MAPLE SYSTEMS' SCADA & HMI GUIDE

Whether you are looking for remote access at the machine level, seeing/acquiring additional information at a supervisory station, or communicating data outside of your factory local network, we'll discuss common topic every controls' engineer needs to consider when designing a SCADA system.

Contents

Maple Systems INC.

Four SCADA considerations for manufacturers

Considerations for supervisory control and data acquisition (SCADA) and human-machine interface (HMI) systems include situational awareness, an emphasis on cloud and mobile delivery and more.

(This article is originally from Control Engineering eBook, SCADA & HMI Spring Edition 2021, and adapted for use in this SCADA & HMI guide)

Supervisory control and data acquisition (SCADA) and human-machine interface (HMI) systems have great potential for manufacturers. However, there are many details that might be missed that could cause major headaches and reduce their overall effectiveness. Consider these four key elements when using them.

1. Pay attention to situational awareness

Problems often occur when users fail to specify and distinguish between the behavior and interaction of their user interface – for example how a window is maximized or resized across multiple monitors, or how zooming and multi-touch, panning are performed. Realistically, a user's acceptance of the "look and feel" of a particular product will be based on a mixture of hands-on evaluation and conversations with existing users. So, organizations must ensure that all of the features required – including a graphics library, automation objects, faceplates, element style, and themes – exist out of the box.

2. Future-proof design for scalability and total cost of ownership (TCO)

Unlimited input/output (I/O) licensing can help organizations scale for future production growth. However, they must ensure that their industrial systems are built to handle it. This can be achieved by ensuring that the SCADA system has been thoroughly tested to handle a large number of I/O points to avoid slow response times and other issues caused by a SCADA system not designed for such use. The TCO is too often only considered at the time the project is designed and implemented. The real cost, however, relates to how long the project can continue to provide a return on investment while continuing to enable the manufacturing facility to be competitive. Built into this calculation is the cost of the 'operational lifetime of a project,' which considers the ability to upgrade and add new functionalities, as well as maintaining the system. Ultimately, it is integral that an organization fully identifies and analyzes what is required of its own internal operations as this will need to be aligned to the company's operations, as well as its products and service offering.

3. Pay attention to how the product is configured

Pre-configured demo systems can be vaporware. However, a system should not be judged on this. Instead, it should be judged on its usability and day-to-day functionality; particularly the time it takes to perform standard day-to-day tasks – both as an administrator and an operator. Organizations should also question whether various personas with varying technical skill-sets are able to perform configuration changes. A surprising number of products require the same information to be entered in multiple places. For example, a tag name might need to be manually typed as part of the RTU/PLC program and the same is also true for a database configuration, as part of a report configuration. This will result in a system that is slow and difficult to configure, and one that is also likely to contain many errors.

Our FREE HMI configuration software has graphic libraries, objects, and elements included. Read more about our HMI software and the EBPro programming environment. Access documentation and resources, sample projects, quick-start guides, and more.

4. Think cloud first and mobile delivery

SCADA is an integral part of a business, not just its operations. The flow of data from the control room to the board room must be seamless. In the past, supervisory control and manufacturing information systems have not been integrated. This is changing and companies are realizing both of these investments only achieve their full potential when they are capable of seamlessly working together. Likewise, native cloud and web technologies are imperative to harness the domain expertise of multiple engineering centers. Fundamental to a successful project implementation is the deployment of the best domain experience. It is very often necessary to use several engineering houses to build a total system– but as soon as a company does this, issues of integration, consistency and maintainability come to the forefront. Learn more about how Maple Systems supports the IIoT, including MQTT, OPC UA, and SQL database integration.

Maple Systems has been a proud OEM partner of Aveva Edge 2020, formally Web Studio for over 20 years. Pairing Aveva Edge with our Industrial Panel PCs and Industrial Box PCs creates a scalable, powerful SCADA solutions.

Award-winning AVEVA™ Edge 2020 is a powerful HMI/SCADA software package that enables you to create custom industrial control applications for your unique industry. With easy-to-use commands/tool bars and a Microsoft Windows® environment, AVEVA™ Edge 2020's feature-rich application puts you in the driver's seat of creating your industrial process.

HMI software advancement for IIoT optimization

Unified human-machine interface (HMI) software centralizes device management and machine data, enhancing usefulness and increasing connectivity across the enterprise.*(*

This article is originally from Control Engineering eBook, SCADA & HMI Spring Edition 2021, and adapted for use in this SCADA & HMI guide)

Increasingly connected and higher-performing manufacturing plants require corresponding automation advances. While sensors and programmable logic controllers (PLCs) have become smarter over the last decade, not all human-machine interface (HMI) software experienced the same technological boosts. Now, though, the latest generation of HMI software has many advances including:

Maple Systems HMI configuration software, EBPro, and our HMI with local IO configuration software, MAPware-7000 offer advanced features such as remote access, web server, MQTT, OPC UA, Ignition, SQL integration, and more. And our powerful Windows based software, Aveva Edge that runs on all of our Industrial PC, is a scalable SCADA software.

- **Improved graphical characteristics**
- **Onboard productivity applications**
- **The ability to connect to a wider variety of devices, and**
- **The capability for users to define their own scripts and data pipelines on the HMI's open platforms.**

These advances are optimizing industrial HMIs for use with devices in Industrial Internet of Things (IIoT) applications.

Improved operational technology

Digitalization is no longer a competitive advantage in manufacturing; it is a competitive imperative for profitability, longevity and responsiveness to evolving market trends. Unified HMI software meets these challenges by allowing developers to build sophisticated, responsive, and feature-rich applications suited for the digital age.

This new wave of HMI software, running on dedicated devices or PCs, is more attuned with modern smartphones than with its clunky and antiquated predecessors. Modern unified HMIs ship with preinstalled applications for viewing documents, watching instructional media clips and accessing external web-based systems. Improved multitouch gestures – such as zooming and panning – allow for smooth document navigation and web browsing (Figure 1). Operators can use multitouch swipes to change screens and scroll within lists.

Figure 1: Maple Systems Capacitive HMI devices provide support for multi-touch gesture recognition, Touch gestures can trigger various actions such as change window, set bit, set word, execute macro, popup window, keyboard input, and screen hardcopy. Triggering a sequence of actions using a single gesture is also possible.

Watch our video on our capacitive touchscreen HMI with vibrational feedback, swipe, pan, zoom, and multi-touch features.

Support for native web technologies like HTML5, scalable vector graphics (SVGs) and JavaScript is increasingly common. This functionality gives developers the ability to customize and animate HMIs, and the move from pixel-based to vector-based graphics improves on-screen aesthetics and machine visualization.

Web server capability allows authorized operators to remotely access HMI applications from any device capable of hosting a web browser – such as a laptop, smartphone or tablet – without install apps or plugins. This enables opportunities for collaboration between plant-floor staff and engineers in the office, making it easier for teams to troubleshoot issues.

HMI, IIoT collaboration and connectedness

For small machine shops and international enterprises alike, collaboration is vital to operational improvement. To encourage increased collaboration, unified HMI software supports sharing of screens, tags, alarms and production data among multiple devices on the plant floor, which stores all data at a central location. Modern HMI devices also support data transmission over multiple protocols such as message queuing telemetry transport (MQTT) for cloud connections.

Regardless of the plant layout, it is advantageous for manufacturers to consolidate all production data for analysis and process improvement. In the past, each machine type often required its own third-party driver for data transfer to a central location, but unified HMI software overcomes this time-worn obstacle. Built on platforms such as the .NET programming language, unified

HMI software system connectivity extends beyond plant-based historians to higher level organizational workflows in manufacturing execution and enterprise resource planning systems.

Developers can leverage the integration of unified HMI software with these workflows to define rules and actions for business processes influenced by triggers from production data. It is also possible to monitor production key performance indicators and include this data in business process reporting. By installing optional apps within a unified HMI software environment, operators can receive production-related mobile alerts and notifications via a parallel app installed on their smartphone, smartwatch, or tablet.

Shared software ecosystem

The key to connectivity across the plant is the unified HMI's shared software ecosystem. Shared software means one HMI development and runtime environment is used with all visualization devices – control room computers, smartphones, tablets and panel HMIs. All visualization interfaces share a common library of application objects, SVGs and scripts. Because symbols can be reused across device types, it is no longer necessary to spend time and money developing new graphics as plant production expands and additional visualization devices are brought online (Figure 3).

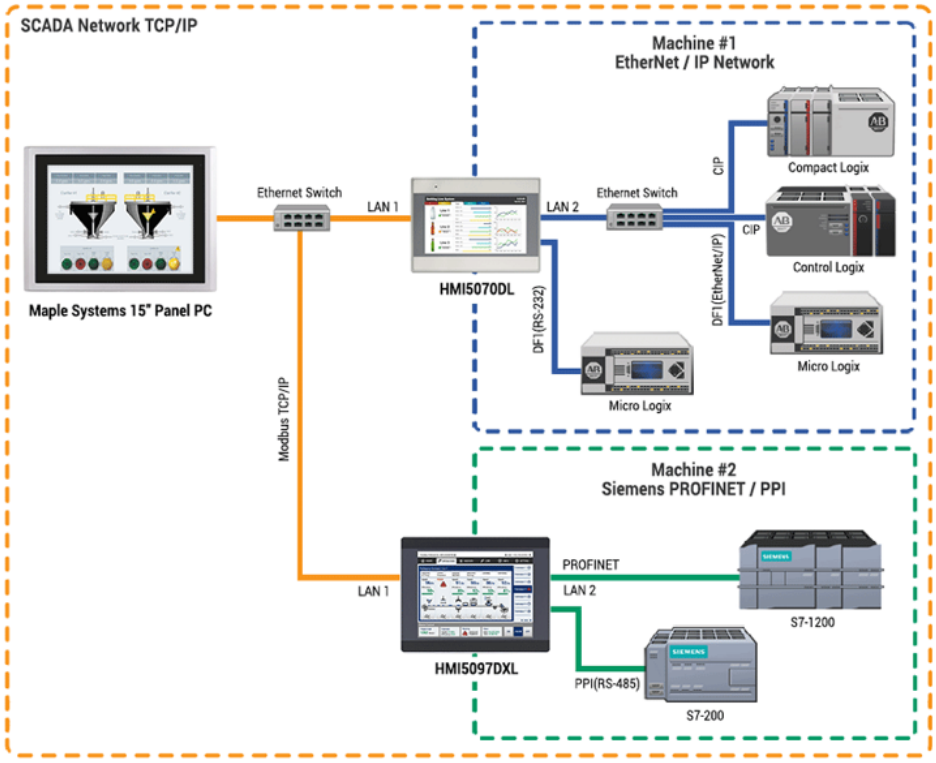


Figure 3: Maple Systems HMI software enables management of numerous devices. Scaling is simple due to a common library of application objects.

Shared software advantages do not stop at the HMI level. Unified HMI software comes with its own suite of apps, which empower plant owners to modularly select and build out their software infrastructure to suit specific company needs. These apps provide business workflow integration, machine-to-machine (M2M) data exchange, data visualization and analysis, central device management, and other functions.

For users, a shared software ecosystem means a similar look and feel across all visualization and control interfaces, including mobile devices. This leads to enhanced operator familiarity and better decision making because less effort is required to understand multiple interfaces, which frees up time to focus on operational improvements. A parallel and intuitive interface across devices also lends itself to less user frustration.

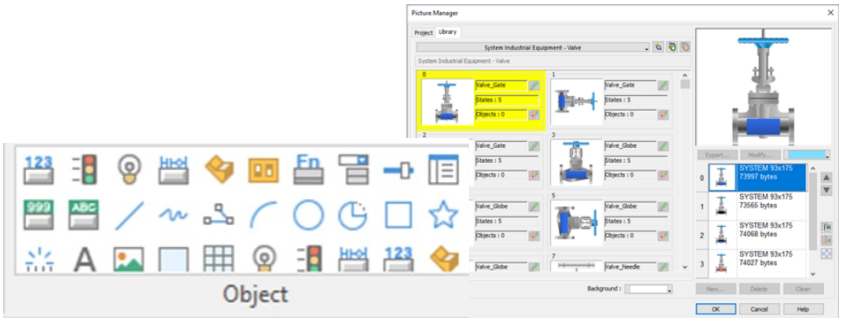
Openness for modern plants

On top of consistency throughout its own software ecosystem, unified HMI software gives users the ability to import custom controls and files. Developers can import objects created with third-party tools into the unified HMI software for deployment in runtime applications. The software's openness also allows for exchange of large amounts of information with databases and other systems through the use of common .NET and C++ frameworks.

Users also can create open application programming interfaces (APIs) for integration with business and production workflows. Machine builders and end users alike can inject their custom programming into the unified HMI software's DNA as open APIs. For example, developers can create comparison reports and debugging traces to catch errors in application code or device configurations before they manifest, reducing commissioning time and mitigating machine malfunction risks.

Application openness delivers the accessibility required to analyze data generated throughout the plant, without creating unnecessary inefficiencies or downtime. Runtime openness provides third-party apps with direct access to HMI runtime tags and custom web controls for increased equipment and workflow flexibility.

Offline data collection tools are natively included for submitting data to a designated server. This allows for exchange of large amounts of information with database systems – as well as sharing screens, tags, event archives, and historical alarms.



Our FREE HMI configuration software, EBPro, comes with stock image libraries to make programming easy.

Security at the core

Gone are the days when security was an afterthought. With breaches picking up in frequency across industry, machine builders and plant owners must treat software security seriously.

Unified HMI software comes with several built-in measures for securing against unauthorized machine access. Unified HMI devices contain separate control panel and runtime layers built on top of the operating system (OS). A system administrator can allow each authenticated user access to one or both layers and also can configure user authorization for OS access. Default applications, user apps and APIs reside on the control panel layer while the runtime layer handles the familiar HMI application for production system control.

An administrator may enable and disable physical ports – USB, Ethernet, and buses – as well as SNMP and transfer protocols. Using central device management, an administrator can create rules for allowing or disallowing certain applications for each device group and manage security patches across all connected devices in the enterprise.

Unlike older HMI software, no third-party central management software is necessary because the same unified HMI software for programming and runtime includes all required tools for central device management. This software also enables device and data integration with other applications. Communication among all devices running unified HMI software is encrypted and HMIs can be configured for automatic system backup to prevent data loss.

Security: 10 ways our HMIs protect your project

In today's IIoT world, security is a top priority. Demands for instantaneous data from all levels of production have put increased pressure on OEMs and systems integrators to provide remote access to the manufacturing plant. Just as important though, is ensuring that the safety of employees and protection of company equipment and intellectual property is not compromised. Maple Systems HMIs provide several layers of security features that keep your control system safe, yet still accessible to personnel located outside the plant.

These and other features can be used to improve operations. For example, a machine builder was struggling to keep up with growing demands from its stakeholders for greater functionality and usability. The manufacturer recently ceased use of legacy HMI products and installed unified HMI software on its machines to deliver greater performance and flexibility.

This empowered the manufacturer to import its own software and applications for maintenance support, and the many native communication protocols made it possible for users to centrally manage their new device alongside existing machines.

HMIs for the future

As an increasing number of smart devices and enterprise-connected software systems are implemented in industrial plants around the world, HMI software technology must keep pace. Unified HMI software delivers modern graphical interface qualities, while enabling connectivity with a multitude of external devices and software systems.

By implementing these advances and continuing to evolve, manufacturers can maintain a competitive edge, increase production output, and improve efficiency.

With over 300 PLC & Controller communication protocols, our HMIs will easily integrate with your preferred PLC brand Including Allen-Bradley, Siemens, Omron, Emerson, GE, Panasonic, and Mitsubishi. Creating a powerful edge gateway at a great price has never been easier.

See the full list of supported controller manufacturers

Parker WATLOW Koyo
YOKOGAWA Allen-Bradley SIEMENS
OMRON ABB MITSUBISHI
Danfoss EMERSON BOSCH
Panasonic YASKAWA BECKHOFF
CROUZET KEYENCE Matsushita
copley controls BALDOR

A Mission Critical Mindset at Any Scale

High Reliability Isn't Just for Large Systems

(This article is originally from Control Engineering eBook, SCADA & HMI Spring Edition 2021, and adapted for use in this SCADA & HMI guide)

Small does not mean unimportant.

For those who don't spend a lot of time hanging from ropes, a carabiner is a simple metal shackle that allows users to connect one thing to another quickly and securely. For example, climbers use them as part of a safety system that includes pitons, harnesses, and rope. As they make their way up a rockface, they hammer in a piton, attach the carabiner and pass through a rope. In this way they can create an extended redundant system that can support multiple people. But at its most simple level, one carabiner must be able to hold one person. It cannot fail. It is mission critical.

Is it the size of the system that dictates its criticality? No, the life of one rock climber is precious. A string of Christmas lights hanging from 100 carabiners is not. In the automation world, many systems that are small in scope can still be critical in nature. The downstream, knock-on effect of a system outage may introduce errors and defects in the items being produced, possibly going unnoticed.

In industrial systems, "mission critical" was traditionally synonymous with big. Mostly because, in the past, the equipment and infrastructure required to harden an industrial system were prohibitively expensive. Instead, smaller utilities and businesses simply learned to live with the consequences of downtime. They worked around the failures in their critical system because, at one time, there was no other choice. However, recent advancements in technology have made the cost of applying mission critical methodologies far more accessible.

In this article, we will focus on supervisory control and data acquisition (SCADA) systems and discuss the factors that keep smaller entities from adopting the kind of zero-downtime principles that have been a standard part of industries such as power generation and pharmaceutical production.

What does "mission critical" actually mean?

Mission critical means, it just has to work. Not just some of the time, but all of the time. Critical can mean different things to different people. Some processes and systems may be able to tolerate some downtime, others cannot. Remember Apollo 13? Having to power down and restart a system to make changes can leave you in an extremely vulnerable position. Will it restart? Will your software crash? There are countless examples in the industry of a simple restart not going as planned, followed by significant downtime.

A mission critical mindset

A mission critical mindset needs to be part of the DNA of an organization. You need to look at all aspects that have an impact on your system. This is typically a drill-down approach. Start at what you are trying to achieve and then drill deeper to see where there are dependencies. As you do this, you can look at the interaction between different parts of your system, large or small. That way you can build a better picture of whatifs. What-if this part of the system fails? What systems would be affected? By working through this process systematically and then reviewing with others in your organization, you are more likely to eliminate blind spots and ensure your system achieves maximum uptime. Reaching this has never been more affordable and achievable.

Underestimating the cost of failure.

Since, for many smaller users, downtime is seen as an unavoidable cost of doing business they don't bother looking closely at what the loss of monitoring, control, and Alarms is already costing them.

Public safety – Loss of alarms and real time data can lead to dangerous spills and leaks that pose immediate and long-term threats to public and staff alike. This is the highest priority of a mission critical system.

Damage to equipment and infrastructure – Set points and alarms play an important role in protecting and extending the life of important industrial assets such as pumps, motors, valves, UV sterilization equipment etc. Alarm notification systems ensure that those alarms reach personnel who can react in a timely manner. No alarms means that an extended power fault could ruin a motor, a jammed tree branch can damage a pump leading to a spill, and a loss of power can destroy a chemical process.

Fines and legal accountability – In addition to the cost of the actual cleanup, there is also the risk of governmental fines which can be in the million of dollars. In the last decade, water and wastewater utilities and the individuals who run them have faced increased legal accountability. Add to that the possibility of civil and class-action lawsuits from those affected by industrial accidents.

Loss of data – Some costs of failure can be harder to quantify. What happens if an historical data server is destroyed? What happens if a loss of communication results in data not being logged? The cost of recovering lost data can be hundreds of times more than the cost of the systems itself. Assuming that there are backups to work from, it is often a long and cumbersome process to manually synchronize secondary computers or backed up databases. As a result, history may be permanently lost, resulting in inaccurate reporting. This may have a knock-on effect, as these reports may be assumed to be correct leading to operational inefficiencies for years.

Loss of production revenue - In simple terms, system downtime leads to production loss. This is compounded if your software application needs to be shut down each time you need to make even a small configuration change. Downtime, even small amounts, add up over time, affecting profitability.

What makes a SCADA system mission critical?

Built in scales better than bolt on – Many software platforms, though sold as a single product, rely on third-party products for core SCADA components such as Historians, alarm notifications, thin clients, and scripting. A common issue with this approach is that, over time, these components work less and less well together increasing the likelihood of downtime or loss of functionality. This is a common issue with third-party alarm notification systems. A single SCADA product ensures that everything works together seamlessly with new software versions. It also eliminates the risk that components are altered or discontinued by their manufacturers. Best of all, a unified approach means, one install, license agreement, training track, and support contract.

System-wide redundancy – Many SCADA platforms are limited to a primary and a backup server. Look for a product that can provide unlimited levels of redundancy. Ensure that there is robust failover for all components like alarm notifications (email, SMS text message, voice-to-speech call out), thin clients, networks, etc. Can you configure a redundant communications network? If so, is there an alarm to inform you if the backup fails?

Application Version Control – Many system failures are the result of unexpected consequences of innocent configuration or sometimes even the malicious acts of disgruntled workers. When things go wrong it is vital to identify who did what and to roll back to the last known working version immediately. While some SCADA providers support third-party version control, there are benefits to this being a native component such as the ability to automatically distribute the encrypted change list across all servers.

Real-time system backup and bi-directional synchronization – Traditionally, SCADA systems are backed up offline or online. The former involves shutting down the system leaving operators blind and unable to manage alarms. The latter can corrupt data during the process. Additionally, few platforms automatically sync historical data after a failure. Often a separate backup methodology is required for third-party historians. Automating backups may require custom scripting. Manual backups are easily forgotten. Systems that support bi-directional synchronization provide real-time backup of all your SCADA services. In addition to the historian, this includes events, alarms, security, and application settings. This means each SCADA server can be an up-to-the-second copy of your whole application. No missed backups.

Fast response to vulnerabilities from the vendor – Software platforms regularly release new versions and features and often connect to devices developed long after applications are deployed. This ensures that security gaps will appear over time. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) regularly conducts vulnerability analysis on products used in critical infrastructure. When they identify a potential security exploit, they contact the vendor who then has time to patch the vulnerability and distribute the solution before the vulnerability (and hopefully the fix) is made public.

Selecting HMI remote access options

Two leading methods exist for establishing mobile human-machine interface (HMI) connectivity; one providing more cybersecurity.

(This article is originally from Control Engineering eBook, SCADA & HMI Spring Edition 2021, and adapted for use in this SCADA & HMI guide)

Mobile HMI access is a necessity for many industrial automation applications, and two typical methods exist to implement this connectivity with routers and virtual private networks (VPNs):

- **Standard router without VPN**
- **Cloud-hosted VPN router.**

The first is a standard router, and although it is not secure, it is still used in many existing mobile HMI applications, and even in some newer ones. A primary attraction is its low cost, but this approach is discouraged because it poses significant cybersecurity risks when port forwarding is enabled in the firewall as this exposes the network to external threats.

A cloud-hosted VPN router simplifies information technology (IT) complexity by creating an encrypted connection from a local VPN router to a cloud-hosted VPN router via the internet. Remote users can securely access the local components and systems via the cloud-hosted VPN router. This option provides a high degree of cybersecurity, along with simpler configuration and maintenance.

A third type of router connectivity with a traditional VPN router implementation is not considered here due to the complexities of deploying this type of connection. It involves opening inbound connections and creates complications and risks similar to a standard router implementation. To evaluate each of the two types of remote access for mobile HMIs, accessed from a laptop, smartphone or tablet, see the table summarizing differences.

Standard router

In many industrial applications a standard router and firewall is used to protect the corporate and industrial plant network, requiring users to manually configure and manage all routing and firewall settings. This type of router does not usually have a VPN to encrypt data, but it creates port forwarding "holes" in the firewall for remote users to access specific applications and components in the plant network.

Most HMI users want the same level of access whether remote or local. Laptops normally connect to the HMI web server for monitoring data and making changes to setpoints and other parameters, or they connect to the HMI with programming software to troubleshoot or make program changes.

To connect remotely using a standard router, port forwarding is usually configured to allow access to the HMI, or to a local PC running remote access software. The local PC provides the remote user with the ability to run the HMI programming software. HMI mobile apps also require port forwarding so the remote user can access the local HMI for control or viewing data. These apps usually provide the same functionality as browser-based remote access, but via an app rather than a browser.

The main concern with this approach is the security risk associated with port forwarding in mobile and PC-based applications. It's easy for a hacker to determine which ports are open on a firewall, thereby gaining entrance to the corporate or plant network through the router.

While port forwarding can be extremely efficient and useful when done within a corporate or plant network, it is extremely dangerous to use this functionality at an internet-corporate interface. Organizations should avoid this router approach for new installations and should convert existing standard router installations to a more secure connection such as a cloud-hosted VPN router instead.

Cloud-hosted VPN router

Cloud-hosted VPNs provide a secure connection with simple setup and network configuration. Typical cloud-hosted VPN options include a local VPN router, a cloud-hosted VPN server, a VPN client and connected automation components.

A secure connection is established after the local router (at the plant/controls network) and VPN client (software installed at the user's laptop or mobile device) each make a connection to the cloud-hosted VPN server. The local router makes this connection immediately upon startup, but a VPN client only connects upon a verified request from a remote user. Once both connections have been made, all data passing through this VPN tunnel is secure.

Most cloud-hosted VPNs provide a free monthly bandwidth allocation for basic operation and then throttle data access once this allocation is reached, and also offer a premium plan for additional bandwidth.

For example, one product offers 5GB of free VPN data exchange per month, which is sufficient for most troubleshooting, monitoring and programming needs. Security risk is reduced when the local router initiates communication to the server via an outbound connection through standard open ports such as HTTPS. This usually requires no changes to the corporate IT firewall and satisfies IT security concerns. For added security confidence, users should look for cloud hosted VPNs that have an industry-certified information security management system such as ISO/ IEC 27001:2013. This indicates the supplier has implemented comprehensive security programs and controls.

Easier router configuration

Another advantage of a cloud-hosted VPN is simple router configuration. Since the secure local router will be connected to a predefined cloud server, the router comes preconfigured with complicated VPN networking settings in place, allowing non-IT staff to install it. All that's required is knowing the IP addresses of the automation components connected to the local area network and if the internet service provider (ISP) or corporate-wide area network router (not the cloud-hosted VPN router) provides IP addresses dynamically or statically.

Other advanced options may include cloud data logging and alarm notification, which provides a subset of HMI functionality and also is easier to use than custom programming. These services allow users to log system data and receive customized critical alarms on their mobile devices or laptops, providing a convenient, web-based historical record of system performance available when needed.

Mobile app-based remote access

Industrial HMI and programmable logic controller (PLC) components are increasingly supported with mobile apps. This provides users with remote access anytime from anywhere, with monitoring and control capabilities. To securely access industrial equipment, the mobile device must also employ VPN technology to encrypt the data from the mobile device to the plant network. Without mobile VPN, the firewall ports at the plant will need to be opened, creating a similar scenario to the standard router and leaving the plant network vulnerable to a cyberattack.

Using a hosted VPN provides a secure VPN connection for laptops and mobile devices; the latter is via a fully supported mobile application with VPN. Once securely connected to the plant network through the mobile VPN app, the third-party HMI or PLC app can then be opened and connected to the local HMI and PLC components as if the mobile user was on-site, because the user is there virtually.

Some routers provide a hosted VPN with connections for laptops and mobile devices. Apple iOS and Google Android mobile device apps are available, providing users with a secure connection to the plant network.

App-based access in action

Some cloud-hosted VPN vendors also provide app-based access to data logging software running in the cloud, along with widgets for configuring customized dashboards to be viewed remotely (Figure 1).

Figure 1: Maple Systems HMI mobile app, EasyAccess 2.0 works securely. It's also available for Google Android.

This built-in cloud logging could be particularly effective for an original equipment manufacturing (OEM) machine builder with thousands of machines installed worldwide at hundreds of locations, each with multiple users. The OEM would provide a VPN router for each machine, pre-configured to log data and including customized dash boards for remote viewing on the mobile app. No effort would be required by the OEM's customers to configure, install or maintain remote access software — other than installing an app on a smartphone or tablet.

For more comprehensive access beyond dashboards, remote users could access local HMIs and PLCs via apps using the mobile VPN provided by the hosted VPN supplier. For example, some mobile HMI software works securely when used in conjunction with a supplier-specific VPN router. Local equipment could also be securely accessed remotely by a PC for programming, monitoring or troubleshooting.

Cloud-based VPN security

Access to local HMIs and automation systems by mobile devices and laptops is a necessity for many OEMs and other companies. Using a cloud-hosted VPN to provide this access results in a secure system with simple installation, configuration, and maintenance.

Table comparison of remote access HMI connections

	Standard router	Cloud-hosted VPN router
HMI programming from a laptop PC	Not secure	Secure
3rd party mobile app support	Not secure due to port forwarding	Secure through mobile VPN
Security risk – laptop	High	Low
Security risk – mobile	High	Low
Changes to existing firewall	Required	Not required, although an outbound rule may be required
External cost Initial	Low	Medium
Sustaining	Low	Bandwidth dependent
Required technical expertise	Medium	Low
Data dashboards, alerts	Typically not available	Available through subscription

5G can help SCADA systems in plant control, process automation applications

A plant's supervisory control and data acquisition (SCADA) system could benefit from mobile broadband on 5G with cost reductions for enhanced capabilities being applied to plant asset management.

(This article is originally from Control Engineering eBook, SCADA & HMI Spring Edition 2021, and adapted for use in this SCADA & HMI guide)

The utilities sector was an early adopter of cellular networks, coming to rely on Global System for Mobile Communications (GSM) as an enabler for monitoring of remote assets. In water applications in particular, this allowed operators housed in a single control room to monitor assets such as pumping stations often miles apart, using a central supervisory control and data acquisition (SCADA) platform.

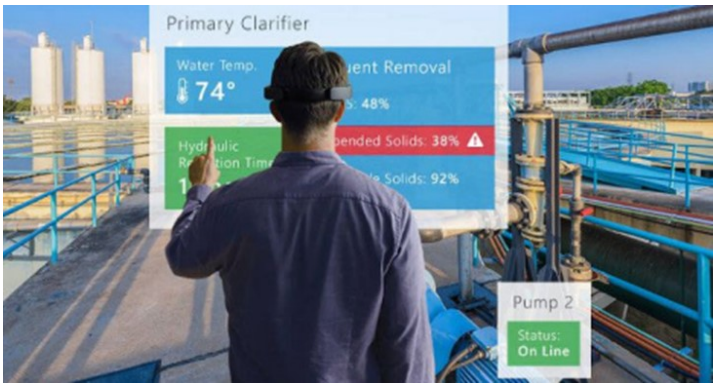
The wider adoption of cellular technologies has resulted in features such as the ability to send alarms, error warnings and general status updates to individuals using text messages, while 3G and 4G cellular networks and web clients have made machine-to-machine communications, and monitoring using mobile devices possible as part of the Industrial Internet of Things (IIoT).

Just as these network advances have been an enabler for easier wireless communications between automation systems and devices, so they have also been a barrier due to functional limitations. However, 5G however looks set to remove this barrier, supporting higher speed, higher bandwidth communications with improved reliability and very low latency.

This paves the way for many use cases in plant control and process automation, and it could have a disruptive impact on the wireless connectivity market. There is the potential for 5G to become a de-facto standard for wireless communications throughout the plant – from field level up to the cloud and all the layers in between. Support for industrial Ethernet will accelerate its uptake in plant automation, enabling simple integration with a complementary wired infrastructure.

In the context of a plant's SCADA system, superior mobile broadband on 5G could bring substantial cost reductions for enhanced capabilities being applied to plant asset management. Removing the need for hundreds of meters of wired IO, 5G expands the potential for decentralized control and wireless sensor networks. Further, the reliable, high speed and low latency communications promised by 5G

5G can help SCADA systems in plant control, process automation applications



There is the potential for 5G to become a de facto standard for wireless communications throughout the plant – from field level up to the cloud and all the layers in between. Image courtesy of New Products for Engineers Database

could open up the possibility for wireless solutions to be used for closed loop control in process automation.

As the first practical mobile communication technology for automation, 5G offers performance as high as 20 gigabits per second (up to ten times faster than current 4G networks. It offers significant potential as an enabling wireless technology for applications that generate and rely upon big data.

As we journey towards an era of Industry 4.0, 5G will inevitably come to complement SCADA as a key building block for the smart factories of the future. It could provide a route for allowing devices and processes to be rendered intelligent, with SCADA providing the mechanism for aggregating this data to form the interface between the information technology (IT) and operations technology (OT) worlds within a plant. SCADA could then be exploited to a much fuller potential, freeing up communications from the limitations of both wired and existing wireless infrastructures.

There are, however, also limitations to 5G. Some plants are electromagnetically noisy and so mobile signal strength will be an issue, likewise critical automation systems will always use the most reliable control method and have redundancy built-in. Where this is not the case, we may well see many traditional wired Ethernet or Wi-Fi applications migrate to cellular technologies based on 5G.

5G will bring significant new possibilities to plant control and process automation, not simply providing the wireless communications technology of choice in a SCADA context but conceivably even removing the need for or reliance upon wired communications in many applications. With its high speed, low latency and promised ultra-high reliability, from a plant control perspective and with an eye on Industry 4.0, the roll-out of 5G cannot come soon enough.

Replacing seven SCADA systems with one

Toronto Pearson International Airport starts fast on major baggage program with new, streamlined SCADA system that serves as the heart of the ambitious project

(This case study is a reprint from Control Engineering eBook, SCADA & HMI Spring Edition 2021)

When we're travelling, we all want to move through airports as quickly as possible. We want that for our bags too. That's why the Greater Toronto Airports Authority (GTAA) launched its ambitious, $1.5 billion Baggage 2025 program. GTAA operates Toronto Pearson International Airport, and it had a strong vision for improving Toronto Pearson's baggage handling system.

The first step was replacing existing systems with a single upper level/supervisory control and data acquisition (SCADA) system that would serve as the new heart of Toronto Pearson's baggage operation. GTAA enlisted the help of system integrator Brock Solutions of Kitchener, Ontario, Canada. Brock Solutions is an engineering and professional services company specializing in design, build and implementation of real-time systems for various industries worldwide.

Toronto Pearson served more than 50 million passengers in 2019, making it the busiest airport in Canada. GTAA wanted to modernize its baggage handling systems in an effort to provide better services for passengers. The new upper level/SCADA system replaced seven old SCADA systems.

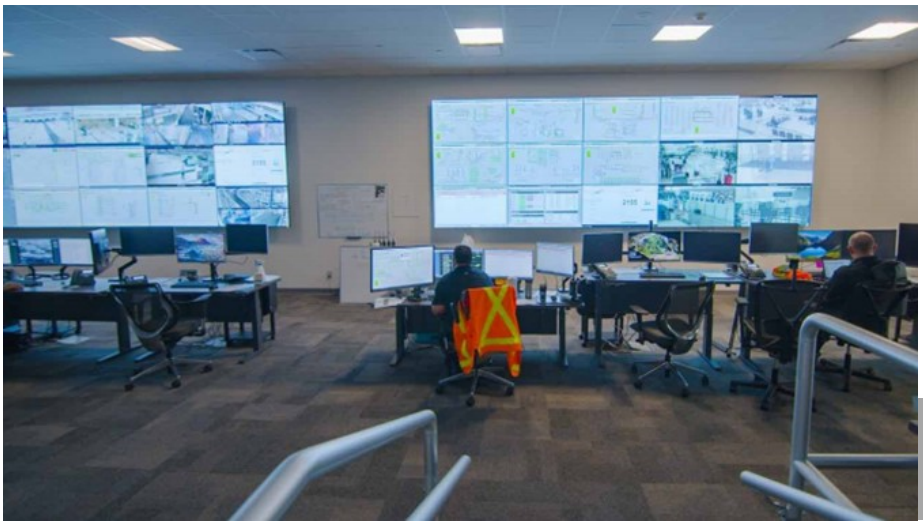
The installed system went live in March 2020. It's a combination of SmartSort (Brock's software for baggage sortation and reporting) and Ignition by Inductive Automation — an industrial application platform with tools for building solutions in SCADA, human-machine interface (HMI) and the Industrial Internet of Things (IIoT). The combination of software packages gives Toronto Pearson a solid foundation for the future.

The Baggage 2025 program at Toronto Pearson International Airport is already improving baggage handling efficiency. Image courtesy of Inductive Automation.

One brain, one journey

"With Baggage 2025, GTAA is reimagining its baggage handling systems," said Mark Holbrook, SmartSuite business manager for Brock Solutions. "The previous upper level/SCADA systems were provided by a variety of vendors over 15 years. These systems were programmed by various individuals using different design principles. This made the system very difficult to support, upgrade and maintain. The new system is much better, because it has one look and feel and is the perfect platform for future expansion and growth."

"The vision was to take the seven separate baggage systems and integrate them under one software umbrella," said Jose Salamo, associate director of baggage system capacity and infrastructure at GTAA. "So, a single application, single control room, one brain, one baggage journey for all bags at Toronto Pearson."



The "wall of glass" at Toronto Pearson. Image courtesy of Inductive Automation

Over the last 30 years, the airport saw continuous development and numerous construction projects that expanded the number of buildings and piers, while adding new baggage systems. The rising number of SCADA systems rose because of these expansions.

"It's been a long road, but we're finally here, working in one large control room with the suite of software applications delivered by Brock," Salamo said. "It's been a massive step forward in efficiency for baggage services here. So far, it's been a complete success. During the factory acceptance testing in early 2020, we had our staff asking if we could please turn the software on the very next day."

Replacing seven SCADA systems with one

Data from the baggage handling system can now be shared with various partners and stakeholders. Image courtesy of Inductive Automation

Zero downtime

The new system will help the airport achieve its baggage handling goals for years to come. "We're looking to enable the airport to be able to process north of 65 million bags by the year 2025," said Zeljko Cakic, director of the information technology (IT) airport development program for GTAA. "Prerequisite for achieving such a demanding goal was the creation of a single unified and integrated sort allocation controller (SAC) and SCADA upper level control system that would allow us to gradually eliminate legacy and obsolete technologies while allowing for zero downtime throughout the entire process."

The previous SCADA systems were replaced by the new one through a careful process of testing and phasing onsite over a period of 12 months. The old systems were systematically replaced by the new SCADA one at a time. Each new portion was brought online in parallel with the existing one so the system could be tested without affecting live airport operations.

Cakic said there were numerous problems with the mix of previous systems. Aging software of various generations, along with an incoherent IT infrastructure, caused plenty of issues. Obsolescence issues amplified difficulties caused by proprietary industrial control systems (ICSs) and technologies. "Integrational levels were not present and data and information coming from all these systems were not integrated and were not made available to the consumers," Cakic said. "We inherited all these systems with troubling reliability issues, without proper data consistency and data integration."

The new system has brought simplified, more efficient technology management and operations. Predictive management and maintenance are now possible, where they weren't before. "We have experienced improvement in resiliency and availability of the baggage systems and services," Cakic said. "Our partners and our internal stakeholders greatly benefit from information sharing and data consistency being shared across multiple business units and multiple business partners. We have seen overall improvements of the baggage efficiency and baggage processing."

First of its kind

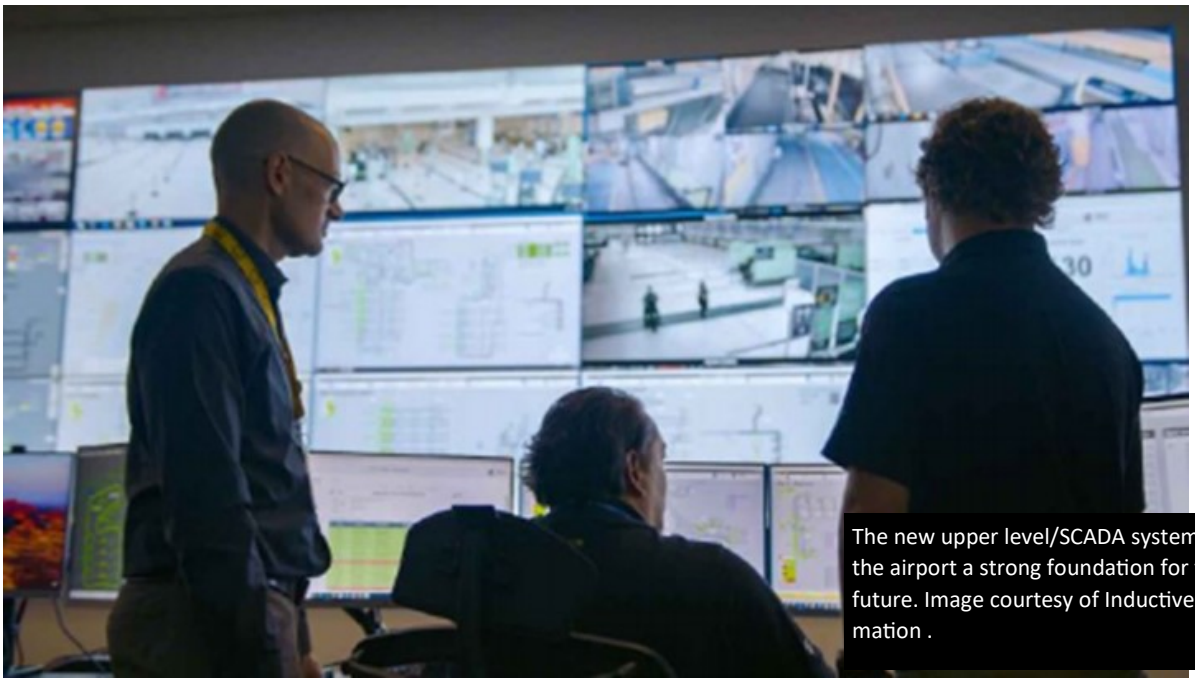
Beneficiaries of more data include airport operations teams, baggage service teams, Air Canada and other carriers operating at the airport.

"We chose the Ignition software because it solved a variety of problems with the existing SCADA," Holbrook said. "It was used because of its performance, innovation and scalability. The old system suffered from performance issues that were causing delays in situational awareness for the operators. This new software is up to the task of solving that issue. And innovation is a factor because this project involves an early baggage storage system that's the first of its kind in North America. This software was needed to help with some of the challenging information that needed to be displayed. And the airport needed a solution that was flexible and could scale to handle the hundreds of PLCs that would need to be connected to this system."

Maple Systems HMIs and HMI configuration software, EBPro; and our Industrial PCs using Aveva Edge 2020 supports Ignition software.

The airport will have the first and largest early baggage storage system in North America, which required innovative design around the communication protocols and graphical depictions. The airport also needed a SCADA system that's geographically aware of its equipment so situational awareness can be designated and managed. The solution also includes alarm-based SCADA navigation and situational awareness controls, such as integration with CCTV.

Replacing seven SCADA systems with one



The new upper level/SCADA system gives the airport a strong foundation for the future. Image courtesy of Inductive Automation .

Integrating seven disparate systems into one was a difficult task. The various systems needed to be studied, and custom tools were developed in order to complete the process. Over 50 SQL scripts had to be written in order to bring the tags over, and over 100 screens had to be analyzed and converted to SVG so they could be imported into the new system. The information came from raw text, XML, CAD, GFX, SQL and other formats. Extensive testing and office emulation also were required.

Scheduling for success

"The difficulty came in maintaining live operations at our busy airport," Salamo said. "This meant that testing and commissioning had to be done in small windows in the overnight period. Careful schedules and detailed phasing plans were developed in conjunction with Brock in order to achieve the accelerated schedule for a process that had to be repeated for every sector.

The biggest challenges were coordinating the nighttime work, day in and day out, and making sure that we didn't fall into the continuous regression testing that you sometimes have in identifying bugs and having to retest certain aspects that had previously passed. With the schedule, there were some instances where we did have to do some regression testing, but overall, it was a great success."

In deciding whether to go with this system for its ambitious, five-year improvement to its baggage handling system, GTAA looked at the work that Brock did at Dublin Airport in Ireland. Salamo said people at Toronto Pearson liked what they saw in the Dublin project

"What we found very appealing was the fact that it was one source of truth, a common interface amongst all of the screens and applications and it was one story to tell," Salamo said. Training of operators is also easier thanks to the new system. "It's advanced — a lot more advanced than the applications we had before," said Gil Pabustan, baggage services training supervisor for GTAA. "For training purposes, training on one application is a lot easier than on three different applications, as we did in the past."

Pabustan added the new system is better overall. "We noticed a big difference. I feel that now, everything's a lot smoother, much better, in respect to reporting and data collection. The team is very happy with the new system."

Brock looks forward to working with Toronto Pearson for years to come. "As the Baggage 2025 program continues over the next five years, there will need to be many modifications," Holbrook said. "This new SCADA system provides a firm foundation on which to build upon for these efforts."

GTAA picked this system with an eye to the future. "It was chosen to meet modern IT standards, independent of PLC and ICS original equipment manufacturers (OEMs), thus allowing GTAA to be in the driver's seat for planning and evolution of systems and technologies employed," Cakic said. "Choosing a partner such as Brock — with a strong IT background, orientation towards innovation, demonstrated agility, and common goals with the airport — was key for our success."

Ignition uses MQTT, a proven, standard, data-transfer protocol that is quickly becoming the leading messaging protocol for the IIoT. Read more about how Maple Systems HMIs supports Ignition and MQTT as part of our free HMI configuration software.