IoT in industrial environments to obtain quality data

Fernando Criado (fercriado@protoinfo.es)
Manager
www.protoinfo.es
Salamanca, Spain

Associated to AETICAL

iotec.usal.es
## Index

### Industry’s challenges
- Principal requirements of IIoT
- Reliability in communications

### Industry machinery overview
- Communication media
- Sensor and actuator control systems
- Monitoring systems
- Automated systems organization
- Industrial networks

### Data acquisition
- From PLCs
- Directly from machines
- A bit of reverse engineering

### Data registry
- In database management systems
- In the cloud

### Conclusions
Industry’s challenges
Principal requirements of IIoT

<table>
<thead>
<tr>
<th>IIoT devices built to be</th>
<th>Must work in extreme conditions</th>
<th>Designed to be more scalable</th>
<th>Difficult accessibility and maintenance</th>
<th>Strong security systems</th>
<th>High customization capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Resistant</td>
<td>• Highest temperatures</td>
<td>• Capacity of increase whenever it is necessary</td>
<td>• Must have great autonomy</td>
<td>• A cyberattack could be fatal and cause large losses</td>
<td>• Adapted according to their function in the manufacturing processes</td>
</tr>
<tr>
<td>• Reliable</td>
<td>• Resistant to rust</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Hardy</td>
<td>• Protection from electromagnetic interference</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Industry’s challenges

Reliability in communications

Unlike the preventive systems, industry requires reliability in communications of sensors and actuators

- Real time working
- Must have accurate data
- In environments where communications can be altered by strong electromagnetic interference
Industry machinery overview
Communication media

Wired communication
- Industrial Ethernet is like Standard Ethernet but more robust
- RS-232, RS-485 serial communication
- HART (Highway Addressable Remote Transducer)
  - Hybrid analog + digital protocol
  - Can share the legacy 4-20mA analog instrumentation current loops

Wireless Communications
- PAN
- Bluetooth / BLE (Bluetooth Low Energy)
- ZigBee – Low power, self healing mesh for communication
- RFID – Readers, Tags, Applications
- LAN – WiFi (IEEE 802.11)
- WAN
  - 3G, 4G and 5G
  - LPWAN (LoRaWAN, SigFox, NB-IoT)
  - Satellite Communications (VSAT)
Industry machinery overview
Sensor and actuator control systems

PLC
Programmable Logic Controller
In industrial processes, sensor and actuator data are governed by PLCs that work in real time

Fieldbus
Usually, sensors and actuators are connected with PROFIBUS DP, Modbus-RTU, CC-Link, CAN, etc. technologies

Industrial Ethernet
In new installations EtherNet/IP, PROFINET, EtherCAT, Modbus-TCP, POWERLINK, etc. technologies are growing
Industry machinery overview
Monitoring systems

**SCADA**

Supervisory Control And Data Acquisition. Software for computers that allows to distance control and supervise industrial processes

**HMI**

Human-Machine Interface is a control panel designed to interact with the process/machine, transmit orders, graphically visualize the results and obtain a situation of the processes in real time
Industry machinery overview
Automated systems organization

Enterprise Level
- ERP
- Business Intelligent
- Cloud
- Predictive systems

Control Level
- SCADA
- HMI

Device Level
- PLC

Sensor Level
- Electric connection of sensors and actuators
Industry machinery overview

Industrial networks

**Industrial Ethernet** has been driven by the IIoT representing 52% of the market with a growth of 22%

**Fieldbus** are widely implemented but with little growth

**Wireless** technologies begin to have a presence with a growth of 32%
Data acquisition
From PLCs

Modbus TCP and RTU
- **Modbus TCP** connect by Ethernet
- **Modbus RTU** connect by COM port using RS-232 or RS485

OPC (Open Protocol Communication)
- **OPC Classic**, Microsoft Windows early technologies: COM and DCOM
- **OPC UA, OPC Unified Architecture**
  Modern Publish/Subscriber communication model over TCP/IP
Data acquisition
From PLCS

Open Source Drivers

- LibNoDave
- Snap7
- Snap7-IoT
  - ARM (Raspberry Pi, Beaglebone, CubieBoard, PcDuino, Udoo Quad, Mele A2000, ..)
  - MIPS (Tested with Arduino Yun)
  - Quark (Intel Galileo Gen 2, Siemens SIMATIC IOT2040)
- S7.Net
- DotNetSiemensPLCToolBoxLibrary

Modbus TCP

```csharp
    // reading
    TcpClient client = new TcpClient("127.0.0.1", 502);
    ModbusTcpMaster master = ModbusTcpMaster.CreateTcp(client);
    // read five input values
    ushort startAddress = 100;
    ushort numInputs = 5;
    bool[] inputs = master.ReadInputs(startAddress, numInputs);
    for(int i = 0; i < numInputs; i++)
    {
        console.WriteLine("Input {0}={1}", startAddress + i, inputs[i] ? 1 : 0);
    }
    // writing
    ushort startAddress = 1;
    bool[] inputs = {false, true, false, false, true};
    master.WriteMultipleCoils(startAddress, numInputs, inputs);
```

Modbus RTU

```csharp
    SerialPort port = new SerialPort("COM10");
    // configure serial port
    port.BaudRate = 9600;
    port.DataBits = 8;
    port.StopBits = Parity.None;
    port.StopBits = StopBits.One;
    port.Open();
    // create modbus master
    IModbusSerialMaster master = ModbusSerialMaster.CreateModbus(port);
    byte slaveId = 1;
    ushort startAddress = 1;
    ushort numRegisters = 5;
    // read five registers
    ushort[] registers = master.ReadHoldingRegisters(slaveId, startAddress, numRegisters);
    for(int i = 0; i < numRegisters; i++)
    {
        console.WriteLine("register {0}={1}", startAddress + i, registers[i]);
    }
```
Data acquisition
Directly from machines

Ad-Hoc Applications adapted to productive processes to collect data of machines and register them in the management system (ERP)

- Ethernet Sockets
- RS-232 Serial Communications
- Converters from RS-485, HART, Current loop, etc. to Ethernet, USB and RS-232 PC connections
Data acquisition
A bit of reverse engineering

In many cases, the existing machinery has incomplete documentation or lacks it.

Sometimes, the only possibility is to sniff the data of existing machinery

- Ethernet Sniffer (Wireshark, ...)
- COM Analyzer
- Others
Data registry
In database management systems

Knowledge of multiple database access drivers
- SQL Server
- Oracle
- MySQL
- PostgreSQL
- MariaDB
- MongoDB

Analysis of data models in existing systems
- Analysis of data tables
- Analysis of the contents of the fields of the tables
- Search for relationships between tables
- Analysis of ERP data and processes
- Maintain the integrity of the data
- Analysis of ERP transactions by tracing queries with tools such as SQL Profiler
Data registry
In the cloud

From applications (Webservices)
- SOAP
- REST
- HTTP

From devices (M2M)
- MQTT
- AMQP
- WAMP
- CoAP
- STOMP
- XMPP
- WMQ
- CoAP
Conclusions

During the last half decade, the Enterprise Resource Planning (ERP), Manufacturing Execution Systems (MES), and SCADA have tried complementing each other in industries, but haven’t been able to gain the expected success levels.

This has left the gap wide open for IoT, analytics, and cloud based technologies to fill in the gap between ERP, MES, and SCADA.