domain. During the two weeks stay in India, Participants were given exposure to different technical aspects in the domain. They also visited Historical monuments in Agra and Delhi as part of Cultural Visit during the course. The participants were also given opportunity to feel the art and music by arranging a Visit to Kingdom of Dreams, Gurugram and organizing cultural evening at CDTI, Ghaziabad.

Group photo of participants of "ICT Policy Planning" course

5. Induction Training of the following batches of Officer Trainees of ITS/ BWS and JTO Probationers were conducted during the period:

i. BWS-2017 batch (2 Officers)
ii. ITS-2018 batch (15 Officers)
iii. JTO-2016 batch (1 Officer)
iv. JTO-2018 batch (10 Officers)

Various training programs like technical modules, LSA attachment, were conducted during this period as per respective training calendar.

6. Following In-Service Courses/ Seminars/ Filed Training Programs were conducted during the period:

(i) Field Training Programme at Bangaluru for Karnataka LSA officers and other LEA officers on 10.02.2020 [43 participants],
(ii) Seminar on Artificial Intelligence on 18.02.2020 at Ghaziabad [30 Participants]

BIS Committees headed by TEC officers

Follwing BIS Committees are being headed by TEC officers;

1. **LITD* 27 on 'IoT and related technologies'**: headed by DDG(IoT) Shri Sushil Kumar. He chaired LITD 27 meeting arranged by BIS on Webex on 21st Feb 2020 for preparing contributions for ISO/IEC JTC1 SC41 e-meeting in May 2020. Around 25 industry, Government & academia members participated. From TEC, Ms. Namrata Singh ADG(IoT) participated in this meeting.
2. **SSD^ 08 on 'Communication Services Sectional Committee'** : headed by DDG(FN) Mrs Deepa Tyagi. The scope of work of the committee is Standardization in the field of communication services provided by professional individuals or organizations to other organizations or common people through physical or electronic means for transfer of information through voice, data, text, sound and/or image including Landline/Mobile Phone, Internet/OTT (Over - The -Top) services.
3. **LITD 06 on 'Wires, Cables, Waveguides and Accessories sectional committee'** : headed by DDG(R) Shri Ashutosh Pandey.
4. **LITD 11 on 'Fibre optics, fibre, cables and devices sectional committee'** : headed by DDG(T) Shri Ashwani Salwan.

* ***Electronics and Information Technology Department***
^ ***Service Sector Department***

Approval Certificate Issued by TEC

Sl. No.	Name of the Manufacturer/Trader & Name of Product & Model No.
A	***M/s Aspect Contact Centre Software India Pvt. Ltd.***
1	Systems Employing Computer Telephony Integration, DCP-00
B	***M/s Panasonic India Pvt.Ltd.***
2	PABX for Network Connectivity, KX-NS1000BX
3	PABX for Network Connectivity, KX-NS300SX
C	***M/s Star Informatics Pvt. Ltd.***
4	OPTICAL FIBRE SPLICING MACHINE, Star FFS-9000

Important Activities of TEC during JAN 20 to MAR 20

Brief About TEC

Telecommunication Engineering Centre (TEC) functions under Department of Telecommunications (DOT), Government of India. Its activities include:

- Issue of Generic Requirements (GR), Interface Requirements (IR), Essential Requirements (ER), Service Requirements (SR) and Standards for Telecom Products and Services
- Field evaluation of products and Systems
- National Fundamental Plans
- Support to DOT on technology issues
- Testing & Certification of Telecom products

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

For more information visit TEC website www.tec.gov.in

DCC/Sub DCC meeting conducted for

- GR on Power system based on renewable energy for telecom equipment
- GR on NGPON2, GR on Micro duct
- GR on 100G Ethernet Traffic Analyser
- GR on Stabilized light source
- Amendment in GR on Raw Material for manufacturing optical fibre cables.
- Amendment in GR on Riser optical fibre cable (for indoor applications)
- Planning guidelines on Li-ion battery

Meeting/Seminar/Workshop attended by TEC officials:

- Participation in ITU-T Study Group-11 meeting in first week of March2020 at Geneva, Switzerland.
- ITU-T Study Group-15 meeting from 03.02.20 to 07.02.20 at Geneva, Switzerland.
- Telecom Summit 2020 with the theme '5G Technology: Forging Ahead into a Smarter India' at Vigyan Bhawan, New Delhi.
- Workshop on "5G Solving the Capacity Crunch & Connecting the Unconnected" organized by IWPC in partnership with TSDSI at Bengaluru.
- Standards for Industry 4.0 in India and Germany: Exploring Opportunities for Harmonisation at 'The Claridges', New Delhi

Other Important Activities in TEC

- Meetings of NWG-11, NWG-13 & NWG-15 were held in TEC
- Guideline on Voluntary code of Practice(VCP) for sustainable telecom has been finalized in TEC and submitted to DG Telecom, DoT. TEC prepared a common industry wide Voluntary Code of Practice (VCP) encompassing energy- efficient Network Planning, infrastructure sharing, deployment of energy-efficient technologies and adoption of Renewable Energy Technology (RET). The voluntary code will be focused on taking reasonable actions within the Telecom Service Providers (TSPs) operations through working with key stakeholders to find long-term solutions to optimize energy usage and resulting reduction in carbon footprint.

Suggestions/feedback are welcome, if any, for further improvement.

टी ई सी संचारिका : दूरसंचार अभियांत्रिकी केन्द्र
अप्रैल 2020 : खुर्शीद लाल भवन
भाग 24, अंक 2 : जनपथ, नई दिल्ली–110001

Editor : Ram Lal Bharti, DDG (NGS) Phone : 23321288 Fax : 23318724 E-mail : ddgs.tec@gov.in, adetngs.tec@gov.in

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