SCADA systems vs IIoT solutions

A debate on the benefits of IIoT solutions vs. traditional SCADA systems

AUTHOR: ANTHONY GLUCINA, PRESIDENT, DEFINE INSTRUMENTS
EMAIL: anthony@defineinstruments.com

Over the last 12 months I have consulted on many IIoT projects for industrial companies across the U.S. These companies have varied from value-added distributors to systems integrators to end users.

During discussions I have found it interesting to note reactions to the inclusion of IIoT in the application. One of the most common reactions forms the basis of this article.

Typically it goes something like this...

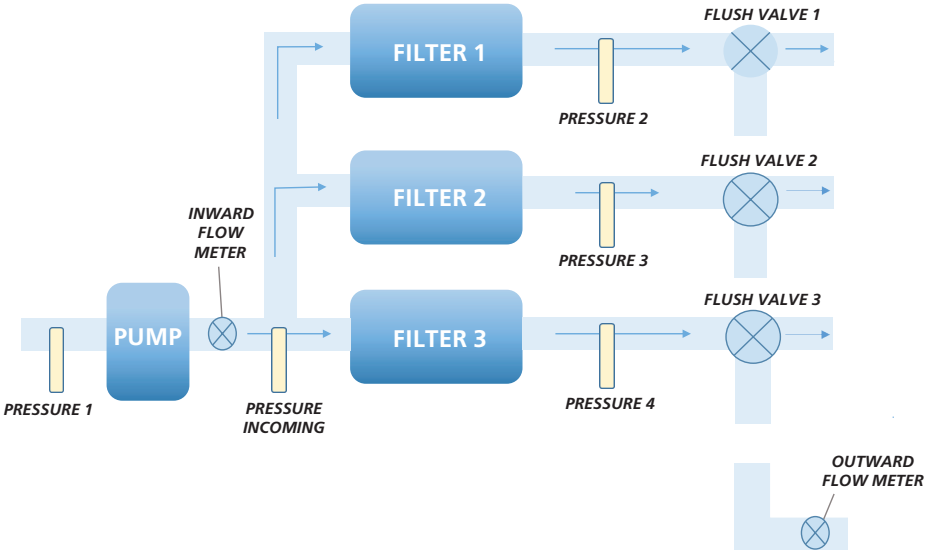
After discussing specific needs there would come a point in the conversation where I would mention Remote Monitoring and Control of Assets, to which the typical response was:

"But we're already doing this with our SCADA systems, what's the difference?"

This is an excellent question and the best way to answer is by comparing the two approaches.*

Remote Monitoring & Control in a Water Filtering Station

For our comparison I have selected a recent application in the Water/Wastewater industry. This system includes the Remote Monitoring and Control of a large water filtering station for irrigation in the Florida region.



An RTU has been programmed to monitor and control the filtration system and by measuring the differential pressure across the filters, the RTU automatically performs a backflush of the filters when required.

The RTU also monitors the flow rate and total flow of water and wastewater. From the information one can determine the general health of the system.

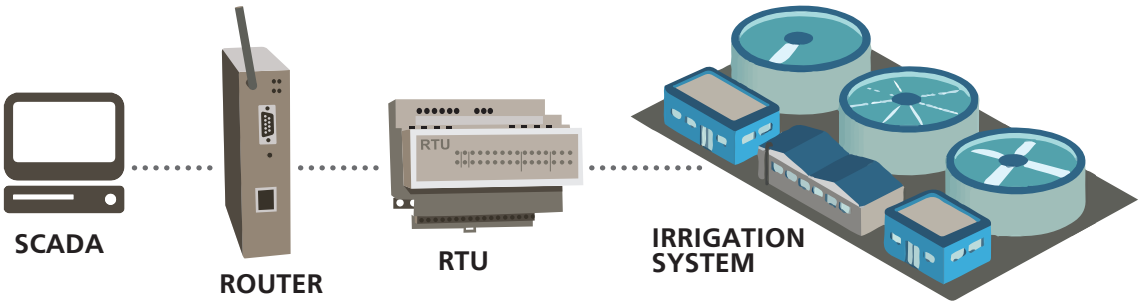
Investigating the reasons for faults currently involves humans

Occasionally, the unit in the field will trip out and stop working. The customer then has to send a technician to the site – a drive of around 3 hours.

When the technician arrives, quite often the only action required is to reset the system, as most of the time this clears the fault.

But what the customer really wants to know is why the system tripped in the first place and how necessary was it to dispatch a technician to the site. If a technician was not required, could the system be reset remotely?

These questions can be only answered by looking at the data from the sensors before and after the trip event.



And so using the traditional approach, a SCADA system must be installed to receive this data. As the system is usually deployed on hardware at the customer's premises, the following must be considered:

- What level of reliability is required?
- Should it be running on Server Grade Quality devices?
- Should a backup power system also be installed?
- How much will this cost in capital and maintenance?
- Who will manage this system?

Once these questions have been answered, the SCADA application can be built. It will of course require a data historian, the setting up of a mimic and possibly an add-on package to deal with the telemetry aspect of modem etc.

Addressing security within the SCADA system

During the building of the system, security must also be addressed. The industry standard approach to this is to add a VPN connection between the SCADA PC and the RTU in the field. This requires using a powerful cellular router that has the capability to both perform the VPN function and to open a port in firewalls and connect to a DNS.

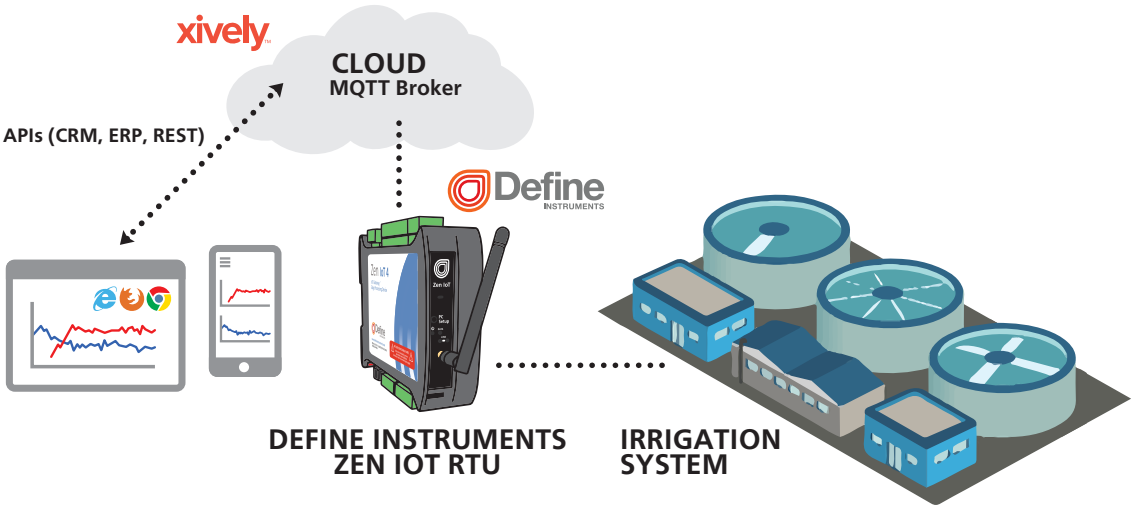
Once the VPN is set up, the SCADA can be set to run mode and will begin polling the RTU in the field.

As is clear, deploying this system is not for the faint-hearted. It requires expert help from engineering or IT professionals and could take some time to set up and test.

The IIoT approach

In the IIoT approach, the first consideration is the choice of Cloud Platform Provider. This is an important first step as not all Cloud providers are created equal – I would consider this as important as selecting the correct hardware.

In this example I have chosen the Xively platform as it has a powerful Connected Product Management feature (CPM) which allows organization of products in domains and sub domains, the importance of which will become clear later.



A typical IIoT system uses a broker in the Cloud. I have chosen to use an MQTT broker as it is available in most Cloud systems.

Coupled with this is the Define Instruments Zen IoT RTU. The difference between this and the traditional RTU is that it is setup to deliver messages to the Cloud broker using MQTT. It uses a publish and subscribe model: the Zen IoT RTU will publish information like pressure and flow rate to the broker and subscribe to a control topic.

Control topics are used to perform tasks such as turning on a relay in the RTU.

The other major difference is that the Zen IoT RTU itself makes the connection to the broker and it does so in a secure mode using TLS and certificates.

This eliminates all the issues related to setting up VPNs, DNS and firewalls. The only information that has to be provisioned in the IIoT RTU is the username and password associated with the Cloud account.

The information is now sitting in the Cloud and in this location it is available to the humans and devices who have permissions to access it. The Cloud platform enables this by providing a rich set of APIs, rules-based engines and standard interfaces to CRMs and ERPs.

For this application a dashboard is required to visualize the data. There are 3rd party dashboards available but in this instance a webpage was created to visualize the data using the REST API. This is akin to setting up the mimic in the traditional SCADA system.

So at this stage in our comparison, the IIoT approach is obviously the simpler of the two to setup for a secure application. And one that avoids the headaches of server-side hardware. You do however have to pay a monthly subscription to the Cloud provider (around $1 per month for this application).

Thinking into the future

Let's now examine a post-installation scenario.

After a few months of using the system the customer comes back and says:

"The system is great! So great in fact that I want to roll it out to monitor the 400+ filtration systems I have throughout the country. And I have some changes..."

The customer explains his clients would like to:

- see how much water they have been using
- see how much wastewater was lost
- manually turn the system on and off by logging in to a website

He further explains how he personally would like to:

- know when the pump has completed 1000 working hours (to schedule maintenance)
- be alerted via his CRM at the 800 working hours mark

Lastly, he leaves this juicy tidbit:

"I was recently speaking to a pump manufacturer and he asked if we could share with him some of the pump data so he could use it to improve his product. I don't see any reason why not..."

The IIoT solution provider can confidently accommodate these requests. He knows that his Cloud partner already provides CRM alerts as a feature, he also knows the Connected Product Management system is another feature already in place to provide different permissions to different users.

All the IIoT solution provider has to do is:

- make 2 new dashboards
- create accounts for the new users
- provision these credentials into the Zen IoT RTUs

But where does the engineer come in? In actuality, an engineer isn't required at all in the commissioning of the sites as an electrician can wire up the units in the field.

After wiring, the electrician isn't required to do much more, just turn them on, run through an automated test setup and ensure any issues are sent as alerts directly to their cellphone (the last part requires a little more work – but just a little).

Employing the IIoT approach, the customer's requests are a cinch to implement and it's smiles all round.

The SCADA headache

Not so for the SCADA provider.

Unfortunately, faced with these requests from the customer, they are plagued by a sense of panic and overwhelm. So many questions, ones like:

- Will the server be up to the job?
- Will it require an upgrade?
- If so, how much will that cost?
- With 400+ VPNs concurrently talking to the field devices, can the SCADA system handle it?
- How will all the permissions be managed to allow 400+ users to get information on the site

Suffice to say that the IIoT system wins hands down when faced with a scaling issue like this. Not only that, the capital and development costs for IIoT are far smaller. As are the costs of expert professional help from engineers and IT specialists.

But this application could just be the start of this customer's IIoT journey.

For example, the information obtained from the systems over time could be useful for improving the design as well as determining the real maintenance and running costs associated with such a system.

Armed with this knowledge, a new business model could be evolved. Offering a maintenance agreement based on the water pumped, for example. Or partnering with a finance company to offer a pay-as-you-go service so clients are only billed for the actual water pumped.

In conclusion, the benefits of implementing an IIoT solution over a traditional SCADA system go beyond the immediate wins of cost, timeline and required expertise. It is also highly scalable and adaptable to customer needs in the future. Anything that gives such a level of security, peace of mind and readiness for what might be over the horizon is an undeniable asset to your business and to everyone else's.

** I have assumed that both approaches require a highly secure solution.*

About the Author

Anthony Glucina is an IIoT consultant and President of Define Instruments, an industrial instrumentation manufacturer. He has worked in the industrial engineering space for over 25 years and holds a Master's degree in Engineering.