# Essential 5C's to Lead IIOT

## Introduction

We all know that IoT has a lot of potential to bring digital transformation and addressing multiple problem statement in not only industries but also in-home automations. However, there are multiple challenges before successful implementation of IoT solutions hence there is always a need of ecosystem which can satisfactorily confirms end to end solutions by understanding backward compatibility, present requirement and future challenges.
As per statistics 84 % of industrial companies face a disconnect between data from connected devices, shop floor managers and strategic decision makers, limiting the digital transformation and challenging the success of IoT implementations.

## Following are few Challenges

### □ Defining the Problem Statements

Most of the IoT projects are not clear with their goals and hence the solution provider is not able to forecast the feature requirement and hence with no visions less competitive solutions are provided and hence the never-ending cycle of development continues for a while. The problem statement should be defined by understanding all the business and technological requirement milestones and clear roadmap should be developed at least for succeeding next five years

### □ Understanding the Readiness for IoT

Finding the readiness of IoT is very important step to direct the IoT solutions implementation strategies most of times industries directly starts defining the IoT initiatives due to IoT implantation pressure in the organisation from management which brings project failure some or other way reasons can be compatible technology, scaling or security. Hence before planning any of IoT project in an organisation it become essential to understand the readiness of the organisation so that the business and technological gaps can be address with featurestic vision and brings compatibility in system working as a whole under one platform. IoT Readiness Services helps operators assess their network's ability to support IoT models, identify gaps and then develop a transformation roadmap leading to a high-performance IoT-optimized network.

### □ OT, PT and IT Convergence

Since IoT solutions require convergence of multiple technologies such as operational technology, process technologies and information technologies hence it require deep understanding and multi fold skill set which most of the times not present in the organisation hence it become essential to acquire the skills from outside organisation or to develop ecosystem partners which can bridge the skill gaps and helps to develop technological savvy solutions.

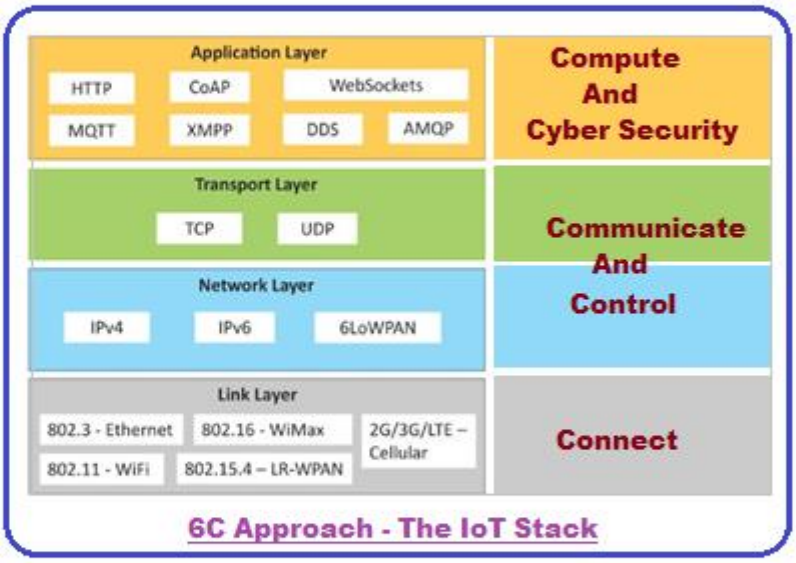
### □ Economical, Sustainable and Scalable System

Before realising the actual IoT implementation plan the multiple aspects of the projects are scrutinised at Micro and Macro level such as business and technological values encashed, ROI, Economy of Scale and Life of projects or technology used etc. once the rational answers to these questions are found we can kick start the projects.

## Understanding 5C Approach

The 5C are the five checkpoints for any of IoT solutioning this solutioning approach brings judgement to the organisation with clear understanding that every micro requirement are addressed to bring end to end compatible solution. The 5C approach is inspired from OSI model however the only focus is to through light on every layer from sensor to analytics of the IoT solutioning.

The five c's are acting as five pillars for IoT and I4.0 solutions further there is dependencies of one pillar with other pillars and hence until and unless first pillar is address, we cannot move the succeeding one this enables us to define the compatible solution at micro level. The 5C are taking care of every business and technological (OT, PT and IT) requirements and their convergence bringing the sustainable, scalable, secure and economical solutions



6C Approach - The IoT Stack

### Connect

Connectivity is the preliminary layer it includes understanding of physical as well as logical connectivity to the system or machine once the connectivity is established the system is ready to interfaced with the remote world. Connect act as a physical layer of OSI model it is the medium by machine get communicated. The components by which we need to establish the connectivity includes transducers, sensors and actuators. The output obtained from the sensor are raw and need to processed further so that it can be converted into either in digital or analog measurable form. Sometimes we also need converter RS232 to RS485, Ethernet to Fiber-optic, Wireless - GSM, GPS etc depending upon the digitisation requirement.

### Communicate

This layer establishes the communication from physical device or sensor to the outside world it includes protocols, media converters, communication module such as Raspberry module, GSM modules, Wifi module, Zigbee module, Lora module etc.

For communication we can also use devices such as communicator, Remote I/O, M2M gateway, Router, Access point, Ethernet Switch, I/O module, IoT Gateway, .Net Gateway, OPC UA, OPC DA etc. Also, for Remote Connectivity we have tools VPN routers and Remote Desktop Access. The communication protocol includes TCP/IP, UDP and many more

## Control

The control layer responsible for performing control operations it acts as a feedback mechanism by which device or machine can be controlled as per the requirements with manual intervention.
The devices used for control systems include SCADA systems (Supervisory Control and Data Acquisition), DCS (Distributed Control System) and Programmable Logic Controllers (PLCs). RTUs (Remote Terminal Units), Human-Machine Interfaces (HMI), embedded systems, edge devices and computing technologies, machinery, physical equipment in plants and Variable Frequency Drives (VFDs) Control layer protocols Profibus, ProfNet, Modbus etc.

## Compute

The compute layer enables computations required by the system or machine it can either be done with help of edge devices or fog or cloud technologies, it ensures validation, desired operation of devices, real time monitoring and recording of data for detail analysis and decision-making purposes. Majorly IoT Platform Player and Proprietary Software's companies are serving the desired computing solutions. Example EMS, Temperature Monitoring, Warehouse Management etc. The compute layer protocols include TCP/IP, MQTT, COAP HTTPS, FTP many more

## Cyber Security

Today securing the OT, PT and IT network become a big challenge henceforth we need to put every possible effort to secure not only the data but also the communication and the complete network so that we can be protect our network from hackers, data losses and obtain the high level of reliability of the network. For securing data, we can use encryption and decryption techniques such as Advanced Encryption Standard (AES), MD5, RSA, WEP, WPA etc. For secure communicating over network we have https, SSL and Firewall security further to ensure high level of security at OT, PT and IT systems and prevent passive and active attacks we can have readily available embedded devices such as Wall IE, Tofino Xenon devices and many more. These devices support NAPT, Port forwarding and Network Address Translation (NAT) which can be easily configured exposing only the devices you decide should be exposed to the higher lever network all without having to change the IP addresses of the machine devices.

## Conclusion

The 5C approach which can be implemented as an IoT stack enable us to address most of initiatives in IoT, IIOT and I4.0 space further it helps us to develop complete end to end architecture right from sensor to real time monitoring and analysis.

Rahul Chandrayan
chandrayan.rahul22@gmail.com