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.
# Table of Contents

Abstract ................................................................................................................................. 2
Background ............................................................................................................................. 4
Security issues are key to the design .................................................................................... 4
A Challenge, Not A Deal-Breaker ....................................................................................... 5
An issue of access .................................................................................................................. 5
A pressing concern ............................................................................................................... 5
A Proposed Solution ............................................................................................................ 6
A Centralized Approach ...................................................................................................... 6
Securely Disseminating Actionable Information .................................................................. 7
From the Edge to the Center ............................................................................................... 7
Summary ............................................................................................................................... 8
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.”

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.

https://www.automationworld.com/scalable-current-real-time-scada-cloud
https://www.digitalhealth.net/2017/10/wannacry-impact-on-nhs-considerably-larger-than-previously-suggested/
https://www.securityweek.com/industrial-firms-slow-adopt-cybersecurity-measures-honeywell
https://go.kaspersky.com/rs/802-IJN-240/images/1C5%20WHITE%20PAPER.pdf
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.

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: Multiple access points lead to multiple vulnerabilities

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 datacenter, 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.

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.
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.
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).

Table 1: Compliance with NIST Cybersecurity Framework

<table>
<thead>
<tr>
<th>Framework Core</th>
<th>Functions</th>
<th>Categories, Subcategories, Information References</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Identity</td>
<td>Automated asset discovery and inventory</td>
</tr>
<tr>
<td></td>
<td>Protect</td>
<td>Automated patch &amp; AIV delivery, Secure remote access &amp; data transfer</td>
</tr>
<tr>
<td></td>
<td>Detect</td>
<td>Monitor &amp; log collection, Start ports &amp; services against vulnerabilities &amp; attacks, Compliance reporting</td>
</tr>
<tr>
<td></td>
<td>Recover</td>
<td>Secure remote access by Cybersecurity experts</td>
</tr>
<tr>
<td></td>
<td>Reconcile</td>
<td>Multiple file transfer &amp; infrastructure failure restore</td>
</tr>
</tbody>
</table>

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.

For More Information

Learn more about Honeywell’s SCADA solutions and SCADA-as-a-service cloud infrastructure, visit http://www.honeywellprocess.com/Elevate or contact your Honeywell account manager.