Industrial IoT: Requirements & Use Cases

15th - 17th Nov, 2016
Shane He, Bell Labs & CTO, Nokia
shane.he@nokia.com
While the past has been about connecting people, the future is about connecting things – improving personal life, optimizing business processes.

The programmable world improves people's lives through automation, enhanced connectivity and intelligence. It also helps industries to become more efficient, agile and real-time.
The Industrial Internet of Things (IIoT) is narrowly-defined as the use of Internet of Things (IoT) technologies in manufacturing.

- Integration of automation and ICT technologies
- Digitalization of devices, communication, platforms, and industrial data
- Major trend with significant implications for the global economy*
- Including manufacturing, energy, agriculture, transportation, ...

* Source: Accenture, Driving Unconventional Growth through the Industrial Internet of Things
2.1 Devices of Industrial Internet: sensors, actuators, and robots
Providing intelligent devices is the first step of Industrial IoT

Device should be digital, functional, and scalable

System should provide complex resource, information, and computing power to devices

Actuator
Sensor
Applications

Capability
Functionality

Submit data
Initiate Monitoring
Advanced Analytics
Device Management
Applications

Cameras
Platform

Deliver Command

2.2 Connectivity for Industrial IoT

Multiple communication technologies

To meet the typical requirements of low latency, ultra reliability, massive deployment, providing multiple communication technologies for all kinds of scenarios:

- Industrial Ethernet
- IPv6
- Industrial WLAN
- Mobile Broadband (LTE, NB-IoT → 5G)
- MulteFire
- Short Range transmission (ISA100, WirelessHART...)

Confidential
2.3 Converged system for Industrial IoT
Interoperability, flexibility, cross domain applications

<table>
<thead>
<tr>
<th>Applications &amp; Services</th>
<th>e.g. Multiple factories dispatch</th>
<th>e.g. Warehouse management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>Security oneM2M Platform</td>
<td>Monitoring &amp; Control</td>
</tr>
<tr>
<td>Connectivity</td>
<td>LTE WiFi Ethernet</td>
<td></td>
</tr>
<tr>
<td>Device</td>
<td>Vehicle RFID Sensor Robot</td>
<td></td>
</tr>
</tbody>
</table>

Semantic
Customized applications
OS interworking
Aligned procedures
Security Solutions
Access management
Intranet and extranet
Firewall
Interfaces interoperability
Equipment integration
Use case of a resource/data sharing architecture

- Building Automation Management System
- Production Safety Monitor & Control System
- Joint decision-making
- Data sharing architecture

Resource sharing

Lights

Cloud Server
2.4 Industrial Big Data
Requirements & Value

- Generate
  - Order
  - Process Schedule
  - Resource Distribute

- Analytics
  - Add value
  - Cost control
  - Improve efficiency

- Interoperability
  - IoT semantic

- Industrial Data
  - Manufacturing
  - Delivery
Use case of the cross factory data delivery

Source: oneM2M TR-0018 Industrial Domain Enablement
3. Standardization Activities

- NIST: Smart Grid
- oneM2M: Industrial Domain Enablement
- OPC Foundation: Unified Architecture
- ITU-T SG20: Requirements
- ISA 100
- Object Management Group: DDS
- International Electrotechnical Commission (IEC)
- Industry 4.0: RAMI 4.0
- IIC: IIRA
- International Organization for Standardization (ISO)
- National Projects
Challenges for future industrial IoT

Interoperability
Cross system
Industries & IT

Mobile devices
Logistics
Latency

Automation Safety
Information Security
Privacy

Convergence

Value of data
New business model

Consumer demand delivery
Customization requirements

C2M support

Mobility

Security

Service