The Advantages of Cloud-Based SCADA Systems for Operations

By Jon Tandy – Elecsys International (A Lindsay Company)

The "Cloud" is rapidly transforming our world. Its impact is being felt everywhere, from cell phones to coffee makers. Everyone seems to want to be connected. Cloud solutions promise to increase value for consumers, manufacturers, and service providers. In the industrial sector, the July 2020 Forbes article touts the Cloud as the "Future of Industrial Monitoring."

In the last several decades, adoption of "IIoT" (Industrial Internet of Things) has accelerated, whether using traditional private networks or newer "cloud" solutions. IIoT has advanced due in part to advancements in remote monitoring units (RMU), communication modes (cell or satellite), software tools, edge devices, data storage options, and central dashboards. Smart, progressive industrial companies can now employ IIoT to enhance how they do business in the 21st century.

Over the past several decades, **Elecsys International** (A Lindsay Company, Olathe, KS) has been a driving force in the IIoT revolution. Elecsys began with rugged, reliable cathodic protection monitoring systems for oil and gas pipelines, then developed IIoT programs for various industries. The US company designs and builds remote monitoring units (RMUs), edge devices, "smart farm" ag control systems, and liquid crystal displays. Elecsys offers state-of-the-art electronic manufacturing, engineering, and software development designed to facilitate IIoT and SCADA systems.

The Challenges and Benefits of IIoT

IIoT promises to:

- Enhance industrial efficiency and productivity by optimizing human activities and business processes.
- Increase cost savings through remote reporting of emerging problems. IIoT reduces the need for routine, onsite human inspections and service interventions.
- Facilitate compliance with regulatory requirements.
- Support effective, timely, and well-informed decision-making.

IIoT helps industries discover problems long before they become major issues or failures and keeps production systems running optimally. SCADA (Supervisory Control and Data Acquisition) systems alert staff to concerns before they spin out of control and allows firms to make better business decisions with optimal investment.

Remote monitoring units (RMUs) and sensors receive data from industrial activities, the environment, or machines, and transmit their data either directly or through edge devices into the "cloud" (or local network). Data can then be tracked, disseminated, and further analyzed at a central location. Depending on the set parameters, monitored data can trigger alarms and actions in the real world. Once a problem is detected, the system can send the location and situation details to service personnel. Armed with timely data from the IIoT system, firms can improve the way they work and do business moving forward.

PaaS (platform-as-a-service) and SaaS (software-as-a-service) providers, such as Microsoft Azure, Amazon Web Services, and IBM BlueMix, offer full-featured and rapid application development platforms. These tools are mature, and their systems can integrate data to provide better visibility of business processes. But there are challenges to overcome:

- The increasing volume and types of data can overload transmission channels and storage capacity. Edge devices (such as Elecsys Redigate products) help reduce the volume of transmitted and stored data by performing data analysis and logic functions before passing the central dashboard.
- Communication requirements must be chosen from a diverse set of options (cell service, satellite, etc.). Users must take into consideration network bandwidth, reliability, security, and latency.
- Legacy protocols must be considered for retrofit applications

Users of IIoT systems must also consider:

- Communication costs
- The data and control capabilities of each unit
- The effort to configure, update, program, and manage remote devices and their data
- The security of the cloud platform or corporate network

SCADA and the Cloud

SCADA control systems facilitate high-level process supervisory management activities. One can find SCADA systems in many industries, from oil & gas and energy companies to food & beverage, process manufacturing, tank truck loading stations, and anything requiring real-time operational monitoring and control of equipment.

A typical SCADA system combines links, sensors, edge devices, computers, and networked data communications with data fed to a central user interface - the SCADA "host." The system often includes peripheral devices like programmable logic controllers (PLCs) and discrete proportional-integral-derivative (PID) controllers to interface with process plant or machinery.

An excellent example of a central dashboard is **Elecsys Connect**. "Connect" is designed to display periodic reporting and situational notification from multiple RMUs using web-connectivity. Connect offers routine monitoring with automatic and frequent updates, which works well for many applications. On the other hand, Elecsys International's RediGate edge devices provide SCADA systems with real-time data fed to control rooms that monitor live data updated within seconds and are staffed 24/7 by operators. Construction and other industries use SCADA to manage operations and project-driven processes.

Over the last 10-20 years, traditional SCADA systems have fallen behind on several fronts. Older SCADA systems maintain real-time control and monitoring of operational data. However, over time, firms began to need additional data outside the rigid SCADA network, such as hourly or batch flow measurements, calibration of sensors, responsive gas quality calculations, and CP monitoring. A broader view of data acquisition was necessary. More timely data acquisition and analytics were needed to manage business

processes, improve measurement and maintenance, streamline billing, and support ERP and CRM systems. The deficiencies in old-style SCADA systems led to the rapid advancement of new methods that promise to revolutionize our industrial future.

Older SCADA systems use a poll-response model to acquire data. With this method, each device reports to a single host on a one-to-one basis. The rigid relationship between the device ("thing") and the host ("app") made it difficult to scale the system. If another department asked Operations for data, the response was often, "Go get your own data." Operational data was collected from discrete devices and fed in "silos" unable to operate in real-time and connect.

In other cases, personnel needed to retrieve the data from test stations manually. The result was an inefficient and disconnected data gathering process. Increasingly, firms have begun to recognize the need for "big data analytics" and a holistic approach to increase operating efficiencies.

MQTT Publish/Subscriber Architecture

Enter "MQTT" (Message Querying and Telemetry Transport) – a publisher/subscriber architecture initially applied to the oil and gas pipeline industry. **Elecsys International** was an early adopter of this technology for its SCADA systems. Elecsys has been a significant IIoT player for decades and is uniquely positioned to apply this technology.

MQTT is an OASIS (Organization for the Advancement of Structured Information Standards) open standard and is certified by ISO/IEC 20922 as a standard messaging protocol. MQTT has been instrumental in facilitating the Internet of Things (IoT) and other uses, such as Facebook Messenger. Its publish/subscribe network architecture is:

- Simple, straightforward, and flexible. It is lightweight in terms of its demands on network bandwidth and requirements
- Ideal for constrained devices and systems with low bandwidth, high latency, or uncertain reliability, while still ensuring an efficient delivery
- Ideal for connecting remote devices using a small code footprint
- Well suited for mobile applications where bandwidth and battery life are at a premium
- Able to be combined with TLS or VPN encryption, access control lists, etc.
- Able to be built into many different enterprise middleware packages and Cloud solutions
- Highly flexible as an architecture for data payloads

Today, MQTT appears in industries beyond oil and gas, such as automotive, manufacturing, telecommunications, etc. MQTT breaks the rigid 1-to-1 link between device and host, allowing a device to publish data easily accessed by multiple host systems. MQTT is now one of the leading protocols for Cloud/IoT/IIoT solutions since it can connect various devices to numerous applications. Due to its small bandwidth requirement, MQTT does not burden other real-time SCADA operations and enterprise-related data. MQTT takes data from "publisher" devices and makes it available to "subscriber" applications. MQTT is ideal for report-by-exception and push-messaging. MQTT v5.0 and v3.1.1 are now OASIS standards, and ISO has ratified v3.1.1. TCP/IP port 1883 is reserved with IANA for use with MQTT. TCP/IP port 8883 is registered for use with MQTT over SSL (Secure Socket Layer).

Is the Cloud Secure Enough for Operational Technology?

So, what about security? Are Cloud-based IIoT systems secure enough for Operational Technology (OT) systems in critical infrastructure applications?

In 2014, at the API Cybersecurity Conference, the answer from many participants from significant oil and gas companies was, "probably not." At that point, the "Cloud" seemed like the "Wild West" of the public internet, full of spam, viruses, and hackers.

OT systems have historically relied on private networks to ensure security and reliability. SCADA systems used dial-up, leased phone lines, private networks, and private radio systems for communication to field devices. Security was based on the inaccessibility of the systems by outsiders.

But this reliance is proving to be unsustainable, given current Cloud development. These older technologies are either going away or are too difficult to manage with a reduced staff of skilled technicians. The old approach fails to benefit from what newer Cloud-based solutions can offer. With current IT technologies, OT functions can take advantage of Cloud opportunities without compromising the reliability and integrity of critical operations.

New SCADA systems are increasingly turning to cellular modems through public carriers (AT&T, Verizon, Sprint), along with satellites in remote locations. Although they are public carriers and use the same cellular towers and back-end networks as commercial data traffic, they can still ensure the safety of secure "private" communication networks through:

- Dedicated router channels
- Encrypted MPLS (multiprotocol data label switching) and VPN (virtual private networks) connections
- End devices that may also use encrypted protocols to ensure data integrity over the air

Unlike completely public airwaves, MPLS/VPN connections provide robust security that isolates critical systems from risks that might exist on the carrier network's public-side. Also, carriers like AT&T employ thousands of employees to monitor networks for security incidents and threats. Cloud solutions use the same IT principles, which offer:

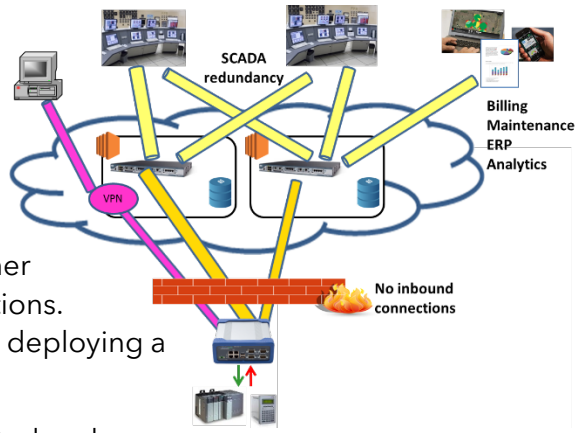
- Secure authentication/encryption from field devices to the Cloud
- Secure the MPLS or VPN from the Virtual Private Cloud to the corporate enterprise.

In this way, users can combine a private network's benefits with Cloud-hosted IIoT solutions' powerful features. Cloud solution providers, such as Amazon Web Services (AWS), also employ thousands to maintain their infrastructure and protect the security of their networks. Contrast this with the relatively limited IT staffing resources of even the largest oil and gas or electric utility companies.

Toward a Better SCADA

Here is a practical example of a SCADA upgrade that can bring the benefits of IIoT to a traditional OT solution. A liquids pipeline company wants to migrate from an old poll-response SCADA system to a modern MQTT multi-client architecture. What needs to happen?

The first step is to add an edge gateway to gather data from legacy field equipment through redundant satellite and cellular modems. The edge gateway includes a wide variety of wired and wireless connections, including serial links. The I/O on the intelligent device makes it easy to connect legacy industrial systems with your new network. The gateway uses Ethernet, cellular, or other wireless networks to connect and communicate. The gateways give pass-through access, so the existing SCADA poll-response system can operate with the new SCADA running in parallel.



Next, the company implements Cloud-based MQTT servers running in redundant Virtual Private Cloud systems. The gateways use report-by-exception and periodic updates to publish field data using MQTT. Rather than polling over the air, the new SCADA system uses the MQTT subscriber to gather field data. Access Control Lists further secure remote connections. Cloud server instances can be quickly set up or shut down for deploying a test environment in parallel with the current polling system.

Security is assured from the Cloud to SCADA through dedicated and secure MPLS/VPN circuits. MQTT through TLS-encrypted tunnels and firewall on the gateway devices, ensure device security. Due to redundancy and high-availability Cloud servers, the system can run with near 100% availability. Once the new system is validated, the user can eliminate poll-response messages, remove the pass-through configuration from the gateways, or retain pass-through for occasional direct access to the end devices (such as remote PLC programming).

For devices located on public networks, such as cellular modems, the gateways can block all inbound (mobile-terminated) connections for additional security due to MQTT's client-originated nature. The user can set up a permanent or on-demand VPN connection to the gateway for maintenance or real-time diagnostics if needed. In this way, there is no compromise of device-level security.

In addition to real-time data for the SCADA system, the gateway can also acquire non-real-time data and publish it using MQTT using different topic names. Many other business systems, such as measurement, billing, maintenance, ERP, etc., can subscribe to this data to implement intelligent business analytics processes to improve financial or operational performance. The SCADA system need not be burdened with these other data publications.

The Future of SCADA

In summary, Cloud/IoT solutions are everywhere, and the migration towards them is inevitable. There are many significant benefits and limited risks. The cloud solution offers:

- Rapid deployment of powerful applications
- Cost savings, efficiency, analytics
- Data archival and retrieval
- Robust and redundant networks architecture
- Ease the burden on company IT resources

Adopting a new system still involves some challenges:

- Diverse data, protocol, and network requirements
- Latency, bandwidth, isolated data silos
- Tight coupling between device & host application
- The entrenched mindset of "private SCADA" systems

Operation Technology (OT) tends to dismiss the benefits of the Cloud in favor of traditional networks' perceived security. However, their companies are already turning to IT solutions (VPN, etc.) to utilize public carrier networks, challenging this perception.

The MQTT protocol provides a flexible architecture, next-generation data acquisition, using low bandwidth publish/subscribe technology. New technologies can be adopted using data gateways to acquire and post field-data for real-time (SCADA) and other enterprise applications. Authenticated/ encrypted VPN and tunnels, access control lists, etc. ensure device security. Enterprise reliability and network integrity are secured using MPLS/VPN connections from high availability Cloud servers.

This transition from traditional SCADA to cloud-based IIoT need not require a substantial investment in hardware, software, and network management. The user can achieve the benefits of cloud solutions without sacrificing private networks' security by combining IT with OT solutions.

For questions about this white paper, contact:

Jon Tandy, Product Line Manager, Industrial Data Gateways

Elecsys International (A Lindsay Company)
846 N Martway Court
Olathe, KS 66061

General phone: (913) 647-0158

Customer Support: (913) 825-6366

sales@elecsyscorp.com

****

Elecsys International (A Lindsay Company), headquartered in Olathe, KS, is the industrial technology arm of Lindsay Corporation (Omaha, NE). Founded in 1980, the firm serves the IIoT needs of the oil/gas, rail, infrastructure, agriculture, and aerospace industries. Its "Elecsys Connect" system serves as a hub for various IIoT networks and fields an average of 148,000 transactions per hour from clients all over the US and internationally.

Elecsys International offers a full array of US-based, in-house engineering capabilities, hardware manufacturing, software, and firmware development. The firm offers specific expertise in remote monitoring devices, sensors, and network gateways designed for demanding and rugged environments. Elecsys is DoD ITAR Certified and Clean Room compliant.
