More Data, More Sources, More Problems

Despite today's ever-changing technologies, we seem to find ourselves with many of the same problems. The challenges facing the Automation Industry—both discrete and process—can be found in one of the most critical but often overlooked components of an Industrial Control System (ICS): connectivity and communication applications. There are five key challenges facing the Automation Industry as it relates to data access. The first and most obvious challenge is interoperability. If users cannot connect, there will be no data, control, or monitoring. This results in a lack of information-based decision-making. There are many sensors, Programmable Logic Controllers (PLC), Distributed Control Systems (DCS), Flow-Computers, and data sources within the highly heterogeneous environment of a modern business. Getting access to these disparate devices and the information they provide can be difficult.

Each industry has unique data handling requirements, which makes functionality the second challenge. These unique requirements tend to drive operators to a limited number of available solutions, which can often result in the selection of multiple communications drivers (for handling special cases).

The third challenge is reliability, a fundamental requirement of any device or software application. In an increasingly competitive landscape, businesses must capture and utilize data to gain a competitive advantage. Losing data is unacceptable and costly.

Scalability—the fourth challenge—is critical, but often a secondary concern. Solving immediate connectivity and communications problems are the top priority, but preparing for and solving the next set of communications challenges are just as critical in today's fast-paced business climate. The ability to adapt, change, and scale are pivotal to a company's success, and this requirement applies to all levels of a business.

The last challenge is safety and security. There are rising concerns among users as they take what were once isolated systems and connect them to internal and external applications like intranets and internets. In the wake of targeted attacks on control systems like Stuxnet and Flame, security and safety is in the forefront of everyone's mind.

Successfully navigating and solving these five challenges is critical to an organization's success in increasingly competitive industries.

Synopsis

To begin understanding the challenges engineers face every day in their quest for Data Access (DA) Automation, we first need to look at and understand the numerous components that make up an Industrial Control System (ICS). First, there are the Information Technology (IT) components comprised of hardware appliances and software applications. Next, there is infrastructure, which ranges from the building that houses the control system to the network that ties all of the components together. There are security and safety systems, and there is also a human element that handles the tasks that cannot be automated. This includes ensuring that the control system is performing as expected through both a strong understanding of the system and by initiating preventative maintenance. Finally, there is the environment and its effect on the control system; and, in turn, the control system's impact on the environment.

Hardware

The hardware that is found in an ICS can vary greatly based on what the system is producing. In a discrete manufacturing environment, you may find Programmable Logic Controllers (PLC), weigh-scales, barcode readers, and Computer Numerical Control (CNC) machines for milling or cutting. In a continuous processing environment, you may find Distributed Control Systems (DCS), mixing tanks, and quality control systems. These are not exhaustive lists by any means, but what these components and many others have in common is that they serve little purpose on their own. It is the combination of the components that is essential in building an automated system that can run efficiently and effectively. It is worth noting that these components often come from a variety of vendors, some of whom are direct competitors.

Software

Software also plays an important role in an ICS. At the lowest level, software is typically made available for the purpose of configuring the individual hardware appliances. Beyond that, software provides users with the ability to monitor and control aspects of the control system, usually from an application referred to as a Human Machine Interface (HMI) or Supervisory Control and Data Acquisition (SCADA). Historian applications exist for comparing current performance to past performance, and for determining undesirable trends that could be corrected before they become a problem. There are also business systems that allow management to view production and run the business. This includes Manufacturing Execution Systems (MES), which allow for the managing of product definitions, the scheduling of processes and resources, and the dispatching, executing, and tracing of work orders. Enterprise Resource Planning (ERP) systems allow organizations to integrate and view all facets of an organization, including development, manufacturing, sales, and marketing.

Like the hardware components described above, these software applications may also come from different vendors and provide very little value until they are integrated within the system.

In order to connect these different systems, vendors must design and build products that are capable of exchanging information. On the hardware side, this usually means that the appliance exposes a communications interface via Ethernet, Serial, or Wireless. This communications

interface provides the medium that will be used by two or more components to exchange information. In cases where an appliance may not expose a communications interface, it is common to hardwire the inputs and outputs to another device or sensor that does provide the necessary communications medium for sharing information.

The components must also be able to speak the same language, which is known as a protocol in the device world. This can be likened to the phone system. Two people from different parts of the world can call each other (assuming that they have a phone and phone service), but will not be able to exchange any information if they speak different languages.

Even supporting the same protocol may not be enough. For example, devices with an Ethernet interface may have the common Transmission Control Protocol/Internet Protocol (TCP/IP) stack embedded within the unit. The TCP/ IP protocol in itself is a container for application-specific data. We can think of this as a device-specific protocol that is encapsulated within a well-known protocol that is used in various industries. In this case, the devices must have the same knowledge of the device-specific protocol in order to interpret the information that the other device is making available. This can also be likened to our phone example, in that our phone system makes it possible for people all over the world to connect by dialing a code and sequence of numbers that are specific to that country. Making the connection is useless unless the two parties understand the same language. That is fundamental to exchanging thoughts and ideas.

Infrastructure

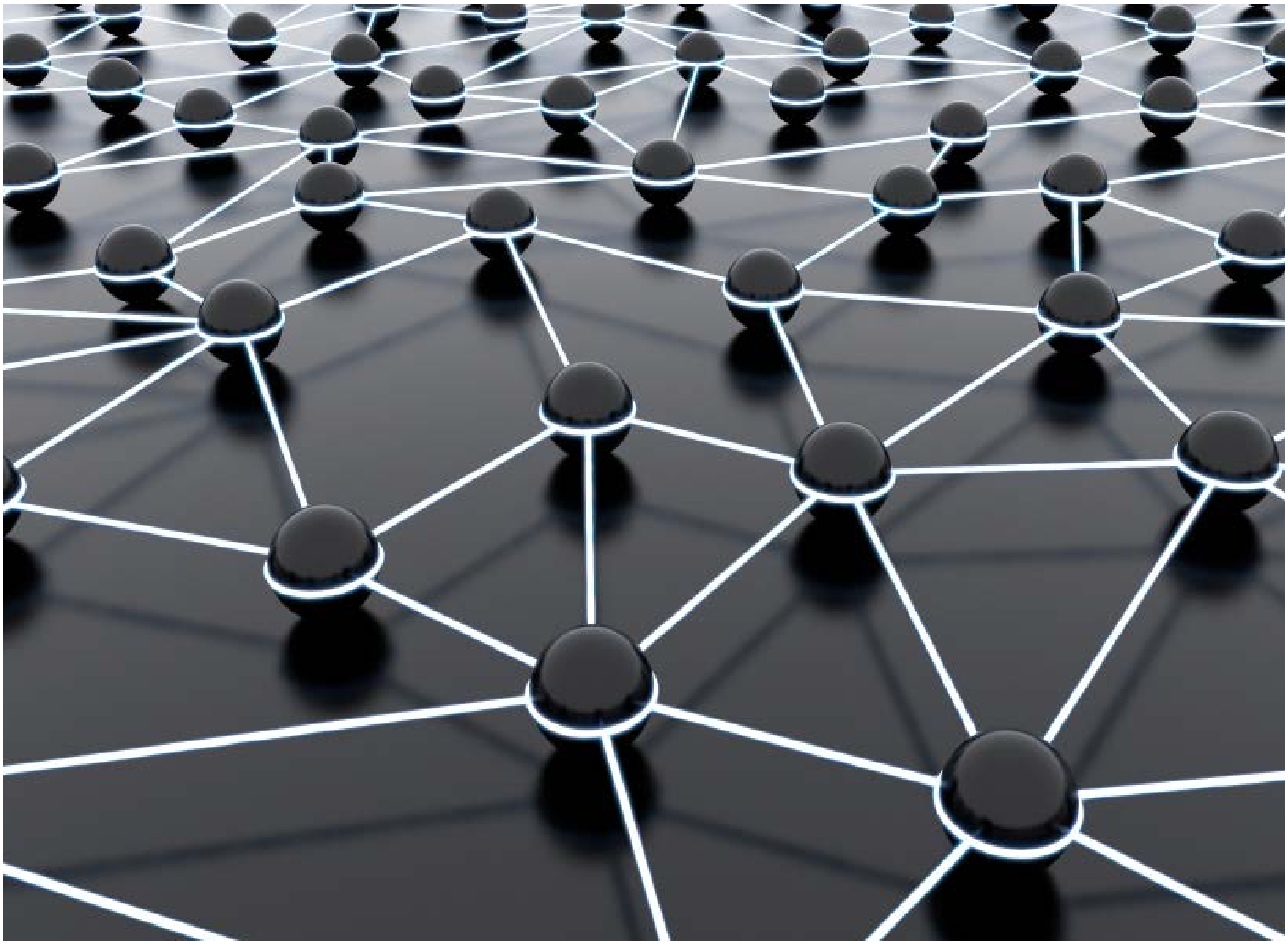
A control system will link the hardware and software components through the creation of a communications network. The network depends on the different components that make up the control system and their respective communications interfaces. For wired Ethernet capable devices, this may require running the Category 5 Cable (CAT 5), which is a twisted pair cable that allows the transfer of electronic signals for exchanging data. Each is terminated with an appropriate RJ45 adapter that is plugged into the communications interface of compatible devices. In an Ethernet network, there will be one or more switches to route communications requests to the appropriate devices: each allows two or more devices to exchange information. For wireless Ethernet capable devices, this may require installing one or more wireless access points that are capable of supporting the 802.11 standards that are supported by the appliances—and are also connected to the same switchable network. For Serial capable devices, this may require running a serial cable terminated with the appropriate 25 or 9 pin connectors. For great distances, it may also require installing data modems or a mix of Ethernet-to-Serial appliances.

The communications network is only one piece of the infrastructure. More and more control systems are starting to tie in elements of the building infrastructure, as well. This includes Heating, Ventilation, and Air Condition (HVAC), lighting, power generation, security systems, and any other system that has an impact on (or could be impacted by) the ICS. Fortunately, the modern systems that are used for building automation and control typically hook into some of the more common communications interfaces we have already discussed and interact just like any other device on the control systems network.

Bringing all of these components into the ICS requires the IT devices' connections to other systems be available to a wide range of personnel inside and outside of the organization. The IT devices are no longer isolated from non-IT personnel or from the outside world. As such, a security strategy must be employed in order to ensure the ICS's continuous reliability and integrity while building a system that can scale over time (so that add-on devices, systems, and functionality may be integrated in the future).

Human Element

Industrial Control Systems are rarely 100% automated: there is usually some human element that is needed to validate the results on a continual basis and determine how the control system should be modified to meet expected output production results at the required quality levels. In order to achieve this, people must be able to monitor system outputs and control system inputs. Remote



and local access to this information may occur. In either case, safety and security are required to provide and restrict access to prevent damage and financial loss to the systems and its operators.

It is not only imperative that the human element adds value to the control system, but also that the systems and processes are not negatively impacted when they interact. Likewise, the system must expose the required functionality in order for the human element to perform effectively.

Environment

The environment can also impact the ICS. It may be as simple as controlling the ambient temperature to ensure that systems do not overheat and fail, or monitoring the levels of rain runoff pouring into the water source of a water treatment plant. Wireless technology requires line-of-sight, and makes it necessary that buildings, trees, and other obstructions be taken into account when laying out infrastructure. There are also harsh environments that may cause atypical wear and tear on the ICS's different components, making parts management crucial to the long-term success of the system. The environment can be a critical input into an ICS and can significantly affect an automation process.

Conversely, the ICS's designers and integrators have a responsibility to ensure that their systems have little to no impact on the environment. From minimizing pollutants into the air and water to the amount of resource consumption required to operate, the industry has to take into account how the outputs of its systems affect our environment. This will most certainly require that additional components be installed and maintained, thus adding to the complexity of the ICS.

Challenges

As you can see, automation and ICS involve a lot of moving parts, some of which are more easily controlled than others. Although automation is not new, the advances in technology and the way that systems are built and maintained through their lifecycle are still evolving. Organizations want to monitor and control all aspects of the automation system to ensure they are utilizing business intelligence and realizing operational excellence. This can be a daunting task that never really ends and requires continual improvements.

Although the components are diverse, they must seamlessly interoperate with one another as if provided by a single vendor. As a whole, they must provide the functionality necessary to meet the expectations of those who own the system. They must also allow those responsible for running the systems to access the information needed to make sound operational decisions. The system must not only be reliable and able to withstand elements that may impact its operation, but also be extensible over time and able to scale for future needs. Lastly, proper security and safety must be built into the system to prevent costly damage while safeguarding the environment and the surrounding community.

This paper will go into more detail on these topics and on the technology currently available to help meet the demands of these challenges.

Interoperability

Perhaps the biggest challenge that the automation market has faced over the years is the ability to fully integrate the hardware and software components that make up the ICS. Most hardware companies aspire to be one-stop shops for automation needs: as a result, a majority of their efforts over the years have been spent ensuring that the different appliances they manufacture can be easily integrated with one another. The consideration and attention to integrating third-party appliances (which are seen as competitors) is often overlooked or treated as an afterthought. On the other hand, the market wants the flexibility of purchasing best-of-breed components from a wide variety of vendors. The likelihood that a single vendor has a complete and superior solution at the right cost and with the most functionality is small.

Thankfully, many hardware vendors enabled access to their proprietary methods of exchanging information between their products. By making these communication methods available, competitive vendors could start integrating with each other's appliances. Issues with scaling arise as a greater number of disparate devices and vendors become incorporated into a single environment. The heterogeneous environment requires that vendors implement all the necessary communication methods and continually manage them as the various vendors update them. Usually, this comes at a loss of performance to the market. The market is vulnerable to vendors who optimize data exchange over their own proprietary interface versus third-party interfaces in order to secure a competitive advantage. The market is also at the mercy of vendors to implement the necessary integration points, which may not align with the markets timeline. Unsurprisingly, the market has driven the creation of better solutions to this integration problem over time.

Let's look at the automation market and how it has broken up into smaller, more specialized markets. Some of these specialized markets include the Automotive, Power Distribution, Building Automation, and Oil & Gas industries. To simplify third-party connectivity in these specialized markets, end-users have forced vendors to collaborate and develop common standards for integrating the equipment you would typically find in their respective settings. For example, in the Power Distribution markets, vendor collaboration has resulted in the development and acceptance of the Distributed Network Protocol (DNP) as a means for exchanging information between systems like electrical substation equipment. Likewise, the Building Automation and Control Network Protocol (BACnet) has been developed to tie HVAC and security systems with the systems that monitor physical access to the building, thus allowing an efficient use of energy depending on when and where people are located within the facility.

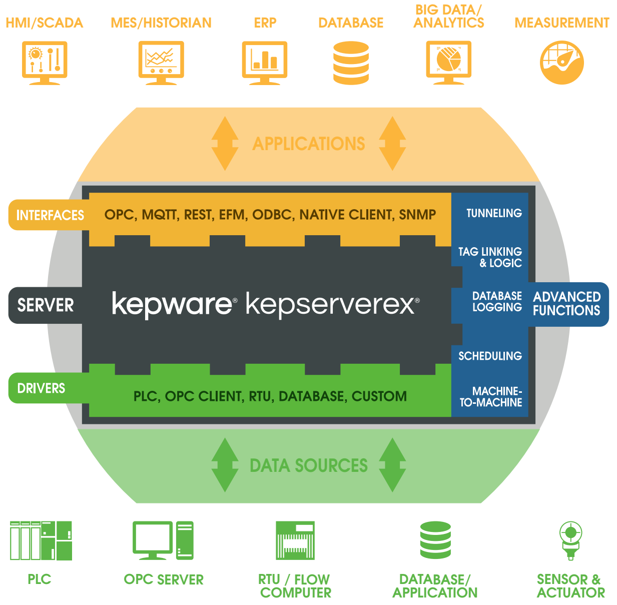
Unfortunately, these are not the only "standard" protocols in the respective markets. Globally, different regions have created their own standard protocols for local markets. DNP and BACnet are considered North American centric, whereas their respective counterparts in Europe are IEC-61850 for Substation automation and KNX for Building Automation. Vendors who manufacture and supply products all over the world are tasked with keeping their product lines up to date with regionally-specific protocols. Furthermore, an ICS could be comprised of multiple systems from separate markets. In the case of a power generation facility, there is still the building infrastructure that affects overall productivity and needs to be accounted for. For this to be possible, the integration points between the power-specific equipment and the building infrastructure would need to be able to communicate over the DNP and BACnet protocols. While not impossible, this is not desirable as the complexity of the environment grows over time. As manufacturing becomes more intelligent and sustainable, it will be more common to integrate building automation along with the required power generation systems to manufacture any type of good for any type of market. It may perhaps be utopian for automation if there was a single protocol that could be leveraged by any hardware or software component in any ICS. For this to be achievable, we need competitive vendors across different markets and from all over the world to come together and collaborate on a single specification. This effort exists and is managed by the OPC Foundation.

The OPC Foundation was initially formed in the mid-1990s to focus on the generic collection of real-time data found in process control environments by HMI/SCADA applications. Since the software applications at that time primarily targeted Microsoft Windows, OPC leveraged Microsoft's technology of the day to share information between different applications. This technology was referred to as Object Linking and Embedding, which gave the Foundation its original name of OLE for Process Control (OPC). The Foundation released a well-known interface for exchanging real-time data via this OLE technology, and it was soon adopted by many. On the protocol side, vendors wrapped their proprietary methods with this open technology and created server-based applications to provide the necessary services that would allow other applications to discover, read, write, and subscribe to real-time data. The HMI/SCADA became OPC client-based applications that consumed data in order to provide visualization and control of the process control systems. This initial framework was very simple and generalized data down to its most current Value, Timestamp (indicating the freshness of the data), and Quality (indicating if the Value should be trusted). OPC provided a first step in the realization of a common protocol in process control to equipment that could model their data in this format.

Over the years, OPC has matured into a more cohesive platform for richer data models across multiple market segments and is no longer confined to its process control roots. In addition to real-time data, OPC allows for the exchange of alarm and event information, historical data access, and any other type of domain-specific data. By developing a general but fundamental framework, any market can model their data as OPC. Furthermore, OPC is no longer tied to Microsoft technology and can run on any platform. This opens the door to embedding the basics of the universal protocol into an appliance, thus enabling rich desktop and server applications to leverage the technology's most powerful features. OPC has become the OPen Connectivity standard for automation.

The best solution would be for all components to adopt a universal standard like OPC. In reality, however, this may not be practical. With the benefits that come with generalization, come the detriments of implementing something that may be more complex than needed for a particular component. This is where communications layer come into use. Communications layer were developed to create an abstraction layer between open standards like OPC and the many existing device-specific protocols. OPC's flexibility allows independent vendors to model information from any component found in an ICS (such as an OPC data source) and make it available to the richer applications that need to consume information from a wide range of components. In order to integrate with the system, these richer applications only need to be OPC aware.

The communications layer is responsible for understanding the specifics of the underlying components. This includes how to communicate with the data sources that need to be mapped to OPC, and is typically handled by a specific piece of software referred to as a device driver. The device driver understands the specifics of a particular protocol, including communications mediums (such as Ethernet or Serial). It understands the information that can be exchanged over the protocol so that it can model it in an open format (such as OPC). Lastly, it is capable of making appropriate requests to monitor and control the data exposed by the systems that support the specific protocol.



Perhaps what makes the communications layer the most desirable solution for guaranteed interoperability is its ability to be modified to expose the information it retrieves from the many disparate components it supports into any industry or market-specific standard that exists today (or could be developed in the future). The communications layer is not limited to supporting a single standard: it is capable of supporting multiple interfaces to ensure interoperability between the different varieties of applications users might find within a single manufacturing environment. For example, the communications layer might support OPC for HMI/SCADA and other automation-specific applications while providing information over the Simple Network Management Protocol (which integrates common IT equipment like switches, printers, and personal computers) to IT-specific applications that facilitate the management of these assets. Regardless of the market or products being produced, the communications layer can be considered the heart of interoperability.

Functionality

Although exchanging information in an ICS is critical, the components of the ICS must expose the functionality that is required to adapt to both the specific environment and the operation. The simple act of exposing and consuming standard interfaces does not guarantee that the integration of the many components will be entirely plug-and-play.

On the communications side, the infrastructure or components that make up the system may impact the flow of information exchange. Some components may respond faster to a request for data than others. The networks that physically connect the different components may include bottlenecks that must be accounted for in the interoperability strategy. Each will affect the ICS's performance and the continuity of information flow through the system. The system implementers must define the importance of certain information and the tolerance of communications disruption. This is only achievable if the components allow the configuration of how data is prioritized and optimized—and how time constraints are defined as acceptable—before considering the system to be in error. To prioritize data, implementers will need to establish poll groups with a unique sample rate to indicate how often the data should be acquired from the underlying data sources. Implementers will also want to be able to control how the data collection is handled in order to ensure the most optimal use of bandwidth and other resources. Depending on the mix of data sources, some will surely be more responsive to communications requests than others. Some data sources may be unresponsive at times due to network disruptions, servicing other communication requests, or simply being taken offline for any number of reasons. It is imperative that the availability of any data source does not have an effect on the collection of information from the other data sources. Implementers will need the ability to control the appropriate timing constraints at a per data source level that indicate how long a request should wait for a response before considering it an error. They will also want to be able to take devices that are offline or in error out of the poll sequence in order to minimize the communications impact on the rest of the system.

The market expects to be able to easily connect to any data source playing an integral role in the ICS. As such, there is an expectation that any communications protocol or Application Programming Interface (API) must be able to be integrated into the system. It is improbable that all hardware or software components will be able to communicate with all data sources. Solutions will need to allow implementers to extend connectivity capabilities by providing the tools and interfaces necessary to tie in components that are not natively supported by the solution. Regardless of whether connectivity to a data source is natively supported, the solution should allow for the discovery of data sources and the information they expose. They should also provide a mechanism for streamlining the configuration of the communications network to ensure ease of use and minimize human error.

In many cases, it is necessary to perform operations on the raw data before it is leveraged by higher-end systems. While higher-end systems are likely capable of performing these operations themselves, it would be best if this could be managed as close to the device as possible. This would allow the implementer to define the operations once, instead of at each higher-system application. It also would minimize communications bandwidth by manipulating the data at the lowest level in the ICS and then reporting that data to higher-level systems as necessary. This ensures that the higher-level systems are continually synchronized by having access to the same information at the same time. In the event that some higher-level applications require access to the raw data, the solution must be able to provide both raw and manipulated data.

It is not just applications that need access to data from other sources. The data sources or devices themselves may need to exchange information with other disparate devices or systems, thus creating a need for Machine-to-Machine (M2M) connectivity. If these machines are unable to natively communicate with one another, a solution must be implemented to enable a third-party to broker the communications between the devices and provide the necessary information link between the components.

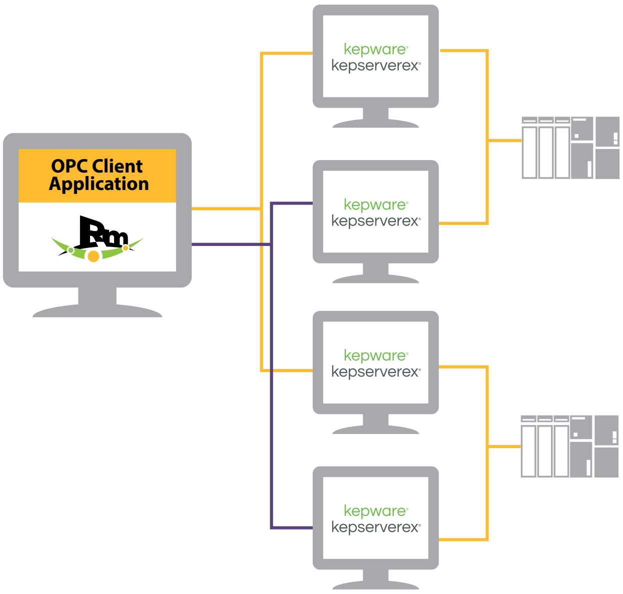
This functionality and more can be found in a feature-rich connectivity platform. The platform represents the heart of the communications network in that it is a central location for the configuration and flow of data between multiple data sources. The best platforms will allow users to easily manage data flow and ensure that communications are optimized, while having a minimal amount of impact on the network infrastructure. Whether it is moving data between hardware and software components, exchanging data between devices via M2M communication, or linking software applications, this platform should provide the appropriate interoperability and the required functionality that is necessary to solve industries' real world problems.

Reliability

The greater the ICS's complexity, the greater the chance of system failure. Nothing is guaranteed to be error free. Software contains defects, and hardware fails over time. In developing a reliable solution, system implementers should consider how to minimize points of failure, build in notifications that alert appropriate personnel when something has failed, and consider a predictive monitoring strategy to detect imminent failures before they occur.

As previously discussed, an ICS is a web of interconnected hardware and software components that work together to produce product. Some components will be more detrimental to the process than others if they fail to perform their actions. When examining the ICS's layout, implementers need to assess any weakness in the system. One area of critical importance is the network infrastructure that ties all the moving parts together. Components that only have a single connection path on a network are prone to disruption, which causes these components to be inaccessible. This is considered a single point of failure. A reliable solution will look to minimize these single points of failure, especially when they involve the most critical components to the system. In order to do this, implementers must build communications redundancy into their systems. The redundancy should be configured such that multiple paths exist between the critical components and the rest of the system, thus minimizing the risk of being unable to exchange information. Typically, these paths are disparate communications mediums (such as Ethernet for the primary connection and a dial-up modem for the secondary alternative for data flow).

A reliable solution will also include component-level redundancy. This is defined as multiple components (each capable of providing the same functionality within the system) that coexist in the event that one component fails. These components usually mirror each other during normal operation, with one component performing the primary role in the ICS. The redundant component will be passive and wait for its turn to perform in the event that the primary component fails. Additional intelligence is required to be built into the solution in order to understand which components are actively playing a role in the control system at any given time. By coupling the concepts of component-level redundancy with communications path redundancy, users can construct a reliable system and minimize the risk of communications failure. This can apply to both hardware and software components.



Redundancy itself does not guarantee that there will never be failures within the ICS. Redundancy can also be very expensive, due to the added investment in additional components that basically serve the same role and the additional network infrastructure needed for the multiple communication paths. As stated earlier, redundancy capabilities will most likely be focused around the most critical parts of the system; however, that is not to say that the less critical parts do not play a role in the control system. The system implementers need to build proper alert notifications into the ICS in the event anything fails that may impact the automation process.

Alert notifications can be built into the same tools that allow personnel to perform their jobs under normal circumstances. This provides the highest level of certainty that the appropriate parties will realize there is a problem with the system, and it will also allow them to act on the problem in real time. The individual components and the information they possess must be evaluated on a regular basis in order to determine if there are any anomalies in the system. If something irregular is detected, this information must be presented to the other interested components in the system and appropriate actions must be taken. This information should be made available in the same way that normal process data is exchanged between components. As such, components in a failed state should provide as much information as possible in order for personnel to understand and correct the problem. Additional insight into the problem can be obtained through the health of the components, the quality of the data, and any additional meta-data that is available.

Most systems will also implement a predictive monitoring strategy within their ICS, which is better than just detecting failures. This strategy ties into the system, much like the handling of process data and alert notifications. It is unique in that the information collected tends to be focused on the attributes of the components themselves, rather than the process data that drives the products being produced. These attributes depict the components' health and can be compared to attribute data that has been collected over longer periods of time—as well as recommended operating parameters for the components of interest. This allows the system to determine when and why components started behaving differently. It also allows the system to monitor operating parameters and ensure that they are running with the appropriate specifications defined by the component manufacturer. This allows personnel to investigate and proactively maintain the system before a real failure occurs, thus minimizing downtime and allowing for scheduled maintenance during non-peak times.

Further justifying the cost of redundancy is employee safety. Industry workers are often exposed to dangerous and remote environments: their safety is priceless. Reliability cannot be an after-thought.

Environmental concerns also drive the need for reliability. A connectivity platform that is part of a leak detection system must be robust and cannot be a point a failure in order to help reduce the risk of the environment being exposed to harmful materials.

A comprehensive connectivity platform can provide the tools needed to reliably interconnect, monitor, and manage the industrial network and all of the components that comprise the ICS. Implementers should be able to easily integrate new redundant components and setup the necessary redundant paths to ensure the highest probability of the continual flow of information throughout the system. In addition, the connectivity platform should generalize how other components can detect and be notified of failure within the ICS. Lastly, the connectivity platform should also be able to provide the right amount of information available based on the ICS's reliability needs and requirements.

Scalability

When initially building the ICS, implementers must be sure that they do not limit their planning, design, and implementation to developing a system that only meets the needs of today. They need to assume that at some point in time, the system will be asked to do more without actually knowing what "more" is. Reasonable assumptions of what "more" may mean could involve scaling the system to produce more products, implementing or enhancing a predictive maintenance strategy, or integrating the ICS with existing or unidentified business initiatives or applications to aid the running of the organization.

The control system should be extensible, allowing for easy growth as requirements change throughout the course of its lifetime. Most control systems exist to aid in the manufacturing of a select number of products: although the type of products produced may not change over time, the demand for them does. In order to keep up with increased consumer demand, existing components and infrastructure must be able to scale and coexist with new components added to the system. If existing components are expected to take on additional load, the performance and quality of past expectations must not suffer. If the system has to expand, the original design should allow for easy replication by allowing some or the entire pre-existing environment to be duplicated. This could run independently or in parallel where resources are shared. Either way, the flow of information through the entire system will continue to increase as the ICS matures.

Once an ICS is operational and meets initial requirements, it will be necessary to provide ongoing system maintenance to ensure that it continues to perform and meet obligations. Employing a predictive monitoring strategy can be most effective. This will put a larger load on the system, however, in order to handle the flow of process data that is critical to automation. Information about the health and operating requirements of the control system's components will also need to be monitored. Sometimes, there will be less capable devices that do not provide the information needed to allow other components to monitor their health. In this case, additional measurement components or sensors that are capable of providing this required information will have to be deployed and integrated. This will place additional demands on the control system's network infrastructure.

Technology is continuing to evolve. The simple, day-to-day things that we use and rely on (which can be as simple as a light bulb or as complex as a security system) are becoming network-enabled. Their impact on the ICS will determine the desire and need to integrate these components into the automation process. The industry refers to this as the Internet of Things: an evolution of Internet-enabling anything that contains useful information for the purposes of monitor or control. Users will perhaps be the primary benefactors of this phenomenon and will be able to build more intelligence into their ICS. By removing the human element and aligning it with other automated tasks, ICS will be more energy efficient in the control and utilization of resources like lighting, heating, and cooling. The benefits will be realized as the ICS expands and adopts components that directly or indirectly impact process.

As a business grows, there will be an increase in the amount of visibility needed to ensure operations are running optimally. Personnel will rely on software applications to provide them with the appropriate information necessary to make informed business decisions. As the amount of visibility increases, there will be an equal increase in the amount of information that must be collected from the ICS in order for these software applications to perform their jobs. When local businesses expand into new territories and become global companies—or merge with another company—the flow of information will continue to become larger and more complex.

How does a connectivity platform scale in order to meet growing needs? Connectivity to all sites is desirable and requires the ICS to scale to accommodate the often-changing landscape. The need to monitor remote processes is one reason why connectivity and communications are so critical. Positioning industry experts at all remote sites can be difficult, costly, and impractical; remote monitoring has provided a way for experts to reside anywhere, monitor the operations of multiple sites at once, and provide consultation when required. Alarms can also be implemented to bring potential issues to attention.

Enabling and allowing real-time analytics solutions to evolve is an important reason why scalability should be factored into a connectivity platform. Often, the algorithms and decision-making functions of these solutions are based on empirical data that is continuously being acquired, stored, and analyzed in a continuous loop. Operational excellence is the driving force behind the development of these analytical solutions as Oil & Gas companies continuously strive to improve their efficiencies in drilling and production, transmission and distribution, refinement, and other operations.

Growth is often achieved via acquisition. This provides another example of why the scalability of your connectivity platform is a considerable requirement. There have been scenarios where a company's acquisition has more than doubled the amount of assets that it needs to monitor and control. It is cumbersome to tear out ICS components after an acquisition in order to enable interoperability with an existing ICS. Writing custom code is an option, but requires internal maintenance and is usually managed by a single non-dedicated developer. Having an ICS built around a connectivity platform that can scale and interoperate with new and existing components is ideal.

A connectivity platform that is optimized for information exchange is required to ensure that the communications infrastructure of the ICS will scale over time—regardless whether it is brokering the flow of data between a few components or several thousand components. The best connectivity platform make good use of available resources in order to communicate with multiple components at the same time, while being responsive to richer applications that are leveraging its services. As components are added to the system, there should be no impact on existing communications and the services provided to others.

Safety and Security

Today's ICS are no longer isolated from the outside world. As we have seen, more and more components are becoming inter-connected to the control systems in an effort to completely automate operations and business processes while providing the necessary information to the right people at the right time. Business applications typically reside on computers that have access to the Internet, while employees who travel or leverage mobile technologies can access critical information from beyond the peripheral walls of the ICS. These machines and mobile devices inherently have access to the control system since they have access to monitor (and in many cases control) the automated process.

Proper security practices must be enforced to prevent unauthorized access to the systems. This may be as simple as allowing access on a per-user or per-machine basis, or it could involve more granular control on what particular users can and cannot do within the system. Because information will flow over public communications domains, the data must also be encrypted and protected from those who may cause harm to the system or jeopardize the safety of its personnel and the surrounding environment.

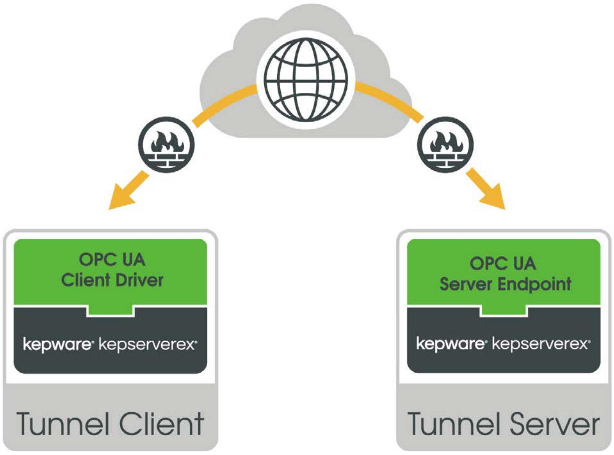
Every component within the ICS that requests or provides data is responsible for the integrity of who they exchange it with. It must ensure that the delivery of the data cannot be compromised by those who have gained unauthorized access. Typically, integrity validation is done at the time when one component connects to another. This involves the exchanging of identity information in an effort to develop a trusted connection. If the identities on both sides are acceptable, the components can trust further communications between each other; otherwise, the connection is broken and any further communications will be rejected. Trusting the other party does not mean giving them full access or control of the system, however. If this is a concern, different access levels can be configured based on the components required interactions. By setting access levels, components can provide as much or as little information that is needed for users to perform their jobs. This will minimize the possibility that another component may accidentally modify process data critical to a running process. It also provides another layer of defense in the event that an unauthorized user is somehow able to gain trusted access to the system. The less information that is exposed, the less chance that anyone will compromise the well-being of the ICS and its surroundings.

When information flows over the public domain, there is the risk that data could be intercepted, deciphered, and used for malicious purposes. How easily this can be accomplished greatly depends on the communications protocols utilized for exchanging this information. There are many automation protocols that exist that are well documented, and provide no means for encrypting the data they encapsulate. These protocols should be avoided when data travels over the public domain, because they can easily be interpreted. This information could result in a breach of confidentiality or expose a company's intellectual property, potentially resulting in financial damage to the organization. A malicious user could rewrite the data as it passes over the public domain in an effort to cause damage to the system or compromise the safety of those responsible for the ICS. Secure communications where the data is encrypted and only understood by the two trusted parties is necessary.

Aside from all the unsecure protocols, there also exist a fair number of secure protocols. Many of these secure protocols are vendor or industry-specific; however, there are some (including the latest OPC standards) that implement and support secure methods for exchanging information based on IT-approved technologies while being industry agnostic. OPC Unified Architecture (UA) supports the ability of components in a system to exchange certificates in order to create a trusted relationship. These certificates are then utilized to encrypt and decrypt the secured information that is exchanged over any communications medium. OPC UA also allows different users of the same systems to pass along their user-specific credentials so that the system can provide them with only the relevant information and actions that they need to perform their respective duties.

Although many components will never leverage the robust security model of a technology like OPC UA, this does not mean that these components cannot be leveraged in a secure manner. By utilizing a connectivity platform, unsecure protocols can be segmented into private communications networks. Any data that must be sent over the public domain can first be transformed by the connectivity platform into a secure protocol before transmission. In this respect, the connectivity platform acts as a secure tunnel between private and public domains. Likewise, many components will lack the intelligence and capacity to define the information to which user profiles have access. Again, the connectivity platform can layer on this intelligence by brokering requests and deciding whether it should allow requests based on the user credentials and profile.

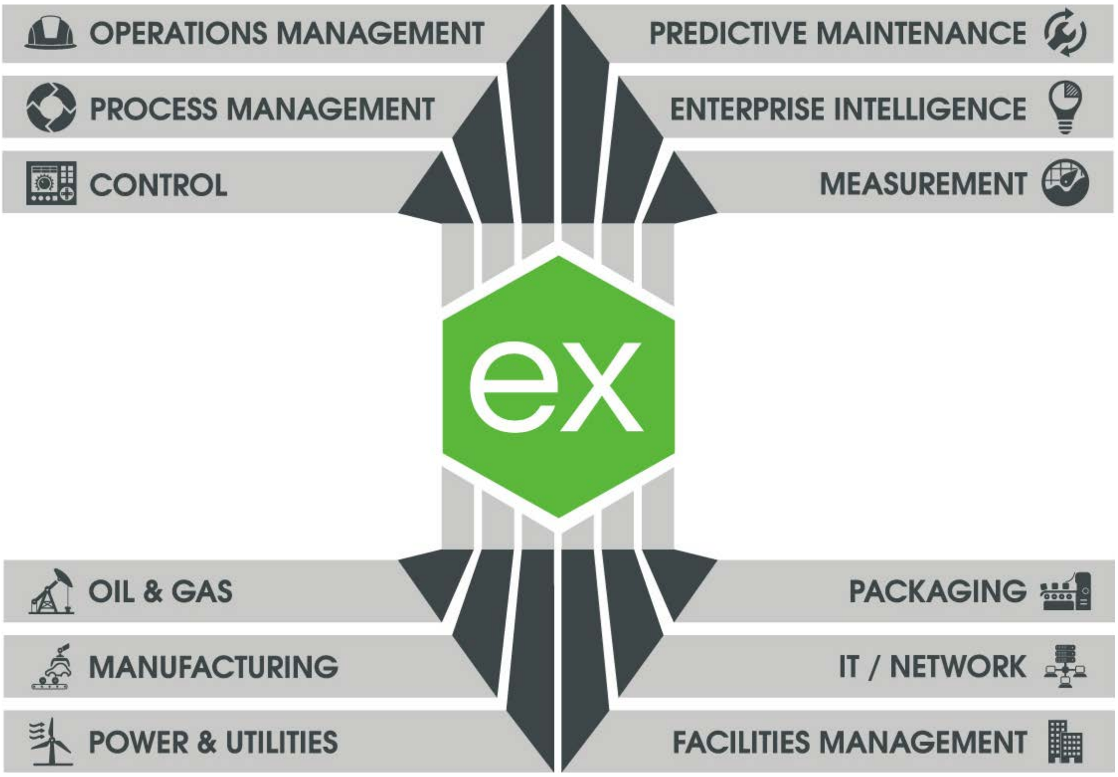
The Automation Industry is constantly exposed to security threats. The Stuxnet incident is a prime example of a malicious intent to compromise a nuclear energy facility's industrial control system. This incident caught the full attention of the world, and highlighted the significance of security and safety. It is not hard to think of multiple scenarios where a cyber-attack could cause bodily and/or financial harm to the Oil & Gas Industry for example, especially when considering the volatile nature of its products. The anonymous and false cover nature of the typical modus operandi of terrorism plays well in the world of cyberspace. Making matters worse, cyber-terrorism can be a relatively inexpensive endeavor but very expensive to protect against. The rapid pace of technology and the ease of sharing information and techniques via the Internet play well for the intentions of a malicious mind while creating nightmares for those wanting to protect against it. Any component in an ICS needs to be developed with "security by default" and not as an after-thought.



As Stuxnet proved, these security concerns are real and need to be protected against.

Security is needed to prevent unintentional harm in operations where multiple entities share access to the same data. That there is data in these systems that would be considered the intellectual property of the system owners complicates matters. Their competitive advantages could be compromised if the data was acquired by an inappropriate entity. Furthermore, there are also situations where some data points must be monitored by multiple specific users. Providing control access to the wrong user at the wrong time could result in an inadvertent mishap, causing damage to the operation or even bodily harm. These security concerns require that the connectivity platform be able to provide restricted access to data objects based on user credentials.

Summary



An ICS is made up of many parts, with many functions, and from many manufacturers. At the heart of an ICS is the connectivity platform, which provides the necessary connections and communications. The ideal platform provides interoperability, functionality, reliability, scalability, and the tools needed to ensure security and safety. Without a connectivity platform that is proven to overcome these five challenges, it is difficult—if not impossible—for an ICS to reach its requirements or full potential.

There are many viable data access options on the market that can solve some of these challenges. For example, there are numerous OPC Servers on the market that provide connectivity to a single device or protocol, but only few that can connect to thousands of devices using multiple protocols. Likewise, there are only a few solutions that can provide the advanced functionality and scalability required to meet the growing needs of tomorrow's ICS. A connectivity platform that can truly claim to be reliable must pass rigorous in-house testing, participate in interoperability workshops, and continually meet certifications requirements dictated by industry and validated by third-party firms. There are only a few platforms that go above and beyond to ensure their layers are safe and secure. The solution that will deliver the integrated ICS of the future is one that can provide centralized communications, proven interoperability, on-demand scalability, and industrial strength.