



Honeywell

Cloud SCADA

Creating Greater Computing Power, Information Sharing,
and Increased Capabilities





INTRODUCTION

For several decades now, SCADA systems have been driving industrial processes and gathering critical data for facilities all over the globe. Yet, it's been within the last few years that we've seen an exponential growth in SCADA capabilities through the advent of the Industrial Internet of Things (IIoT) and Industry 4.0 to drive advances in cloud computing and overall production efficiency.




At the same time, however, these rapid technological gains are bringing with it a new set of threats and vulnerabilities for process companies and their SCADA systems. Increasing numbers of cyber threats and hacking incidents drive companies to desperately search for that balance between optimized production efficiency and secure, constant operation. In order to help process engineers, managers and executives better find that balance, Honeywell and the International Society of Automation (ISA) have worked together to create this in-depth eBook on Cloud SCADA. This digital resource brings together all the information on the latest advancements in computing power and capability, as well as the best practices to secure your SCADA system and the facility overall.

This Cloud SCADA guide has useful articles for everyone from novice SCADA engineers to seasoned facility operators and their executives, including resources such as:

- A detailed look into the history of how cloud computing has driven enhanced SCADA applications such as cloud analytics and machine learning and where these advances stand today.
- A look at one Canadian oil & gas company's experience in teaming with Honeywell to connect multiple oil wells and facilities and bring them into the world of cloud connected operations
- A crucial piece on securing SCADA operations in the cloud, and how to best ensure that company gets the best out of their cloud technology while closing loopholes to hackers.



CONTENTS

-  **SCADA Meets Cloud Computing**
By: Bill Lydon [Page 4](#)
.....
-  **Experion® Elevate enables visibility to production gas wells in record time**
By: [Page 8](#)
.....
-  **Securing SCADA in the Cloud**
The Best of Both Worlds: Flexible and Secure
By: [Page 12](#)
.....



SCADA meets Cloud Computing

By: Bill Lydon

The dramatic growth, capabilities, and economics of cloud computing is creating opportunities for more efficient and broader SCADA applications with lower overall lifecycle cost. The Internet of Things (IoT) and Industry 4.0 initiatives embrace a range of new technologies including cloud computing to provide greater computing power, information sharing, and increased capabilities.

Cloud

Cloud computing leverages shared resources and economies of scale, analogous to an electric utility, delivering powerful computing and massive storage on demand. Cloud computing enables companies to consume a compute resource, such as a virtual machine (VM), storage or an application as a service rather than having to build and maintain comput-

ing infrastructures in house. Companies only pay for what they need, transforming traditional capital expenditure (CAPEX) of investing in dedicated hardware into an operating expenditure (OPEX) where you “pay as you go” or pay for use. Another advantage is that cloud computing enables users to focus on projects instead of infrastructure and software administration details.

Cloud computing traces its origins back to the 1960s, when the computer industry recognized the potential benefits of delivering computing as a service or as a utility. The problem was, the technology at the time lacked performance and reliability to be successful. This included the connectivity standards, bandwidth, database standards, operating system capabilities, and software standards necessary to implement



computing as a utility. It wasn't until the broad availability of internet bandwidth, in the late 1990s, that computing as a service became practical. In the late 1990s, Salesforce offered one of the first commercially successful implementations of enterprise Software as a Service (SaaS) leveraging cloud computing. This was followed closely by the arrival of Amazon Web Services (AWS) in 2002, offering a range of services, including storage, computation, databases, machine learning, and more. Since then Microsoft Azure, Google Cloud Platform and other providers have joined AWS in providing cloud-based services to individuals, small businesses and global enterprises.

Cloud computing has become practical for wide range of applications including SCADA with higher bandwidth communications available, Internet infrastructure, and standards such as MQTT (Message Queuing Telemetry Transport), AMQP (Advanced Message Queuing Protocol), and OPC UA

Cloud Advantages

Cloud computing has a number of advantages including:

Self-service provisioning: End users can spin up compute resources for almost any type of workload on demand. This eliminates the traditional need for IT administrators to provision and manage compute resources.

Elasticity: Companies can scale up as computing needs increase and scale down again as demands decrease. This eliminates the need for massive investments in local infrastructure, which may or may not remain active.

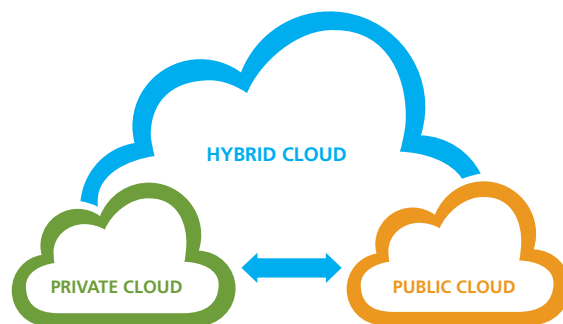
Pay per use: Compute resources are measured at a granular level, enabling users to pay only for the resources and workloads they use.

Workload resilience: Cloud service providers can provide redundant resources to ensure resilient stor-

age and to keep users' important workloads running across multiple global regions.

Cloud computing deployment models

In general discussion cloud computing is assumed to be off-site, but there are number of options users can deploy based on requirements. Cloud computing services can be private, public or hybrid.



Public

In a public cloud model, a third-party cloud service provider delivers the cloud service over the internet. Public cloud services are sold on demand, typically by the minute or hour, though long-term commitments are available for many services. Customers only pay for the CPU cycles, storage or bandwidth they consume. Leading public cloud service providers include Amazon Web Services (AWS), Microsoft Azure, IBM and Google Cloud Platform. Public cloud computing also lends itself well to big data processing, which demands enormous compute resources for relatively short durations. Cloud providers have responded with big data services, including Google Big Query, for large-scale data warehousing and Microsoft Azure Data Lake Analytics for processing huge data sets.

Another crop of emerging cloud technologies and services relates to artificial intelligence (AI) and machine learning. These technologies build machine understanding, enable systems to mimic human



understanding and respond to changes in data to benefit the business. Amazon Machine Learning, Amazon Polly (text to speech), and Google Cloud Machine Learning Engine are examples of these services.

Private

Private cloud services are delivered from a business's data center to internal users. This model offers the versatility and convenience of the cloud, while preserving the management, control and security common to local data centers. Internal users may or may not be billed for services through IT chargeback.

Hybrid

A hybrid cloud is a combination of public cloud services and an on-premises private cloud, with orchestration and automation between the two. Companies can run mission-critical workloads or sensitive applications on the private cloud and use the public cloud to handle workload bursts or spikes in demand. The goal of a hybrid cloud is to create a unified, automated, scalable environment that takes advantage of all that a public cloud infrastructure can provide, while still maintaining control over mission-critical data.

Cloud Analytics & Machine Learning

Available applications hosted by cloud services provide the platform to do the advanced analytics which require significant computing. A great example of a tool that can be used is Microsoft Azure Machine Learning. With an integrated, drag-and-drop development environment, it enables application and

process engineers to create analytics with a library of sample experiments and sophisticated algorithms from Microsoft Research, plus data flow graphs to define relationships. This is a powerful tool to mine data and create optimizations, predictions, and tune operations. Azure Machine Learning reminds me of Visual



Basic that demystified programming and enabled a wide base of users to create solutions tailored to their needs. Potential users can try AzureML for free.


Fog Computing

Another intriguing recent development is Fog Computing. This is a distributed computing model that provides data, compute, storage and application services closer to the edge of the network running in network routers and Edge computers. These work in concert with cloud computing services, but provide a level of local operation for performance and reliability. For example, the story and data can be time tagged, collected and stored locally in a buffer to ensure no loss of data if there is temporary interruption in communications to the cloud.

Lifecycle Cost Advantage

Cloud computing can eliminate a large number of the PCs that may be required in a plant to perform SCADA functions and instead enable simple use of a web portal to receive alarms, access information, adjust parameters, generate reports, view dashboards, and perform root cause analysis.

Constant software upgrades and patches are never-ending ongoing costs to maintain PC software applications, but may be dramatically simplified through use of cloud computing. Many times,



software updates on plant floor PC are delayed for long periods of times, and in many cases this creates systems availability and cybersecurity risks. Cloud software application maintenance is more efficient and thus, also frees local application and process engineering talent at manufacturing and production plants to focus on higher payoff tasks.

Reliability

The large number of aging PCs in a plant can pose significant reliability issues that can unexpectedly impact system availability. Cloud solutions accessed through browsers simplify these systems making them less prone to problems and improve uptime.

Cloud Computing Constraints

Cloud computing does have some constraints and risks that need to be considered.

Communications

The most obvious constraint is the dependency on persistent high-speed communications in order that the servers can interact with the manufacturing facility. This limits the use to functions that can live with interruptions. Manufacturing automation processes that rely on tightly-coupled, high-availability systems cannot risk the loss of communications with cloud computing servers. In this way, companies that store historic data and perform analysis for functions such as predictive maintenance and macro level process optimization can benefit

from cloud computing. That being said, I am always amazed at the speed in which Google returns answers. For example, I did a search for “enthalpy” and it returned results in 280 milliseconds.

Cyber Security Risk

Cloud vendors are working hard to protect data but sending information to outside sources has inherent risks. Users do well to carefully research and understand cloud provider safeguards to protect users’ information. Reputable cloud service providers are well managed with secure sites. Another factor to consider is that studies of shown that computer resources on plant and production sites have a history of cybersecurity issues, and are caused many times by internal people, outside contractors, and system integrators making mistakes or inadvertently bringing viruses into the system. The user ultimately has to make a risk assessment based on these and other factors.

Cloud Computing: A Beneficial Automation Tool

Cloud computing is another automation tool that, properly used, can offer significant benefits in terms of efficiency, scalability, speed and cost certainty. The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them. The cloud aims to cut costs, and helps the users focus on their core task instead of being impeded by IT obstacles.

Experion® Elevate enables visibility to production gas wells in record time



Overview

In November 2016, a growing Canadian oil and gas exploration company acquired new gas field assets in Northern Alberta with approximately 350 producing wells, three gas plants and 720km of pipeline along with a future inventory of approximately 2,147 drilling locations. The existing communication infrastructure for the gas wells was not able to be utilized immediately, nor did it fit the company's direction of being a low-cost producer with the flexibility required to adapt to a changing landscape. Because of a slight change in the closing of the asset purchase, the production wells in this system needed to be transitioned to the new owner and visible to their management and field operations in a very short time-period: approximately 1 month. To accomplish this the company was looking for a vendor with deep SCADA knowledge, proven SCADA solutions


and more importantly, a cloud-based system which would allow them the flexibility, speed of implementation & change and a low-cost approach required by the company moving forward.

The Honeywell sales team demonstrated that we would meet their requirements and secured the order in a very short period. Our project team then successfully completed the configuration of the system on schedule and commissioned the gas wells with the customer much to the customer's satisfaction. The first few wells of the project were online within 2 weeks of the purchase order.

Project Highlights

Solution

The Experion® Elevate solution fit the customer's requirement of desiring to move towards a subscription-style model for the SCADA system to offload some of the higher up-front and long-term costs typically seen with traditional SCADA system solutions. This was heavily influenced by the company's desire to be one of the lowest cost producers in their region as well as allowing them to stay flexible if assets needed to change. Large, CAPEX-style projects would require them to incur more debt upfront than they desired. The subscription approach for the solution based on system size (price per well, equipment, and other factors) and usage allows them to have more predictable costs month over month, yet supports all the features required by a traditional SCADA system.



“ Our project team then successfully completed the configuration of the system on schedule and commissioned the gas wells with the customer much to the customer’s satisfaction. The first few wells of the project were online within 2 weeks of the purchase order. ”

Honeywell provisioned and configured the Experion Elevate solution for communications to both Emerson (previously Fisher) ROC and (previously Daniel) Floboss electronic flow meters (EFMs). The data collected from these flow computers is comprised of real-time and historical data. This covers two needs: instantaneous data for decision making by field operators, and archived historical data from each flow computer for regulatory and production volume reporting to Canadian governmental agencies. Both the real-time data and historical data are stored within the Experion Elevate system. To improve access to the data, a custom interface was developed to transfer this historical production information into the customer’s existing production accounting system.

Communication & Clients

The customer did not have an existing communication infrastructure which could be tapped into to bring the newly acquired gas wells online. To communicate with the remote gas wells in the field,

a couple of similar architectures were created utilizing digital cellular networks to provide the primary backbone. These areas then had a combination of traditional radio components (900MHz) and some cell-connected meters directly.

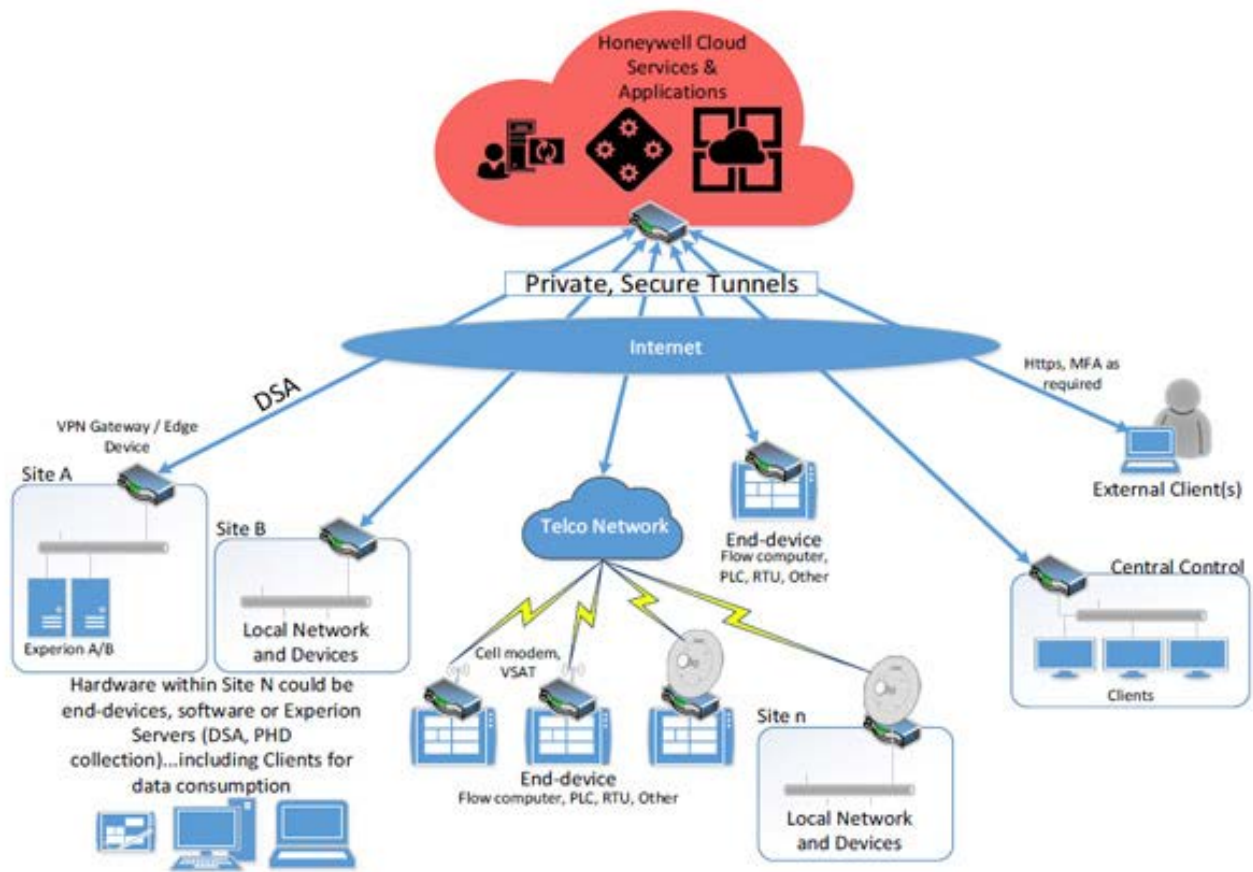
The end-users also required a few different ways to be connected to their solutions. To accomplish this, the Experion Elevate primary client application was built with Experion® Station and delivered via a browser-implemented environment, allowing the end-user to immediately take advantage of the Station client delivered to their full desktop or to a mobile tablet (iPad). The web-based nature of our Station client allows for adaptation to differing resolutions and screen sizes without the need for any HMI conversion.

Along with that access, Experion® Alarm Pager was used for simple alarming and event notifications for the field operators, 24x7.

A full-featured, truly mobile application (iPhone, Android) for Experion Elevate is currently being tested by Honeywell and the customer with release to the customer planned for Q4 2017. This application will work in conjunction with Honeywell Pulse in future releases as well.

Security

With any web-based environment, cyber-security is of utmost importance to the ongoing success of the project. This presents continual challenges for any solution to keep up with. The Honeywell global security group & IT have developed a solution for Experion Elevate allowing the customer to see and discuss options that met their internal security requirements moving forward. Honeywell helped to scope and provision required firewalls and virtual private network (VPN) gateways to fit into the system at key transition locations. These provide secure, private and encrypted data pathways from the field to the Experion Elevate system.



Challenges Faced and Overcome

Meeting the customer's aggressive schedule was one of the largest challenges in this project. Honeywell's ability to deliver a working SCADA solution on this aggressive schedule turned out to be one of the most key success factors for the project and moving forward to future projects with the customer. The original meter templates and communication infrastructure (working with the customer and communications providers) were developed and delivered within 2 weeks from the project start. This allowed the customer to begin monitoring and operating their new assets much sooner than was originally planned. This also meant the customer can discover field issues with the wells quickly, flow computers and communications which were not known at the time of purchase. The quicker these were resolved

the quicker they could increase their production and efficiency.

To date the solution has performed with an approximate 99.99% uptime of the Experion Elevate servers and virtual network.

The customer has expressed delight with the Experion Elevate product and working with the Honeywell team. They are currently discussing several expansion opportunities with Honeywell which would bring in additional wells and incorporate on-site Experion solutions (manned compressor stations) with Experion Elevate. The long-term goal is for approximately 1,800 wells and numerous compressor stations and processing facilities into the Honeywell Experion ecosystem.

Experion[®] Elevate

Technology Elevated to the Cloud
Grounded by Honeywell



Benefits

SCADA delivered as a service greatly reduces on-premises physical footprint, hardware, software, and maintenance.



Predictable costs



Easy upgrades



Continual support



Ease of implementation

We Give You Options

No matter the size of your system or deployment of SCADA, Honeywell delivers flexible and scalable options that are right for you.

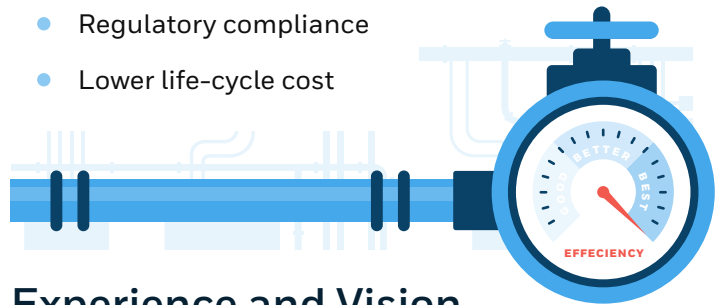
- On- or off-premises combinations
- Subscription-based
- Application-specific by industry
- High-availability options
- Entire suite of solutions available



Operational Efficiency and Agility

Simplify your operations with a solution that brings you business agility and increased operational efficiency.

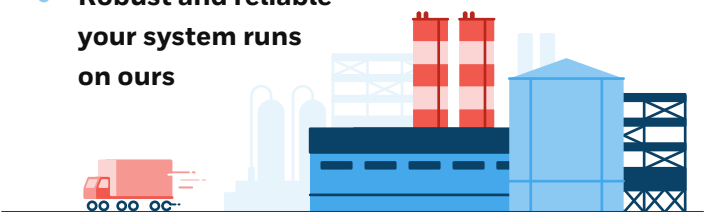
- Latest software and features
- Cyber secure access and collaboration anywhere
- Less on-site support and skills maintenance needed
- Lower cost of entry: OPEX potential
- Regulatory compliance
- Lower life-cycle cost



Experience and Vision

Honeywell invents and manufactures technologies that address some of the world's most critical challenges.

- Transforming data into wisdom
- **4,000 skids, 3,000 terminals, and 400 pipeline projects** delivered to date
- Delivering the best global resources locally
- **Robust and reliable—your system runs on ours**





Securing SCADA in the Cloud

The Best of Both Worlds: Flexible and Secure

Abstract

Cloud-based solutions for SCADA applications offer significant benefits in terms of efficiency, scalability, speed and cost certainty. For many industrial operators, however, the benefits are left unexplored due to fears over the risks of cyber security.

These are real, and the growth of the Industrial Internet of Things is expanding the attack surface for malicious actors. Experience has already shown significant damage can result from attacks on industrial control systems.

It is important to understand this risk exists regardless of where the solution is located. Whether it is a public or private data center – or deep within your plant location – you still need to provide physical security (including from the use of removable storage devices), power and cooling resiliency, and cyber security through firewalls, and patching of OS and application vulnerabilities. The question becomes: Who can best do this and where is the best place to do this?



This paper proposes one solution to do so: Centralizing security within a large centrally located datacenter with great communications connectivity; using a mix of proven technologies designed from scratch to work together is a great start. Add another layer of robust firewall security with intrusion detection and active monitoring and you're getting close. Even better if you can get your chosen SCADA software developer (the company who wrote the application) to take complete responsibility for keeping it operational – including OS and application patching. This solution enables security to be tightly monitored, controlled and enforced with minimum burden and risk to your business. As a bonus, it also offers the best possible performance for geographically dispersed assets.

With such a solution, industrial operators can enjoy the benefits of Cloud-based SCADA with improved cyber security.

Background

The benefits of SCADA in the cloud offers the potential for much greater flexibility, scalability and certainty. It promises the ability to massively reduce capital expenditure, provide predictable costs, accelerate implementation, and quickly accommodate changes when adding or altering assets. As a more efficient model of deployment, it significantly reduces barriers to entry across many industries.

As Vimal Kapur, HPS president, put it during his 2017 keynote speech at the Honeywell Users Group last year: “With cloud-based SCADA, you don't have to set up a control center or backup center. You can leverage the cloud infrastructure from your service provider. Eight to 10 months for a SCADA project can be reduced to a few weeks. You move from a capital model to an OPEX model. You don't have to buy servers. You start with fewer assets. If you want to add more assets, you add them; you want to delete, you delete. Software versions are always kept current.”

“ As control functions are automated, the range of potential targets for an attack increases. Increasing connectivity, with more and more devices and systems networked in the Internet of Things (IIoT), has brought many benefits, but it has also brought cybersecurity concerns. ”

These benefits are increasingly being proven in practice. Honeywell recently published details of a project for a crude oil and natural gas exploration and production company in Canada, where it used off-site SCADA to bring over 300 wells online within a month of signing the order. The technology is not only being used across upstream and midstream oil and gas applications, however; it is also employed in a range of industries, including water and wastewater; power, utilities and renewables, such as solar and wind farms; manufacturing; mining and minerals; and in data centers.

Security issues are key to the design

SCADA in the cloud can offer a reliable and a secure solution. On-site resources and expertise can be supplemented by remote support, continual monitoring and automatic updates provided by the service provider. In many ways the design of communications is similar to topics considered in earlier SCADA



systems, however now it is more important to have a solid cyber secure design.

The issue of cybersecurity is, of course, key in such systems especially at a time of growing threats to industrial control systems. The move to digitization in industrial control systems has plainly increased the cyber risks. Manually operated equipment has one upside: it can't be hacked. As control functions are automated, the range of potential targets for an attack increases. Increasing connectivity, with more and more devices and systems networked in the Internet of Things (IIoT), has brought many benefits, but it has also brought cybersecurity concerns.

It is not just the “attack surface” or number of the vulnerabilities that has grown, but also the potential consequences of a cybersecurity breach. Increased regulatory expectations mean that businesses risk serious reputational damage and costs (in terms of regulatory penalties) even without a successful breach. Those that are successful, meanwhile, have demonstrated that the risks are far from theoretical:

- The Sandworm hackers caused blackouts for more than half a million people in the Ukraine in 2016 – after targeting the US.

- The Shamoon virus crippled tens of thousands of computers at Middle Eastern energy companies in 2012, and resurfaced four years later.
- The WannaCry ransomware spread across the globe last year, and affected more than a third of the UK's NHS trusts – and not just hospital computer systems, but medical equipment such as MRI scanners and blood testing devices as well.


These are just some of the most high-profile examples. More widely, more than half of industrial facilities have experienced some form of cybersecurity incident, according to a Honeywell survey last year, and three quarters expect an attack on their industrial control system, according to Kaspersky Lab.

A pressing concern

Both the number and range of attacks is growing as the threat evolves. Among the most worrying developments is the specific targeting of safety systems. In December 2017, hackers invaded the safety system of a critical infrastructure facility – described as a “watershed” moment in industrial cybersecurity. However, it actually followed an attack on the safety systems at a middle-eastern petroleum company.

In addressing these risks, businesses are hampered by a number of factors. The first is general skills shortages as a result of a rapidly retiring workforce, and specifically a lack of cyber skills. Petroplan's Talent Insight Index 2017 found more than one in five in the oil, gas and energy sectors saying industry lacked the right talent for growth, and more than a third said they needed greater IT skills as the reliance on digitization and big data grew.

Within businesses, meanwhile, operational silos persist – between sites, between businesses within groups and, perhaps most significantly, between IT



and operational technology (OT) staff – despite the technological convergence.

The result is that ownership of and responsibility for these risks is unclear. This is particularly significant since the traditional approaches of IT and OT are very different. Specifically, availability in the operational space is a greater priority, being essential in many cases to safety. Appropriately, security solutions for IT and OT therefore differ substantially. Notwithstanding this, there is, in any case, still a significant lack of clarity over what is appropriate. With little in the way of consistent cybersecurity standards, we don't yet have agreement on what good looks like.

A Challenge, Not A Deal-Breaker

There are, in fact, two key dangers in terms of cybersecurity when it comes to SCADA in the cloud. The first is that they are ignored or inadequately addressed. Unsecured connections through satellite or radio communication provide hackers with an opportunity to target the remote site and hack into the cloud or SCADA system. Every unsecured valve site, for example, becomes a significant source of vulnerability.

“ Security is not only about keeping external threats out of your business, it is about making sure the information can be trusted while empowering the authorized users to improve company performance. ”

The second danger, however, is that the risks are overstated to the extent that businesses are put off from cloud deployment. That would not only mean they miss out on the benefits SCADA in the cloud can bring in terms of efficiency, which would have a potentially bigger cumulative impact on the industry over the long-term than any of the cyber-attacks we've actually seen.

That's clear when you look at attack vectors – how breaches occur, and malware or hackers actually get in. In some cases, that's the result of unsecured points of connectivity to the industrial control system (ICS) environment, with multiple equipment and system vendors given access. Elsewhere it's the result of either external or business network security being compromised. Often, however, it's employees and contractors bringing in the threat, whether through falling victim to phishing or spear phishing attacks or through their laptops, phones, smart watches, IoT devices, or removable media. The last remains a pernicious and pervasive source of vulnerability.

An issue of access

It is worth reminding ourselves that SCADA is used to monitor and sometimes control geographically distributed assets. Many of the SCADA systems being designed today are focused on collecting performance and diagnostics data for analytics to achieve an always up-to-date visualization of the company's performance metrics while giving a much smaller group of people the ability to see leading indicators of future problems and take action now to avoid shutdowns later.

Figure 1

The first level of cybersecurity is simply to limit write access (control) through the application's configuration, to those who need control functionality and only with appropriate authentication. Whether the system is on the customer's site or within a datacen-

ter, this simple role based criteria should be used to significantly improve cybersecurity. This is strengthened by the use of Two or Multi-Factor Authentication where the most common approach is to provide a code to the user's phone (text or dedicated app) to provide a second level and one-time-use code. This nearly eliminates the use of someone else's password to gain access. Security is important when looking at SCADA in the cloud, but it is far from being an insurmountable challenge. Most of these concerns are an issue regardless of where the software is running. The central problem to overcome for securing offsite SCADA solutions is the lack of centralization. Businesses are left trying to secure multiple access points (Figure 1) used by remote employees, contractors,

customers and the vendors of control systems and third-party equipment and software (where they are given remote connectivity for the purposes of upgrades, patching, monitoring or support).

The numbers of these access points and the lack of central oversight and control lead to a variety of problems:

- Only partial data is available on assets and events
- There is no proper hardening
- There is no proper monitoring, nor governance
- There is no proper planning and accountability around cybersecurity.

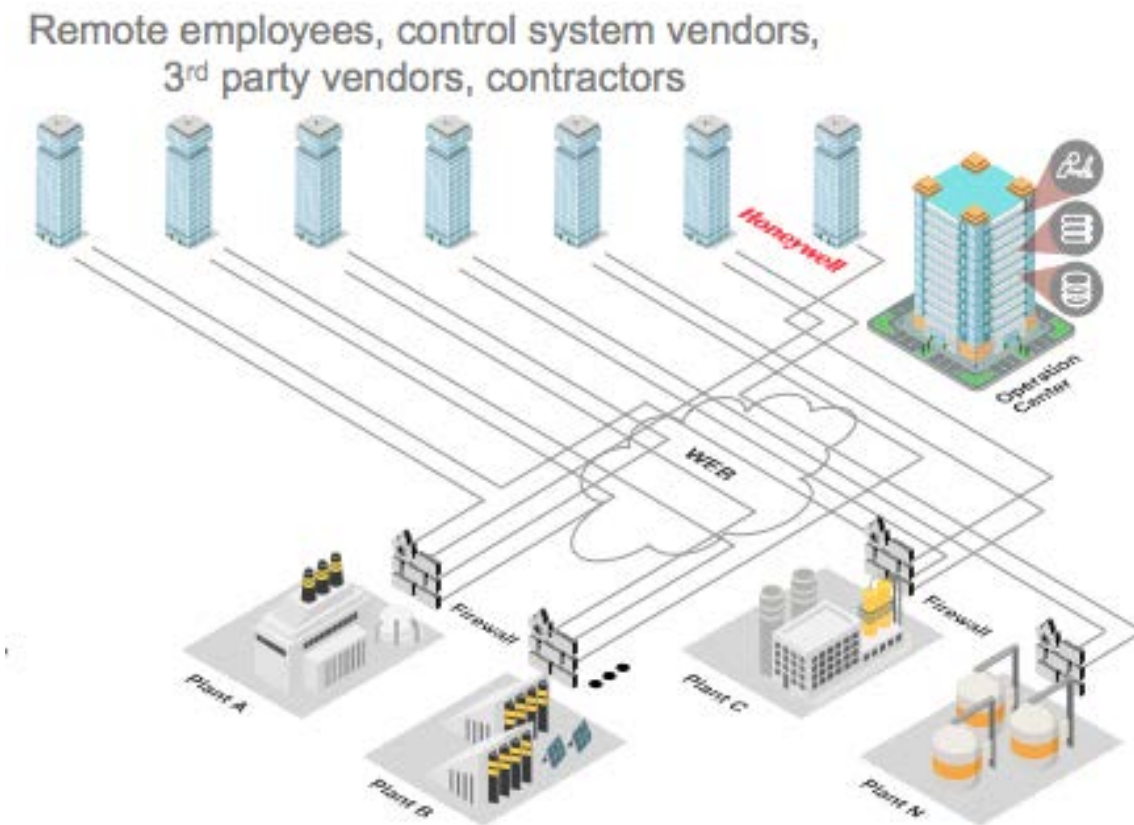


Figure 1 Multiple access points lead to multiple vulnerabilities



Businesses are left to simply trust that each of those making and managing the connection through these access points is doing so in a secure way. That's an unwise assumption.

This problem is only going to become more pronounced as the number of connected IIoT devices grows. Furthermore, alongside this, there is an increasing need for advanced and big data analytics to get value from the massive amounts of data being generated and transforming it into actionable intelligence.

These analytics capabilities will be either at the HQ or cloud-based, requiring a secure data transfer tunnel.

A Proposed Solution

SCADA is by definition data acquisition from dispersed assets. It makes sense to centralize your processing and data storage in the center of the assets (from a communications time standpoint) to minimize delays and communications costs. If you're monitoring assets within a single facility, you'll get your best performance at the Ethernet switch shared by most or all of the devices.

If you have many sites with great distances between them, you'll want to take a closer look at where the network center is located. In most cases, you'll find communications are using IP or Internet Protocol technologies with very fast connections to large data centers. Today's data centers are the communications hubs of our society and already provide the physical security, IT services, and cybersecurity required by today's internet applications.

A Centralized Approach

The key to SCADA in the cloud is security in the cloud – centralizing security through a cloud-based Security Center and Communication Server.

This Security Center can handle the authentication of connections, ensuring these are valid before allowing access to the Communication server. All communications from these sites pass through a secure tunnel using Transport Layer Security (TLS) encryption, and a single firewall rule can be enforced for all remote connections. This provides a distributed architecture with secure tunnels from operations to remote sites.

Traffic from the plants or sites is all channeled through the secure tunnel, while the Communication Server is protected by a firewall. If it is necessary to push down a patch or update, however, the secure connection can also be used to give access to technicians remotely.

This centralized approach to security provides operations with the ability to define, automate and monitor security policies across the SCADA environment, providing increased visibility, reliability and compliance. The business can centrally define plant-wide policies, confidently deploy them, and automate their execution and monitoring. It ensures security of all remote field assets from a single operations center.

Any serious application needing real security will start there, but then add additional layers of security, commonly referred to as defense-in-depth methodology (Figure 2). These layers are meant to slow down attacks to give your intrusion detection software time to identify the threat and trace it back to its source. Using software applications which were designed to work together, even if they are from multiple vendors, helps to avoid surprises later. Then, you add active monitoring of the security solution from a dedicated firewall management team and proactive patching of operating systems and applications. The best scenario is when you can get the software developer to take responsibility for the complete solution.

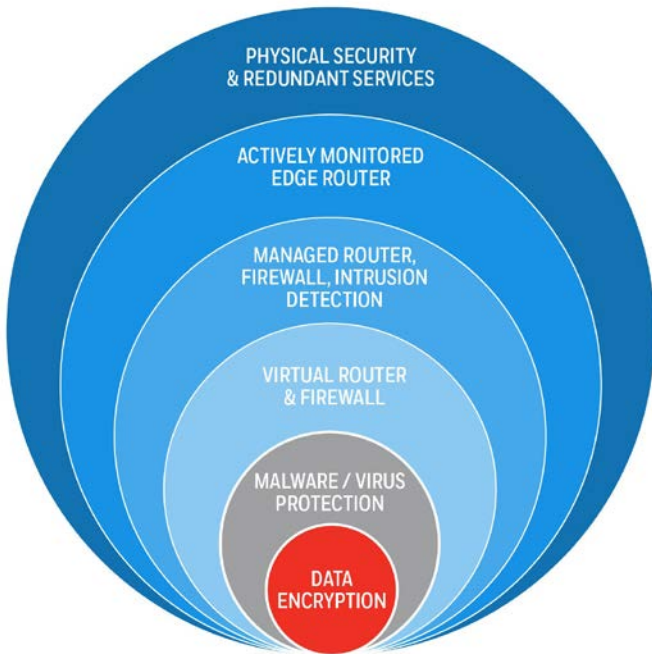


Figure 2 *Defense-in-depth Security*

From the Edge to the Center

The next step is to secure communications between edge devices to the data center. This all starts with the edge device. This is usually an RTU, PLC, or in some cases, a computer. Ideally, you start with an edge device certified to ISA Secure Level 2 which generally includes secure boot, authentication, and data encryption (Figure 3). Compliance with the standard is overseen by the ISASecure program, run by industry consortium ISA Security Compliance Institute (ISCI). An easy to use control software using programming languages like IEC 61131- can be



used to sift through all the data and determine what’s important enough to send to “HQ”. One simple example is that you may be reading all the diagnostics data for all your local devices but only send data for devices which are outside of normal operational parameters.

Reliability can be enhanced using local data storage, so nothing gets lost if your communications link is lost. This is extremely important when using cellular, radio, or satellite communications, but we all experience wired communication losses as well. It is best to store at least 8 hours of data onsite before it is overwritten by new data. Modern RTUs and PLCs should allow for up to 32GB of data minimum, usually accomplished with the same inexpensive SD card storage used in our digital cameras.

Secure communications can be accomplished with Virtual Private Network (VPN) technology and today’s more secure protocols like DNP3, IEC 61850, and OPC UA, which is the latest and appears to offer the most security and functionality of the group.

AMQP and MQTT are transport-focused technologies and can be added to these protocols to go from point-to-point communications to a publish-subscription (pub-sub) model, where one stream of data can be made available to multiple users.

Most solutions today will use point-to-point communications to load all the data into a large database where it can be organized and provide highly efficient historical trends or views of data originating from multiple locations. This centralized approach would then have data mirroring and automated backup processes to secure the data; usually across multiple sites with disaster recovery functionality.

Securely Disseminating Actionable Information

Once you get your data into the cloud, you want applications that turn the raw data into something you can use to improve your business. This typically



means the flexibility and power to graphically bring your attention to abnormal trends or events. Different users need different applications or views of the information as those users are often using data for very different purposes. The field technician is trying to get equipment back into operation; the operator is looking to keep equipment running at peak performance; while the site manager wants to maximize his overall production. An executive may want to be able to reference a dashboard with enterprise-wide production and financial implications.

Security is not only about keeping external threats out of your business, it is about making sure the information can be trusted while empowering the authorized users to improve company performance. The next step is to secure the more valuable information flowing between the data center and those end users who may be driving between sites, managing operations of multiple sites from a Remote Operations Center, working from their office, or even

from home using their phone or tablet to assess the current situation.

This is typically done with encrypted tunnels or VPN connectivity. This proven technology is used for our corporate email systems and banking transactions. The best part is it allows for a wide variety of devices with consistent usability.

As mentioned earlier, control or write functionality can be limited to specific users who have been trained to understand what their actions on the keyboard can do at a site thousands of miles away. It's a great productivity tool to greatly reduce travel to distant sites. It enables collaboration with expert users to fully understand unusual situations. The system protects us from ourselves by requiring user authentication. A user name and password may be enough for low level read-only access but Multi-Factor Authentication may be required for write control of remote sites or sensitive financial data.

Framework Core	
Functions	Categories, Subcategories, Informative References
Identify	<ul style="list-style-type: none"> Automated asset discovery and inventory Policy management
Protect	<ul style="list-style-type: none"> Automated patch + AM delivery Secure remote access & data transfer
Detect	<ul style="list-style-type: none"> Monitor and log collection Scan ports & services against whitelists/blacklists Compliance reporting
Respond	<ul style="list-style-type: none"> Secure remote access by Cybersecurity experts
Recover	<ul style="list-style-type: none"> Multi-site file transfer infrastructure for backup/restore

Table 1 Compliance with NIST Cybersecurity Framework



Summary

Combined with a top-down security management platform, such as Honeywell's ICS shield, this architecture can be used to deliver robust ICS security following the NIST Cybersecurity Framework.

This voluntary framework defines industry standards and best practices to help organizations manage cybersecurity risks. Combining centralized control with the security management platform gives businesses the ability to consistently meet these standards across sites (Table 1).

Existing manual security processes, such as patching do not scale well; SCADA in the cloud can centralize and automate these, while bringing consistency, visibility and control to cyber security across the enterprise.

SCADA in the cloud offers significant benefits, but concerns over security could stop these from being realized. They shouldn't. With a suitable architecture and security, businesses can enjoy the benefits of cloud deployment while not just maintaining their security, but actually enhancing it.

Experion® is a trademark of Honeywell International Inc.
Other brand or product names are trademarks of their respective owners.