SCCE

Secure Communication and Control Experts

In Depth Understanding of IoT and IIoT Ecosystems is Critical

Author: Daniel Ehrenreich, Consultant and Lecturer, SCCE

Introduction

The world will see a step forward towards the Internet of Things (IoT) and Industrial IoT (IIoT) ecosystems, when people will focus on in-depth understanding of how these ecosystems shall be structured without creating cyber security risks and how will they deliver operating and financial values. Important pointing out, that these end-point devices are not communicating each with other (peer-to-peer), but are collecting and sending data to their designated service providers, which upon analyzing the field conditions publish decision-oriented data. Once accepting these highlights, we may start talking about tens of billions IoT and IIoT devices expected in 2020 and 2030.

This paper is aimed to outlining the key considerations related to IoT and IIoT ecosystems, allowing you making business-wise decisions. You shall always verify that the proposed IOT or IIoT ecosystem concept is matching your expected goals and last but not least verify that the proposed ecosystem architecture complies with IoT /IIoT cyber security challenges.

IoT and IIoT Ecosystem Service Providers

Important to point out that IoT or IIoT devices are usually not communicating each with other, but each one shall communicate with its designated service provider. These supply chain computers (see illustrations below) perform a dedicated process related to each ecosystem they handle. Their operation is technology-oriented and business oriented and is aimed to generate the desired operating and cost benefits. The IIoT ecosystems may utilize the same sensing devices which are monitored by the ICS, or communicate with temporarily added IIoT devices, not linked to the ICS.

Table below is outlining few examples of specific "Service Provider" operations which are communicating with IoT and IIoT end point devices, analyzing the received data and are publishing (via the internet or via a secured channel) applicable business or maintenance related decisions.

IoT Ecosystems Service Providers	IIoT Ecosystems Service Providers
• Commercial and Retail ○ Temperature in the store refrigerators ○ Number of people present during the day ○ Level of stock on shelfs/in refrigerators	• Maintenance Prediction on Machinery ○ Data collection on Vibration Monitoring ○ Electric Motor temperature vs. speed ○ Pump efficiency monitoring & fault analysis
• Smart Cities ○ Monitoring # of people at each bus station ○ Tuning the buses' schedule accordingly	• Smart City Street lighting ○ Smart adjusting of the street light level ○ Compensating light intensity for faulty lamps
• Personal Health ○ Consistent analysis of smart watch data ○ Alerting on anomaly condition (hearth rate)	• Cars' and Trucks' Supervision ○ Based on constantly monitored parameters ○ Analysis of malfunction problems & alerts
• Smart Home's Supervision ○ Air condition optimization in each room ○ Cost effective use of laundry machines	• Agriculture Irrigation ○ Irrigation according to soil condition ○ Setting based on the weather forecast
• Just-In-Time Supply Logistics ○ Raw material sent to the production line ○ Periodic monitoring of production rates	• Manufacturing Process Control ○ Allows intelligent tuning of production rates ○ Preventing bottlenecks in processes

IoT Ecosystem architecture

When dealing with commercial-type applications, such as are listed in the left side of the table above, we must pay attention to all system the system sections which comprise the IoT ecosystem:

a) The installed sensors are monitoring the relevant parameters applicable to the IoT ecosystem
b) The network can be cellular (1 step) or a 2 steps link using a gateway and a short-range link
c) A cloud-based service provider/supply chain is handling the IoT ecosystem and publish the results of the analysis to 3rd party users and/or the organization which handles each ecosystem.

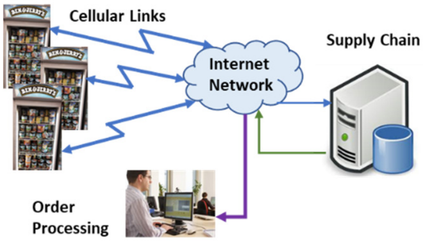

Fig 1. IoT ecosystem through cellular

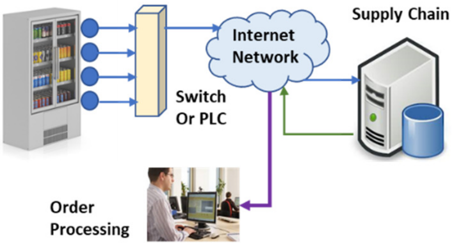

Figure 2: IoT ecosystem through IoT gateway

Figure 1 and Figure 2 above outline 2 typical configurations for connecting IoT field devices with their IoT service provider through a 1 step wireless link and a 2 steps communication network using a gateway.

IIoT Ecosystem architecture

In industrial-type applications, such as are listed in the right side of the table above, some IIoT ecosystem architectures may reuse the existing sensor devices (part of the installed ICS) and some other IIoT ecosystems may require adding new IIoT devices, completely isolated (for cyber security purposes) from the ICS. In this case the following components and system sections comprise the IIoT ecosystem:

1) <u>Architecture similar to IoT Ecosystems</u>

Figure 3 and 4 below are showing two IIoT ecosystem architectures which are similar to IoT Ecosystems. On the left side you see several pumps monitored through a cellular network connecting the service provider to a single sensor. On the right side you see several sensors attached to a pump for monitoring multiple parameters through an on-site PLC which process the collected data. If required a secure unidirectional gateway (diode) can be optionally added.

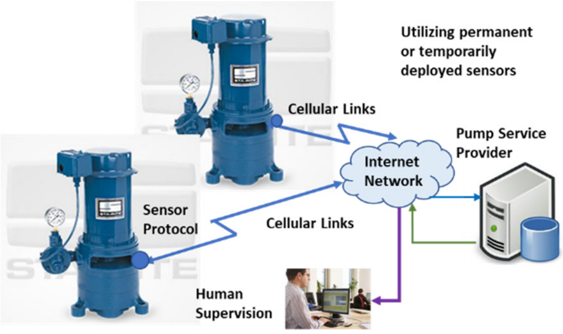

Figure 3. IIoT ecosystem utilizing a cellular network

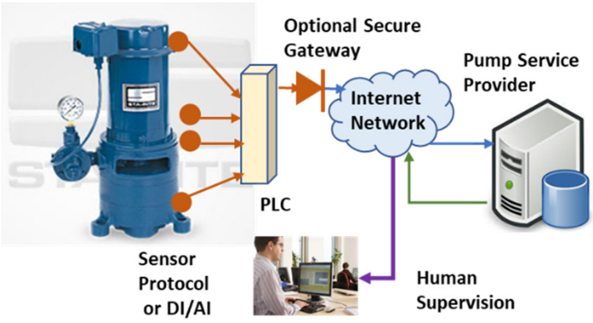

Figure 4. IIoT ecosystem using a PLC collection

2) <u>Reuse of existing sensors which are part of the ICS</u>

a) The ICS sensors are monitoring relevant parameters, also applicable to the IIoT ecosystem
b) These sensors are monitored through the gateway (Fig 5) and the data is sent to the IT network
c) The IT system is publishing the relevant data by a webserver accessible via the Internet
d) A cloud-based service provider/expert center, is handling that specific IIoT ecosystem process, and it will resend the results of the analysis to users or the organization's IT network.

3) Adding new sensors, which are isolated and independent from the ICS

a) The added field sensors are monitoring the relevant parameters applicable to the IIoT ecosystem
b) The data is collected via a data gateway (Fig 5) which is linked to the organization's IT network
c) The IT system is publishing the relevant data by a webserver accessible via the Internet
d) A cloud-based service provider/expert center, is handling that specific IIoT ecosystem process, and it will resend the results of the analysis to users or the organization's IT network.

Figure 5 below is outlining a combined IIoT ecosystem configuration as described in para 2 and para 3 above. As mentioned, the existing sensors will always communicate with the ICS control center through a PLC linked to the network. If for the IIoT ecosystem's purpose, there is a need to add additional (permanent or temporary) sensors, these shall be linked through PLC directly to the IT network. If required for enhanced cyber defense purposes, a secure unidirectional gateway (diode) can be added.

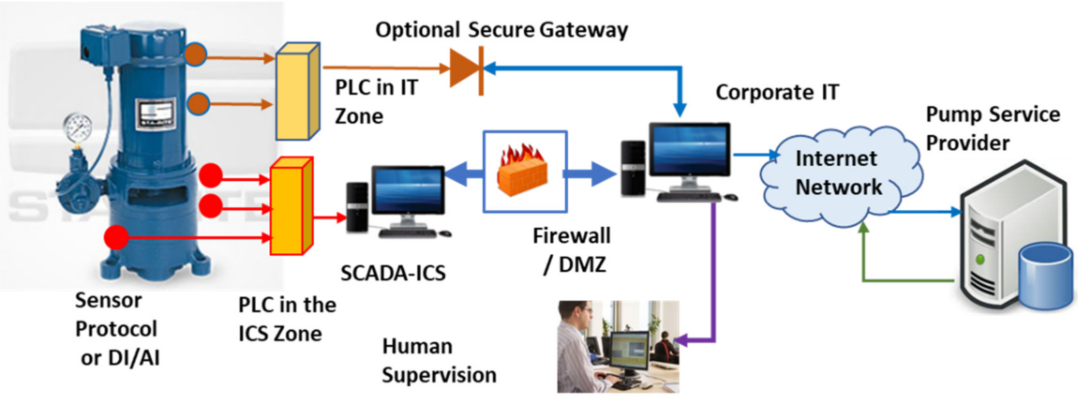

Figure 5. IIoT Ecosystem utilizing existing ICS-related sensors and additional IIoT sensors.

4) Peer to Peer connection among IoT devices

Deployment of IoT end point devices is primarily done for periodic or on-demand monitoring of local conditions related to a broad range of commercial applications. There are just rare cases when these IoT end point devices are required to exchange data each with other. Furthermore, deployment of such process might significantly increase the system complexity and might lead to incorrect processes.

As majority of these devices are not capable exchanging and processing data received from other devices, peer to peer lings are not expected to be popular. However, in the future, when new applications and next generation IoT end point devices will be available and supported with cyber secured communications capabilities, we may see configurable options which allow IoT devices in peer-to-peer configuration.

5) Peer to Peer connection among IIoT devices

Similarly, to explained for IoT ecosystems, in IIoT ecosystems serving industrial applications (see table above), majority of the end point devices are also deployed for monitoring purposes. However, here we must differentiate among IIoT endpoint devices which permanently or temporarily deployed (see figures 3 and 4 above) and those which are part of the ICS architecture (See figure 5 above).

In some specific ICS architectures, IIoT end-point devices may be responsible for assurance of operating safety and reliability. In such cases, they need to perform active operation in coordination with the local ICS control center or the Automation Server (AS). For example, a pump can be activated to fill the water tower even if the ICS control center failed issuing such command and the water tower is almost empty. If peer to peer communication is requested for ICS type operations, in such case the operating range, may be limited to certain time frame or limited to particular parameters.

These functions must be highly reliable and therefore, if peer to peer link is required, they must utilize advanced-type IIoT devices with strong communication capabilities allow. Furthermore, if the peer to peer link is required to activate a Safety Instrumentation System (SIS), such function must be carefully designed and tested to prevent its activation due to "false-positive" detection or other faulty condition.

IoT and IIoT related Cyber risks and defenses

Expanding existing infrastructures (commercial or industrial) with large number of IoT and IIoT end point devices significantly increase the "cyber-attack surface". The meaning of this statement is, that attackers may easily find a huge number of "entry-gates" to your commercial or industrial architecture. The "attack vector" selected for the action describes the path and the available barriers which the attacker from the entry point until he reaches the device or computer which shall be compromised in order to accomplish his attack. Obviously, the lager is the attack surface, more attack vectors can be described and shall be protected. The following list describes some applicable IoT/IIoT defense methods (partial list).

- Physical security shall be in place to prevent unauthorized people from accessing IoT/IIoT devices. Prior installations, these devices shall be configured with a private username and password.
- Both IoT and IIoT devices shall be authenticated prior connection to the network. To maintain their operation and detect any manipulation, these devices shall be properly supervised.
- In case the data is confidential or critical, consider adding end-to-end encryption such as IPsec. Use of cellular communication provides reasonable cyber defense as these channels are encrypted.
- IoT/IIoT devices shall not allow manipulating their program and operating conditions. Locking of these capabilities will prevent converting these devices to an attack tool (part of DDoS process).

Summary

In this paper I outlined multiple system architectures applicable for IoT and IIoT ecosystems. Furthermore, it is important pointing out that all ecosystem-architectures such as outlined above must comprise an entity which handles the IoT/IIoT end point Device Management, responsible for fault monitoring and periodic software updates. Finally, important to emphasize again the following topics:

a) IoT and IIoT devices are not communicating each with other (some exceptions are possible)
b) They communicate with a service provider which provides the operating and financial values
c) IoT and IIoT Ecosystems may utilize similar sensors but the service provider performs different tasks
d) Cyber security shall me an important component for most commercial IoT ecosystems but is highly critical for IIoT Ecosystems serving operation of manufacturing and utility processes.

The achievable benefits delivered by these IoT and IIoT ecosystems always depend on the performance of the (cloud-based) service provider. Understanding these topics will help your organization to deploy successful IoT and IIoT ecosystem. Defining IoT/IIoT architectures in collaboration with the business experts and the IT and OT cyber security experts will put you a step ahead of the attackers.

Daniel Ehrenreich, BSc. is a consultant and lecturer acting at Secure Communications and Control Experts, and periodically teaches in colleges and present at industry conferences on integration of cyber defense with industrial control systems; Daniel has over 27 years of engineering experience with ICS for: electricity, water, gas and power plants as part of his activities at Tadiran, Motorola, Siemens and Waterfall Security. Selected as the Chairman for the ICS Cybersec 2019 conference taking place on 16-9-2019 in Israel and for the Asia ICS Cyber Security conference taking place in Singapore on 7-11-2019. LinkedIn