

# Smart Gateway Reference Architecture for Industrial Internet of Things- Design, Enterprise Implementation, Experience

Jayakumar Vk, Kasi Viswanathan U, Kannan Sankar  
Sensor to Software Innovations Lab, TATA Consultancy Services, Chennai

**Abstract**— *The Internet of things(IoT) enables to connect and control various assets and enables to transfer the data over a network without requiring human-to-human or human-to-computer interaction by providing unique identifiers in cloud(public or non-public). There are sensors and data collectors required when there is a need to communicate between the physical and the software environment. IoT is about controlling devices, that need remote monitoring and analytics enabled control to share the relevant data on cloud. The current communication focusses on challenges to build a generic gateway reference solution that can accommodate various protocols, open and propitiatory, without comprising on security and safety. Though there are many mechanisms to push the data to the cloud, collected from various industrial sensors, the need for a universal industrial standard gateway is imperative*

*Connecting various assets like a device to a sensor for remote communication and monitoring systems at another end to improve reliability and productivity can add great value to solutions. Also connecting devices to the cloud gives an additional approaches to the system – end users, service providers and equipment OEMs. To embark onto such approaches a universal bridge between the cloud and the sensors without disturbing the existing architecture is mandatory. The current work provides a platform independent framework and reference architecture to design a smart gateway for industries, without disturbing their operations or existing configurations. Based on practical enterprise level implementation, an architecture is proposed for smart gateway, which enabled a hassle free implementation of promising application to integrate sensors and improved global supply chain management logistics for assets like HVAC and UPS*

**Index Terms**—IoT, Smart Gateway Reference Architecture, Sensors for Remote Monitoring, Cloud

## I. INTRODUCTION

The Internet of Things (IoT) is regarded to be the next major step towards the acquisition and processing of massively distributed information. In spite of the acceptance on the great potential of the concept and the significant progress in a number of IT enabling technologies, there is a general lack of an integrated vision on the realization [1]. With giant leap in sensor and distributed sensor technology, the ability to infer information from different eco systems has been greatly enhanced [2]. Any framework that claims to encompass IoT technology, is expected to have three important characteristics- comprehensive sensing, reliable transmission through internet, intelligent processing in

cloud. IoT enables any real world object to participate in the Internet. Advancements in both data acquisition and control such as more accurate and efficient sensors and actuators as well as significant advancements in data processing made available due to faster and cheaper processing units has made the possibility of a world of networked, intelligent devices a very real possibility. Though initially designed in the context of supply chain management, IoT has been covering an entire spectrum of applications like healthcare, utilities, transport etc. [4]. To realize an efficient, secure, scalable IoT vision, a universal gateway that connects things is essential. Jayavardhana Gubbi *et. al* proposed an novel integrated Sensor-Actuator-Internet framework around which a smart environment could be shaped[4].

Cloud computing IoT has many potential benefits for both individuals and industries. Some of the potential benefits include improved supply chain management, smarter homes and devices, improved energy management, manufacturing automation, improved industrial diagnostic systems, and better healthcare services [2]. Despite the widespread agreement towards the potential benefits of IoT, there has not yet evolved a concept that is generally accepted [2]. An IoT system must have three important characteristic, a comprehensive sensing of all relevant data, reliable and secure transmission of sensory and control information between devices and to the cloud, and finally processing the data intelligently at various stages in the IoT network [3]. Standardization bodies have developed sensor standard that can leverage internet protocols to access sensor values corresponding to equipment [4, 5]. Based on literature survey, it was inferred that though many architecture conceptualization [2] for IoT has been presented but the design for an unified proven framework to integrate legacy and smart systems has not yet been conceived. In the rest of the communication, the need for an industrial gateway, solution to the problems, generalized architecture, results based on real time vendor agnostic implementation are discussed in detail. The key challenge and the solution to convert a legacy system in an IoT enabled environment is also covered.

## II. NEED FOR INDUSTRIAL IoT GATEWAY

### A. Legacy Sensory Systems

One of the major challenges in implementing an IoT

solution in Industries is that legacy systems use a wide variety of sensors that communicate using variety of protocols. All the segregated data from various systems needs to be made available on the internet. Existing sensors can be broadly classified into the following types:

- Analog sensors, that provide output in the form analog, non-quantized voltage, current, resistance, charge or capacitance.
- Digital sensors, that use serial and parallel outputs to send information contained in bits, pulse or continuous digital signals.
- Intelligent sensors, that performs basic data acquisition and processing at source and provides an output in serial, digital or parallel form.

### *B. Variety of Sensors*

A deeper look into industrial sensors reveals a wide array of sensor types that are currently in use [10,11]. These include, but are not limited to:

- Acceleration sensors, such as accelerometers
- Bio-signal sensors, such as Electrocardiogram (ECG), Electroencephalogram (EEG), Electromyography (EMG) sensors, Electrooculography (EOG) sensors, and Galvanic Skin Response (GSR) sensors.
- Distance sensors, such as capacitive, Hall Effect, infrared and air pressure.
- Force/pressure/strain/bend sensors, such as Fiber Optic Sensors, Flexion Sensors, Force-Sensitive Resistors (FSR), Load Cells, Co-ordinates & Pressure Sensitive Sensors, Miniature Pressure Transducers, Piezoelectric Ceramic and Film, Strain Gauge
- Flow sensors such as ultrasound sensors
- Humidity sensors such as Hygrometers
- Linear position sensors such as Hall Effect sensors, Linear Position (Touch), Linear Position (Slider), Linear Variable Differential Transformer (LVDT) and Co-ordinates & Pressure Sensitive Sensors
- Orientation sensors such as Accelerometers, Inclinometers and Magnetometers
- Radio Frequency Sensors such as Radio Frequency Identification (RFID), Rotary Position, Rotary Encoder.
- Rotary Potentiometer such as Rotary Velocity sensors and Gyroscopes
- Switches, On-Off - temperature controlled
- Vibration sensors such as piezoelectric ceramic and film
- Visible Light Intensity Sensors such as Fiber Optic Sensors and Light Dependent Resistors (LDR).

The Industrial gateway must provide the ability to process information from all of these different types of sensors

### *C. PROPRIETARY PROTOCOL*

Another challenge in industrial IoT is the presence of proprietary protocols. Proprietary protocols owned by a single organization or individual and are not freely distributed, thereby making the data acquisition difficult. Proprietors may enforce restrictions through control of the intellectual property rights. Legacy systems have different proprietary protocols. Connecting different protocols involves providing a common interface between the protocols. But industries deal with a number of sensors and devices. Connecting all these protocols manually is difficult. Thus the IoT gateway helps us overcome this difficulty.

Some common industrial protocols include:

- Process automation protocols such as CC-Link Industrial Networks, CIP, CAN bus(CANopen,DeviceNet), ControlNet, DirectNET, EtherCAT, Ethernet Global Data (EGD), Ethernet Powerlink, EtherNet/IP, Factory Instrumentation Protocol, Honeywell SDS, HostLink, INTERBUS, MECHATROLINK, Modbus, Optomux, PieP, Profibus, PROFINET IO, SERCOS interface, SERCOS III, Sinec H1, SynqNet, TTEthernet, RAPIenet.
- Industrial Control System Protocols such as OPC DA, OPC HAD, OPC UA, MTConnect.
- Building Automation Protocols such as 1-Wire, BACnet, C-Bus, Factory Instrumentation Protocol, KNX, LonTalk, Modbus, oBIX, VSCP, X10, xAP, xPL, ZigBee
- Power System Automation Protocols such as IEC 60870, IEC 60870-5, IEC 60870-6, DNP3, Factory Instrumentation Protocol, IEC 61850, IEC 62351, Modbus, Profibus
- Automatic Meter Reading Protocols such as ANSI C12.18, IEC 61107, DLMS/IEC 62056, M-Bus, Modbus, ZigBee, AFDX, ARINC 429, CAN bus(ARINC 825,SAE J1939,NMEA 2000,FMS), Factory Instrumentation Protocol, FlexRay, IEBus, J1587, J1708, Keyword Protocol 2000, Unified Diagnostic Services, LIN, MOST, VAN

Other features of legacy systems that need to be considered while implementing an IoT solution include data access problem due to single master concept, different data rates of sensors, ruggedness required, noise immunity, managing distributed system, deterministic data identification and analysis, non-intrusive/non-invasive connectivity, control and storage, data security, compactness, low power consumption, easy implementation and low cost.

Figure 1 provides an overview of the problems that a universal industrial gateway can address



Figure 1: Issues to be handled by Industrial IoT

### III. SOLUTION

To address the above mentioned problems, a novel vendor agnostic architecture that addresses above problems is depicted in Figure 2. A single master concept allows data access only through a single node. Also, existing industrial multi-master systems allow only a single master to access data at a time. The gateway allows multiple masters to have simultaneous data access. Legacy systems have different sensing equipment that operate at different data rates. Acquisition of this data would require several interfaces leading to an unreliable system. The proposed gateway architecture provides different interfaces viz., RS 485, RS 232, 3G/4G/LTE, provision shall also be provided for future enhancements in a single device. Industrial sensing elements are required to have a certain level of ruggedness to withstand various physical and environmental parameters such as varying temperatures, humidity, uneven surfaces, harsh environments, simple wear and tear, internal vibration, minor shocks and so on[5].

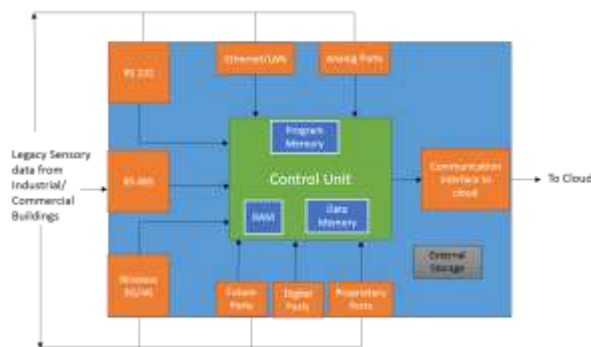


Figure 2 : Generic Framework - Smart IoT Gateway

The gateway system needs to be rugged enough to be compatible with industry standards. Dealing with noise is among the most challenging aspects of any real system. There are several industrial noises that can affect the data from sensing devices such as mechanical noise, fluid noise, pneumatic tools, electrical noise, burst noise, flicker noise, thermal noise and shot noise [6]. Dealing with several noise levels simultaneously is very difficult, as the firmware needs to be robust enough to distinguish between noise and actual signal for the sensory framework. The gateway device must hence incorporate a strong noise cancelling system, which is the basis for EMI/EMC compliance. In any commercial establishments or industries, assets and devices are often not located at a single location but are distributed all over [7]. These distributed systems connect with each other to communicate. Connecting devices over distributed locations is tedious as every system needs different interfaces at different locations. Some of the challenges of distributed systems include, the scarcity of software available for distributed systems, network issues such as saturation and the implementation of secure access [8]. The gateway is expected to allow all devices to connect to the cloud. The gateway needs to be an intelligent product that can differentiate between deterministic and non-deterministic data. Industries have various assets and devices which are maintained and supplied by different manufacturers and service providers. Mounting sensors on devices is not a flexible method either because it might be intrusive to the functioning of the device or it might require taking mission critical devices offline to do so. Hence, sensing the performance of these devices becomes difficult. There exists a need hence to extract the data with nonintrusive and noninvasive functionality. The IoT gateway must hence support noninvasive connectivity. Another aspect the architecture must manage is the ability of control to be exercised in three ways namely local, edge and remote control. Industrial systems often require onboard storage, this is used for control or to store programs to make the system more reliable. However, legacy industrial assets have limited memory space which leads to slow functioning and disables add on program storage. More storing capacity can make the systems more efficient and hence an IoT Gateway can be used as an effective interface to the industry, without compromising on the security. This is a difficult task is legacy systems as they might not contain the necessary hardware and software to ensure efficient encryption. The IoT gateway shall provide various security features which can prevent confidential data from unauthorized access. The device needs to be versatile to suit ever changing demands and requirements. An IoT gateway must encompass a compact and easy to install / upgrade



solution that can plug in and modify per the requirements. Energy efficiency is a vital parameter in choosing any industrial solution. With the improvement in technology, IoT gateways can run on very low power owing to the availability of low power SoCs that can power the gateway.

Finally is important it must have an easily scalable implementable solution. An IoT gateway is expected to be plug and play. It offers a ready-made solution that is completely compatible with existing legacy solutions. All these features including the fact that gateways are cheap and flexible make them a very promising step towards integrating legacy systems with the cloud.

#### IV. IMPLEMENTATION AND EXPERIENCE

The key energy contributors in any facility are HVAC (Chiller and AHU), UPS and Lighting. In fact HVAC alone contributes to 50% of the total energy consumption [12]. All the chief contributors of energy across the facilities of TCS were remotely connected using the multi master enabled industrial gateway. Noninvasive sensors were used to obtain the readings from utilities. Thus, without disturbing the existing system, data was collected in a noninvasive manner. National Instruments (NI) based CRIO (Compact Reconfigurable Input Output) was configured to read the data from legacy sensors. Firmware was developed using LabVIEW at an industrial standard of 15 minutes. Figure 3 illustrates a sample CRIO that was used to collect data.



**Figure 3: Data Acquisition and Management - NI Platform**

Another variant of the data acquisition and management was developed using Intel platform with Linux OS. Figure 4 shows the Intel variant of the data acquisition system designed with the framework as shown in Figure 2. It was observed that there was no difference in the performance with respect to data acquisition.



**Figure 4: Data Acquisition and Management - Intel Variant**

Based on the aforesaid engineering experimentation, a vendor agnostic architecture was arrived which was discussed in detail in Section III. With the above implementation, analytics for assets was performed in

Microsoft Azure platform and reporting dashboards were developed using web based application. Downsizing of UPS at various facilities were performed based on the asset energy information. Just in time logistics for asset purchase was enabled with the above implementation. Optimized HVAC scheduling was arrived for effective operation. Residual Life of UPS battery also estimated based on the designed data acquired from data acquisition system.

#### V. CONCLUSION

The need for an industrial gateway and reference architecture was detailed out in the current communication. Various challenges associated with encapsulating a legacy system as well as smart system viz., legacy sensors, types of sensors, proprietary protocols into a IoT framework was discussed in detail. A vendor agnostic framework and architecture for industrial IoT and for commercial establishment asset energy monitoring of assets was provided. Successful implementations of the proposed architecture in variants using National Instruments and Intel was discussed. The implementation resulted in mapping the sensor data to cloud for energy analytics. Various assets (UPS, HVAC etc.) were optimized for performance and supply chain logistics were enhanced. The future work involves edge level control of assets using analytics. Also the stacks for development of light weight protocols needs to be embedded for enhanced processor performance in the gateway

#### ACKNOWLEDGMENT

The authors would like to thank Mr.Thanga Jawahar Kalidoss, Mr. Sandip K. Ghosh of the Engineering and Industrial Services for their continuous support and encouragement throughout the development. The authors would like to extend their thanks to everyone involved during the execution of the work.

#### REFERENCES

- [1] Uckelmann D, Harrison M, Michahelles F (2011) Architecting the Internet of Things. Springer, BerlinJ. U. Duncombe, "Infrared navigation—Part I: An assessment of feasibility," IEEE Trans. Electron Devices, vol. ED-11, pp. 34-39, Jan. 1959.
- [2] Toma's Sa'anchez Lo'pez, Damith C. Ranasinghe, Mark Harrison, Duncan McFarlane, "Adding sense to the Internet of Things, An architecture framework for Smart Object systems" Pers Ubiquit Comput (2012) 16:291–308 DOI 10.1007/s00779-011-0399-8
- [3] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, Vision and challenges for realising the Internet of Things, Cluster of European Research Projects on the Internet of Things—CERP IoT, 2010.
- [4] Jayavardhana Gubbia, Rajkumar Buyyab, Slaven Marusic a, Marimuthu Palaniswami Future Generation Computer Systems 29 (2013) 1645–1660 Internet of Things (IoT): A vision, architectural elements, and future directions

- [5] Berger E.H., Ward W.D., Morrill J.C. and Royster L.H. (1986). Noise and Hearing Conservation Manual. American Industrial Hygiene Association.
- [6] Pekkarinen and Starck, J. C.(1987) Industrial impulse noise, crest factors and the effects of ear muff, AIHA Journal
- [7] Chia-han Yang, Design and validation of distributed control with decentralized intelligence in process industries: A survey, Industrial Informatics, 2008. INDIN 2008. 6th IEEE International Conference pp-1395-1400
- [8] Smart Grid for Distribution Systems: The Benefits and Challenges of Distribution Automation (DA) (Draft Version 2) White Paper for NIST.
- [9] Kamal Sheel , Mishra “Some Issues, Challenges and Problems of Distributed Software System”
- [10] <http://www.sensata.com/download/sensata-sensor-brochure.pdf>
- [11] [http://ee.sharif.edu/~industrialcontrol/Summary\\_Automation\\_Sensors\\_tutorial.pdf](http://ee.sharif.edu/~industrialcontrol/Summary_Automation_Sensors_tutorial.pdf)  
[http://apps1.eere.energy.gov/buildings/publications/pdfs/commercial\\_initiative/hvac\\_volume2\\_final\\_report.pdf](http://apps1.eere.energy.gov/buildings/publications/pdfs/commercial_initiative/hvac_volume2_final_report.pdf).



**Jayakumar VK** has been associated with the EIS unit of TCS as IoT solution architect for the past 4.5 years. He holds a Master’s degree in Applied Electronics. He has an overall industrial experience of 21 years. He is also a certified reliability professional. His expertise include design of data telemetry systems, underwater navigation equipment, systems engineering of electronics. He was awarded the “Young Scientist Award 2010” by the Ministry of Earth Sciences. His works has been published in various journals including Elsevier.



**Kasi Viswanathan Udaiappan** has been associated with the EIS unit of TCS as IoT solution architect for the past 4.9 years. He holds Masters in Management and Bachelors in Electronics and Communication. He has an overall industrial experience of 18 years. His expertise include design of industrial automation systems for various verticals, development of embedded systems, Manufacturing Operations Management, Energy Management and Internet of Things. He has published many white papers on different technical titles.



**Kannan Sankar** has been working with TCS for the last 4.4 years. He has a Masters in Nano electronics. He is currently working in the field of data analytics in Engineering & Industrial Services group of TCS. Kannan has worked as Junior Research Fellow, funded by Department of Science and Technology, Govt. of India, New Delhi, during his Master’s program. He has filed a patent in the field of parallel manipulators. His works has been published in American Scientific publishers and Interscience Research Network.