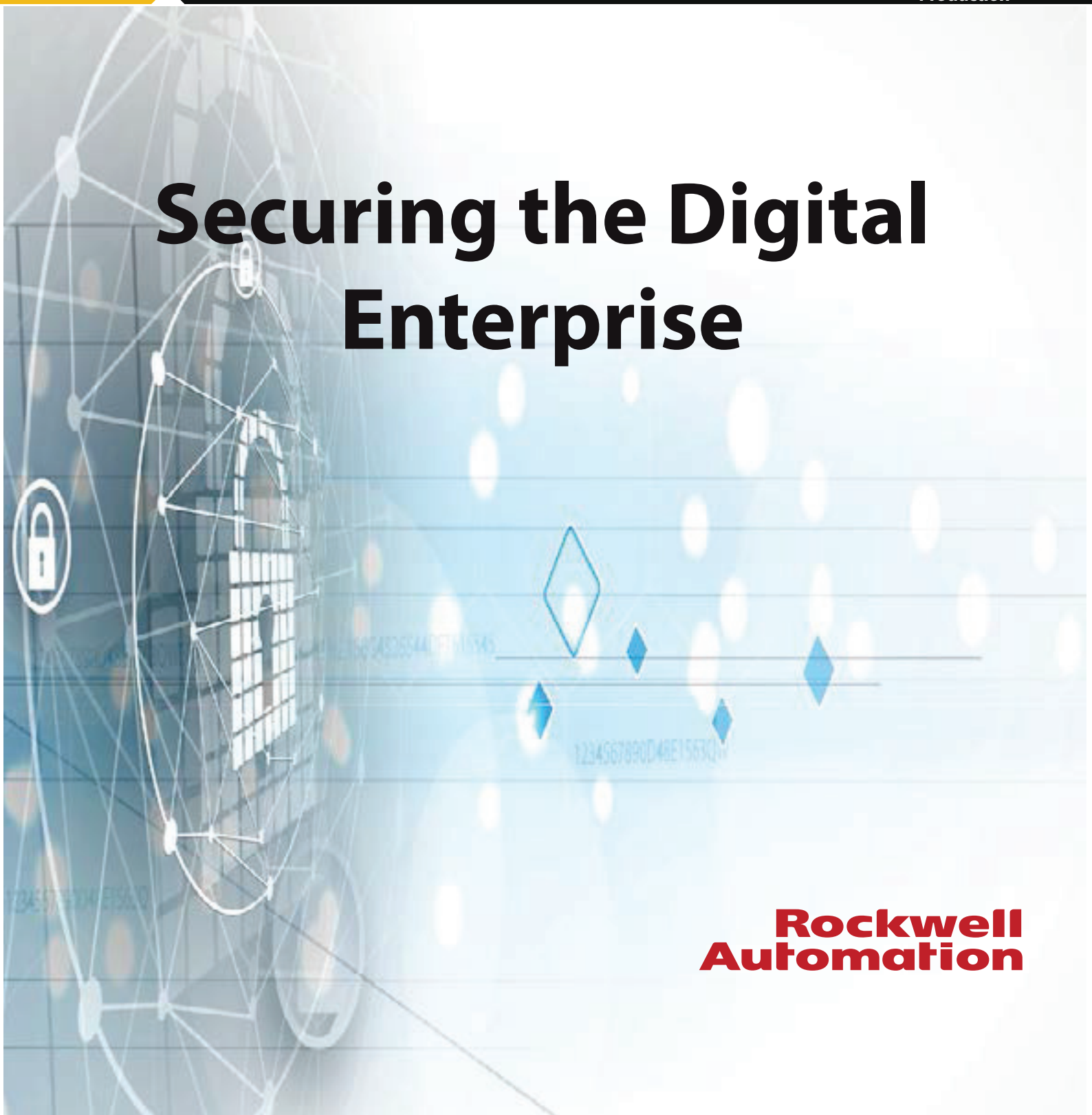
December 2018 Issue 58

Automation TODAY

South East Asia

Inside



Securing the Digital Enterprise

Rockwell Automation

Contents

Automation Today Asia Pacific
December 2018, Issue 58

This magazine is published 4 times a year by ROCKWELL AUTOMATION Inc. for Asia Pacific

This magazine is produced and printed by

Regional Headquarter in Singapore
Rockwell Automation Southeast Asia Pte Ltd
No. 2 Corporation Road,
#04-05/06, Corporation Place,
Singapore 618494
Main Telephone Line : (65) 6510 6688
Main Fax Line : (65) 6510 6699
Website: http://www.rockwellautomation.com/en_SEA

To subscribe or unsubscribe, visit :
http://www.rockwellautomation.com/en_SEA/go/ATAP

EXECUTIVE MESSAGE

Securing the Digital Enterprise

Digitalization enables a secure flow of data throughout the enterprise and supply chain, helping companies dramatically improve productivity, quality, compliance and profitability. It offers enormous opportunities to industrial companies and as a result, the race is on to digitalize from the plant floor all the way through to enterprise systems.

To be competitive, you must be connected. **Smart Manufacturing** is significantly transforming companies and their operations. But with opportunity comes increased risk. More connected operations can create more potential entrance points for industrial security threats.

Taking a holistic approach to **cyber security** is of paramount importance, especially in today's rapidly evolving digital manufacturing environment. Holistic industrial security is enterprise-wide, starting at the plant level and encompassing every individual end device.

Smart industrial devices coupled to robust and secure OT networks often fall outside of the comfort zone of traditional IT managers, so you should consider vendors that can deliver both OT and IT experience. There are plenty with experience in IT, and a fair few with OT knowledge, but experience with both is not easy to find, so you need to make an incredibly objective decision.

This issue of Automation Today dives deep into the latest technologies and industry insights related to cyber security and the **digital enterprise**. It also covers how you can embrace the benefits of digitalization while protecting your enterprise from the risks introduced by increased connectedness.

It focuses on the topics that are top of mind to our customers including:

- Security for smart manufacturing
- Changing security risks and how they can be addressed
- A step by step guide to smart manufacturing.

This issue also includes the latest products and technologies, recent company news and events and customer case studies revealing how we help customers address their application challenges.

As the technologies that enable digital transformation advance, smart manufacturing is going to continue to get smarter and new security threats will present themselves.

Cyber security needs a proactive holistic approach. So, as 2018 comes to a wrap, I hope you will enjoy this issue of Automation Today and continue the discussion about the importance of securing the digital enterprise.

We look forward to an exciting year in 2019, and wish you Happy Holidays!

Joseph Sousa, President
Asia Pacific Region, Rockwell Automation

Proven Expertise For Your Success

Leverage In-depth Experience to Achieve for Smart Manufacturing

Solution Partners, as part of our PartnerNetwork™, are comprised of global system integrators with differentiated skills and industrial experience in your domain.

Our growing community of system integrators in Asia Pacific understands your challenges, combines new technologies and simplifies system deployment with their application expertise.

This is how we bring your Connected Enterprise to Life.

Rockwell Automation Recognized System Integrator

Rockwell Automation Solution Partner

Experience the power of our PartnerNetwork:
www.rockwellautomation.com/global/sales-partners

Rockwell Automation

Rockwell Automation 2018 Automation Fair Event Unveils New Brand Platform and the Promise of 'Expanding Human Possibility,' Debuts: Innovative Solution Launches

Automation Fair 2018, hosted by Rockwell Automation and members of its PartnerNetwork on 14-15 November in Philadelphia, Pennsylvania, officially unveiled the company's new branding and shared announcements about innovative solutions for customers.

The new brand promise, Expanding Human Possibility, supports Rockwell Automation emphasis on bringing The Connected Enterprise to life and how, by connecting people, machines and data digitally across an entire organization, manufacturers can become more effective and productive.

"The new Rockwell Automation brand builds on our company's legacy and emphasizes the central role that people play in advanced manufacturing. It underscores our focus on the ways we can help businesses maximize performance, advance innovation and drive growth," said Blake Moret, chairman and CEO, Rockwell Automation. "Together with our partners at Automation Fair, we demonstrated how to bring The Connected Enterprise to life, empowering our customers to build more efficient, nimble and productive businesses."

Automation Fair 2018 saw thousands of global manufacturing leaders gather in Philadelphia to experience the latest technology and discuss industry trends impacting today's manufacturing climate such as digitization, cybersecurity, female leadership, the skills gap and STEM.

Automation Fair also saw the launch of innovative new solutions, **FactoryTalk InnovationSuite** and **MetsoMetrics**, from Rockwell Automation and its PartnerNetwork members, that are designed to create value and increase productivity by harnessing the information within organizations.

Joe Sousa, president, Asia Pacific, Rockwell Automation, commented: "The new Rockwell Automation branding underlines our single-minded commitment to bringing the Connected Enterprise to life. By combining our expertise with that of our PartnerNetwork members, we can bring to market innovative new solutions and helping customers to define their Industry 4.0 journey.

"The Asia Pacific region is extremely diverse and fast-moving. Our full range of solutions allow customers to achieve deeper insights into their business and ensure their preparation for success, whatever market they are in, and the ability to overcome the unique conditions that their business or industry may face."

FactoryTalk InnovationSuite: Following the announcement of the partnership between Rockwell Automation and PTC in June 2018, Automation Fair saw the launch of Factory Talk InnovationSuite, a new collaborative solution from Rockwell Automation and PTC offering designed to drive digital transformation across industrial enterprises.
FactoryTalk InnovationSuite, powered by PTC, improves connectivity to operational technology (OT) devices on the plant floor, natively supporting the rapid, scalable and secure connection of the most commonly used industrial equipment. Combined with data from information technology (IT) applications and systems, decision makers can now gain a complete digital representation of their industrial equipment, lines and facilities from anywhere in the enterprise.

Metso Metrics: A new predictive maintenance solution for the mining industry and a collaboration between Metso and Rockwell Automation was launched during Automation Fair. Designed to provide global mining customers improved visibility and new insights into their equipment and processes, Metso Metrics allows for deeper insights into analytics, condition monitoring and predictive maintenance.

The Industrial Internet of Things (IIoT) solution is built on the Rockwell Automation FactoryTalk Cloud platform, powered by Microsoft® Azure™. It securely collects data from hundreds of sensors within Metso equipment all used to assess process performance, as well as predict component wear and failure. Metso performance teams analyze the data with the support of advanced machine learning algorithms, to help customers optimize equipment operations and processes.

Collaborate and Accelerate - Singapore Customer Experience Center Brings the Connected Enterprise to Life

See something, and you remember 35 percent of the content.

Do something, and you retain 75 percent of the knowledge.

Seeing a concept in action is good. Experiencing that concept is that much better. At our Customer Experience Center (CEC) in Singapore, customers can do both. Established in 2018, the CEC in Singapore is an expansive state-of-the-art space. Designed to create an ideal environment that allows customers to experience the opportunities of smart manufacturing in an interactive manner, and collaborate with Rockwell Automation to innovate their future business needs.

Bringing The Connected Enterprise to Life

We have several excellent CECs around the globe. What makes this CEC unique is the way we articulate **Connected Enterprise** messaging through scenario-based demonstrations, to help customers achieve specific business outcomes.

While many customers get a brief introduction to The Connected Enterprise at high-energy (and crowded) global events like **Rockwell Automation TechED** and **Automation Fair**, visiting the CEC is a chance for a completely unique experience as the sessions are personalized for each customer.

"This CEC focuses on the individual's experience with our company," said Geoff Irvine, Strategic Account Manager, Rockwell Automation. "The tagline, 'Bringing the Connected Enterprise to Life', is exactly what happens for each customer. Customers see the Connected Enterprise journey of our own company and understand how our manufacturing operations utilize information to optimize operations. After visiting the Center, I'm amazed with how well the Connected Enterprise message is brought across."

How it works

Here, personalization means:

- Short demonstrations start the discussion. No PowerPoints, no lectures. This time is about conversation.
- Connected Enterprise applications show our offerings and capabilities in action.
- Tour aligns to five to six customer outcomes achieved through implementing our solutions (rather than focusing on a particular product or technology).

Abhay Dubey, Industry Manager, AP, added, "A global agri-business operating from seed to shelf, visited our CEC. Before the visit, they had some ideas on Connected Enterprise but did not know how the concept can be implemented.

After the demonstration and presentations, they were convinced that we are the right partner for their digitalization journey. We were then awarded a pilot project and later a similar order for an entire plant in Vietnam.

With initial success, they placed another order in Spain and sponsored two members from Singapore to visit their Spain facility to conduct a site survey for a potential long-term collaboration."

AP Customer Events Calendar Upcoming in January - March 2019

Event	City/Country	Date
Rockwell on The Move (RAOTM) 2019	Bangalore, India	22 January
Rockwell on The Move (RAOTM) 2019	Bangkok, Thailand	5 March
Cisco Live	Melbourne, Australia	5-8 March
Food Safety & Compliance Conference 2019	Auckland, New Zealand	18-19 March
Auspack	Melbourne, Australia	26-29 March
Automation World 2019	Seoul, South Korea	27-29 March
China International Petroleum & Petrochemical Technology and Equipment Exhibition 2019	Beijing, China	27-29 March

* Each event is subject to change

For more details, visit : www.rockwellautomation.com/global/events/events.page

ASIA PACIFIC EVENTS

Destination Digital: A Step by Step Guide to Smart Manufacturing

The drive for digitalization is accelerating the need for digital manufacturing plants that offer the highest flexibility, combined with reduced production costs. By enabling a secure flow of data throughout the enterprise and supply chain, companies can dramatically improve productivity, quality, compliance — and profitability.

Real-time information from enterprise and manufacturing systems can facilitate demand-based production planning that efficiently adjusts to variations in customer demand. Through digitalization, manufacturers can significantly reduce lead times and improve customer satisfaction.

The Case for Connection

To be competitive, you must be connected. That is why industrial companies around the world are undergoing a digital transformation and moving toward smart manufacturing. By creating a unified network architecture – one based on the use of standard Ethernet and Internet Protocol (IP) technology – that leverages both the information technology (IT) and operational technology (OT) that make up the Industrial Internet of Things (IIoT), companies can:

- Gain real-time visibility into operations
- Optimize production assets
- Predict downtime issues
- Improve collaboration and innovation

Start with Your Infrastructure

The true value of smart manufacturing can only be realized if a secure and reliable information infrastructure is in place. Unfortunately, the production systems that many companies are using today were not designed for connectivity. This has created islands of data and automation, which makes it more difficult for companies to understand their operational and cyber security risks.

Furthermore, the security-related concerns that are associated with greater connectivity have made some companies hesitant to begin the process of connecting their systems.

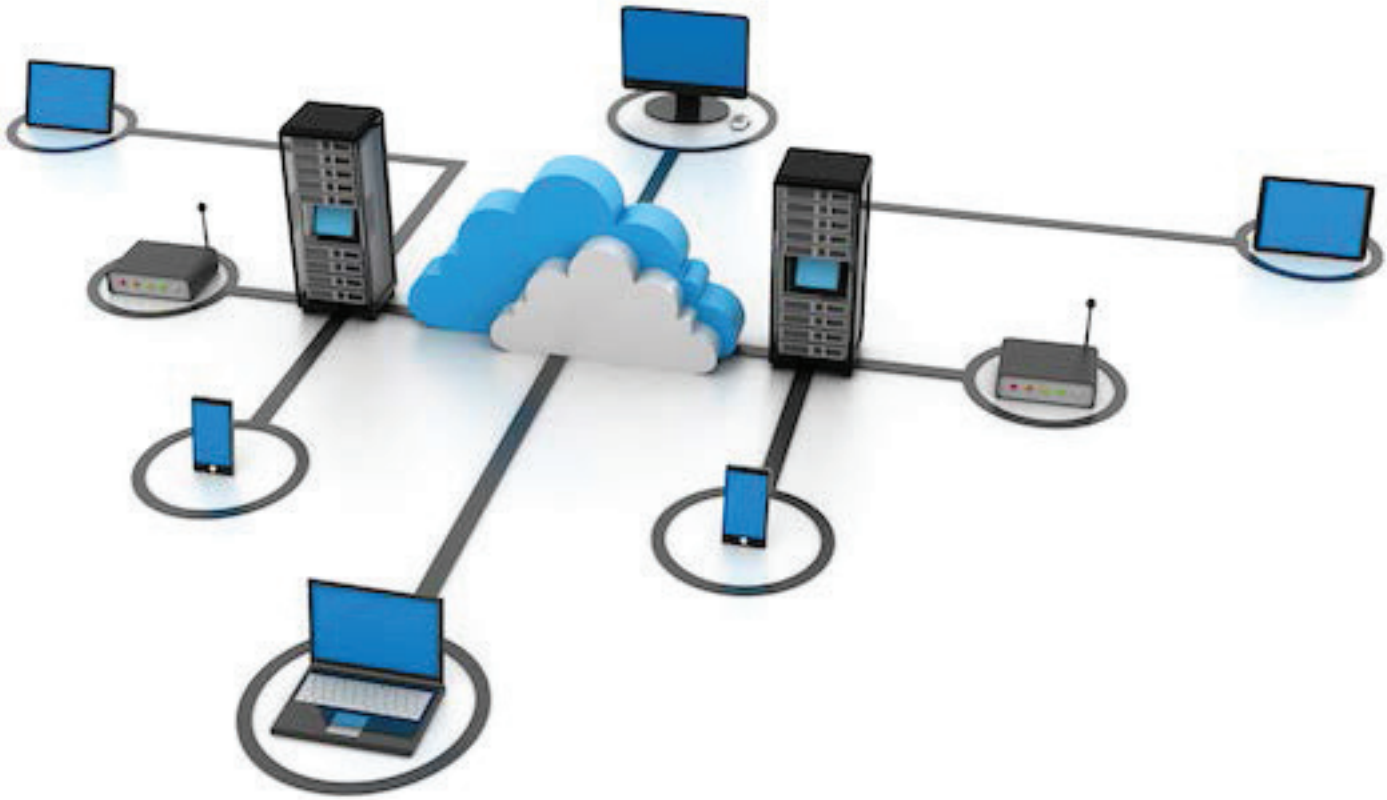
The good news: With the right focus and support, you can simultaneously manage risks, and address performance and security needs as you build and manage your information infrastructure.

A modern, secure and reliable information infrastructure connects your assets, people and information. It is central to everything you do. It is the source of endless opportunities for improving your operational performance.

"Having connected terminals allow us to respond more quickly to changing market conditions without compromising our way of running our terminals." – BulkLiquid Storage Company

A Journey Toward Connection

Smart manufacturing delivers value through tighter integration between industrial assets on the production floor and the rest of the enterprise value chain. This tighter integration requires a secure network infrastructure and accessible data that can be managed



under a common system. It also contextualizes data from the production environment to turn it into information that can be shared.

There are four stages to deploying this type of connection:

1. **Assess and Plan:** A comprehensive assessment will establish to what extent your infrastructure can be upgraded, or if it needs replacing
2. **Secure and Upgrade:** Securely upgrade your network and controls to facilitate communications between plant-floor and enterprise systems in line with your company's business drivers and risk tolerance
3. **Manage and Analyze:** Define and organize data, and turn it into actionable information that can be more easily viewed and securely shared for continuous operational improvements
4. **Optimize and Collaborate:** Optimize your operations and drive collaboration across your teams, suppliers and customers.

The process of creating a secure information infrastructure that can deliver on your needs is woven into these four stages. Each company's transformation will have its own unique considerations.

"Our new remote capabilities have significantly reduced troubleshooting time and costs." – Supplier of Rail-maintenance Machine

Mapping Your Journey

Every path to smart manufacturing will be unique based on production goals, connectivity and security needs, and the production infrastructure currently in place in your facilities. However, there are four key questions to ask as part of any plan:

1. What performance goals do I need to achieve?
2. How do I assess, design and implement the secure infrastructure that I need to achieve my goals?
3. How will I protect and maintain my infrastructure?
4. How can my infrastructure help improve the performance of my devices and system in a way that will continue to deliver on my performance goals?

What Are My Performance Goals?

Your production goals will drive your information infrastructure strategy. These goals may require specific operational improvements such as gaining real-time visibility into operations, including KPIs and asset performance; optimizing asset utilization and worker productivity; improving collaboration, whether it is between plants or with outside partners; reducing risks that are related to safety or the industrial skills gap.

It's important to know your goals as they will drive your requirements. Some performance benefits producers can expect from an improved information infrastructure include:

- Multi-discipline application convergence
- Improved asset utilization
- More common toolsets, required skills, and training for your workforce
- Standardized IT security technology, policies and procedures
- Seamless information sharing

Whatever your goals, they will rely on a robust and secure Converged Plantwide Ethernet (CPwE) network architecture and should be formalized into a plan with a defined scope, timeline, budget and related security considerations.

How Do I Assess, Design and Implement the Right Infrastructure?

Once you have defined your goals, you must next determine your infrastructure needs in order to reach those goals and maximize ROI. This process has three key phases:

1. Assess

Infrastructure assessments help determine if your networks meet your needs and align with industry best practices. Risk and vulnerability assessments also help uncover security gaps and prioritize necessary updates so you can improve your security posture and reduce risk.

2. Design

Your information infrastructure should be designed to: Drive optimal network performance; Mitigate security risks; Increase data availability and use; and provide a foundation for future technologies.

Pre-engineered solutions can help drastically reduce design time and risk for some aspects of your infrastructure. Infrastructure-as-a-Service (IaaS) can be supplied as a complete and installed system, reducing your capital expenditures. Industrial Data Centres (IDCs) are pre-engineered solutions that provide all the hardware you need for a virtualized infrastructure. They can be less costly, less complex and less time-consuming than building a solution from the ground up.

3. Implement

Your implementation must meet the needs of both your IT technologies and OT environment. It should also aim to simplify and accelerate your infrastructure's deployment.

Connected Services from automation vendors can help you:

- Shorten infrastructure projects timelines by up to 50 percent
- Reduce future industrial IT CAPEX by up to 67 percent
- Reduce OPEX by up to 33 percent

How will I Protect and Maintain My Infrastructure?

Enlisting a traditional IT company to support your information infrastructure can be risky, as IT vendors typically do not have enough expertise in industrial environments or plant-floor priorities to meet requirements for the quick response times that minimize downtime.

But enlisting the support and counsel of industrial vendors who understand the needs and demands of OT environments is a valuable means of supporting blended IT/OT applications.

"Now, we can produce hard data that demonstrates how our pumps and other components last longer. We can use hard data in warranty fulfillment. We can alert our customers when it is time to swap out air filters or come in for an engine rebuild. The possibilities seem endless." – Heavy Equipment and Machinery OEM

Manufacturer Makes the Switch to OT Support

A major food producer that deployed Ethernet and managed switches on its plant floor struggled with the support provided by its traditional IT vendor. The vendor couldn't respond with the speed required to keep production moving.

As a result, the manufacturer switched to an automation vendor for support. The new vendor set up monitoring of 400 switches, which included alarm profiles for eight key parameters in every switch. SLAs established alarm-response times of 10 minutes.

Since making the switch, the manufacturer has seen a significant improvement in uptime and a decrease in downtime events.

How Can My Infrastructure Help Improve Asset and System Performance?

Your goals may also require the implementation of new capabilities that are related to system or asset-performance management.

With a secure and robust information infrastructure, you now have the connectivity that is required to tap into strategies that can boost your bottom line. Large amounts of data lives within your production assets, but it needs to be transformed into useful information to drive performance improvements.

Asset Reliability services combine a mix of industry expertise and electrical automaton controls knowledge with continuous improvement processes, reliability techniques, and asset intelligence systems to help drive plant productivity, improve asset reliability over your equipment lifecycle, and streamline maintenance activities.

Preventative Maintenance service agreements can keep your critical assets running at peak efficiency. From identifying pending system failures to recommending which components should be repaired or replaced, these services can help mitigate the unnecessary repairs and associated costs that occur with most time-based preventative maintenance programs.

Remote Monitoring services can reduce Mean Time To Repair (MTTR) by 76 percent and reduce the cost of managing your infrastructure.

Analytics services can help you predict machine failures, reduce Mean to Between Failure (MTBF), and automate maintenance activities to reduce downtime by up to 30 percent.

Such services also have value beyond day-to-day process improvements and issue resolutions. You can use access to insights to optimize your larger operations and transform how you do business, reduce downtime recovery, help integrate your supply chain, design material orders to automatically replenish after a certain number is met, or even build customized dashboards to view production data and asset or system health that is most important to your specific needs.

"We've seen how the right control and information infrastructure can turn data into information. Contextualized, that information becomes knowledge that improves accountability and collaboration." – Equipment Supplier

The digital transformation of manufacturing is rapidly connecting the plant floor with the entire enterprise and beyond. Digital operations allow machines to communicate and collaborate, while providing real-time data to improve both plant processes and the products they create.

It's is a good time to give some thought to what may be holding back your company's digital success and how can you take the right steps to address these. At

Oil and Gas Producer in India Maximizes Critical Equipment Uptime and Improves Maintenance to Keep Product Flowing

Vibration monitoring system from Rockwell Automation reduces downtime

Background

A swelling middle class in India has created growing market demand for and increased consumption of petroleum products.

This oil and gas producer is one of India's largest petroleum product manufacturers and distributors, with a processing capacity of 6.5 million metric tonne per annum (MMTPA).

The plant must steadily keep petroleum products pumping through the station because any unplanned downtime can cause critical product shortages.

Contributing to the ability to reach zero unplanned downtime is healthy equipment, like pumps, achieved through maintenance and monitoring.

The company's pipeline supplies the interior areas of India. Seven pumping stations along that pipeline already used Rockwell Automation for several years with almost no downtime. The goal is to maintain and even improve that performance.

Challenge

The biggest challenge for this customer is timely distribution and accurate pumping of products 24 hours a day, seven days a week. Any disruption could increase refinery inventory and leave retail units without adequate supply.

To maintain continuous flow, each pumping station uses three pumps: Two are at work at all times to maintain line pressure across the pipeline to the next terminal. The remaining pump is on standby in case one of the other pumps fails.

Oil pump operation is precise. Undetected or unreported wear and tear on the pump is not acceptable because even the slightest shift in pump operating parameters can cause damage. An aging Bentely Nevada 3500 system, installed years ago, did not function, and there was no ability to communicate with the station PLC to identify and rectify system faults.

Solution

To reduce the number of systems it needed to maintain, the customer preferred a single system (and a single system supplier) that worked with their control system, HMI and the machine monitoring system (MMS), and offered continuous and reliable support. Since continuous operation is required, this customer could not shut down the system for a switchover. The company requires seamless integration of this system, including the MMS, with existing systems.

Given the scope and complexity of the requirements, the customer wanted a supplier with proven skills, experience and support and selected Rockwell Automation for the company's extensive experience in automation and global support. With a local office and authorized distributor just five kilometers from the site, Rockwell Automation had the required expertise to manage the requirements of the project, from initial design through engineering, integration and implementation.

Optimize Production, and Improve Profitability

Effective solutions for the terminal included seamless integration on a single **EtherNet/IP network** with the flexibility to configure parameters using the existing graphic user interface. Separate training was not required so the new systems were easily accepted by the operations team.

Rockwell Automation Global Solutions implemented a vibration monitoring solution that:

- Interfaces with existing systems to monitor vibration data of the pumps, and alert operators of any abnormal situations.
- Allows operators/engineers to easily set parameters and provides trending, alarming, and exception handling.
- Works with existing equipment, including probes and sensors, by ensuring compatibility.
- Offers the plant manager complete and accurate information in real-time.

The solution is built on:

- **Dynamix™ 1444 Condition Monitoring System** using a common control system, **ControlLogix® L72**, with a common development environment to provide high performance in an easy-to use environment. The system's tight integration between the programming software, controller, and I/O modules reduced development time and cost at commissioning and during normal operation.
- **Logix5000™ controllers** and Add-on Instructions (AOI) to increase productivity and make troubleshooting easier.

Results

With this solution and the integration of various OEM control systems to enable plant wide visibility and real-time monitoring, Rockwell Automation helped this customer reduce the risk of critical equipment failure.

Reduce risk of critical downtime by 20%

At the same time, the solution improved the ability of operators to monitor conditions and immediately address concerns before problems turn into downtime. The solution ensures that any abnormalities in the process conditions and deviation from the standard operating parameters will be immediately highlighted to avoid problems and improve reliability.

As a result of implementing the Rockwell Automation vibration monitoring system, the customer reduced the risk of downtime by 20 percent, and also reduced its dependency on multiple vendors. The flexible graphic user interface helped reduce operator training time and expense.

The next iteration of the solution could include the ability to create real-time dashboards for production and utility data.

The results mentioned above are specific to this customer's use of Rockwell Automation products and services in conjunction with other products. Specific results may vary for other customers.

Jim Beam Modernizes for Increased Production and Maintains a Tradition of Quality

Jim Beam implements Model Predictive Control at Clermont, Kentucky Distillery

Background

The Jim Beam Distillery in Clermont, Kentucky has been producing some of the world's finest spirits for more than 75 years. At Clermont distillery, over 90 million bottles of spirits are produced annually and shipped to more than 200 countries worldwide. A number of leading bourbon brands are distilled at the facility: Jim Beam Bourbon, Jim Beam Black, and the ultra-premium Small Batch Bourbons: Basil Hayden, Knob Creek, Baker's and Booker's.

More than 600,000 barrels of bourbon are aged in the 27 rack houses on the distillery grounds making the Jim Beam Clermont plant one of the largest in North America.

Process

It is said that for bourbon, 100 percent of the color and 60 percent of the flavor comes from the barrel. The other 40 percent of the flavor results from the grains in the mash bill, the yeast, the fermentation conditions and the distillation proofs of the low wine and the high wine. Maintaining the low and high wine proofs, ensures that the desired congeners, substances, other than alcohol, produced during fermentation that affect the flavor, are preserved in the high wine, while undesirable congeners are removed.

The grains listed in the mash bill are cooked and then fermented using yeast to produce "distiller's beer". This distiller's beer, which is about 9 percent alcohol is fed to a continuous, multi-stage, column still called the beer still, where the alcohol is concentrated in the vapor leaving the top of the column. The vapor is condensed and the resulting "low wine", which is about 60 percent alcohol or 120 proof, is stored in the retention tank.

The remainder of the distiller's beer leaves the bottom of the still as

"thick slop". The low wine goes through a final, single stage of distillation in the "doubler". The vapor from the doubler is condensed and the resulting "high wine", which is about 65 percent alcohol or 130 proof, is stored in cisterns until it is diluted or "proofed" to the desired concentration before being put into new, charred, oak barrels.

To avoid losing any alcohol, the side streams collected from the beer still, the bottoms from the doubler, as well as other waste streams from the distillery are collected in a tank and fed to a small column still, known as the "heads and tails still". The alcohol is concentrated in the vapor leaving the top of the still and is condensed with the low wine.

Challenge

In the last few years, there has been a boom in the worldwide consumption of bourbon whiskey. Jim Beam was looking to modernize sections of their facility to maximize throughput while respecting equipment and process constraints. In order to achieve this objective, reductions in process and quality variance would be required to allow the plant to push closer to their operational limits, increasing throughput while maintaining product integrity. The application will provide real-time model predictive control through the implementation of the technology components.

Solution

The **Pavilion8 Controller** implements multivariable control with constraint handling, feed forward, decoupling and dead-time compensation. Process models are used to optimize controller actions. Where conventional Model Predictive Control (MPC) uses linear models, The Pavilion8 Controller allows nonlinear models to be used.

The Pavilion8 Controller calculates recommended set points for lower level process control loops, typically PID loops, to optimize real-time control performance. These controllers can be placed on or off MPC control by the board operator. More complex strategies may be implemented by configuring one Pavilion8 Controller to write set points to another Pavilion8 Controller's controlled variables.

Stable Distillery Operation, Better Product Quality & Improved Distillation Yield

The Application for Jim Beam

- Maximizes feed to the beer still to increase throughput, up to the process and quality constraints
- Manipulates the steam and reflux flows to the beer still to maintain the low wine proof and ensure that no alcohol is lost in the thick slop
- Manipulates the steam flow to the doubler to maintain the high wine proof
- Manipulates the steam flow to the heads and tails still to ensure that all alcohol in the collected streams is recovered
- Manages the material flows through the distillery to maintain the material balance (tank levels, etc.) freeing the operators to focus on more complex tasks

The Results

- Allows operators to focus on high value tasks
- 60% Decreased Variability while Maintaining Proofs
- Stable Distillery Operation, Better Product Quality & Improved Distillation Yield

Security for Smart Manufacturing

For all the benefits that smart manufacturing can offer, it also requires a more comprehensive approach to security. Seamless connectivity and smart devices are the catalysts to smart manufacturing – but they can also be a conduit for security threats.

The growing use of widely available technologies in industrial control systems and the growth of more connected, information-enabled enterprises inherently increases security risks, and with it the responsibilities of control system providers and users alike.

Historically, industrial control systems used proprietary technologies and were generally segregated from the information systems at most companies. The systems were largely incompatible and the commercial technologies that were used in office spaces simply didn't fit the requirements of control systems.

As commercial technologies advanced in recent decades, they were adapted for use in control systems, improving costs, compatibility and ease of use. With these improvements, connectivity between systems became simpler and increasingly demanded by users.

Bringing together enterprise-level IT and plant-level operations technology into a common infrastructure creates more opportunities to improve operations, but without proper cyber security hygiene may also provide increased opportunities for cyber-attacks against industrial control system equipment.

Such attacks, if successful, can have severe impact on worker, environmental and product safety, intellectual property, reputation and productivity. Attacks on control systems have increased dramatically in recent years. Global cyber-attacks – like WannaCry and Petya – affected thousands of targets and networks around the world.

Leading industrial control system providers constantly test products and review applications to identify and remediate vulnerabilities in products. Disclosing remediated vulnerabilities through patch and version management helps protect against cyber-attacks.

At Rockwell Automation, this is part of an ethical and comprehensive cyber security strategy to help verify customers' security and safety. While this is not actually new, the increased focus on security in recent years and the more frequent disclosures may seem surprising to some. To others that have worked closely with IT, it will seem natural and expected. To all, it should be welcomed as a clear focus on supporting the safety and security of industrial control systems.

Mitigating Security Threats with Network Segmentation

An open and unsegmented network is a gift to cyber attackers. Once an attacker finds and exploits the most vulnerable point of entry, it could turn into a potential 'kid-in-a-candy-shop' scenario. They may be able to pivot to more easily access a larger part of the network and potentially anything connected to it – from product designs or recipes, to machine controls, to company finances.

It's important to note that it's not only external threats that pose a danger on an unsegmented network. Internal threats, whether it's a disgruntled employee or human error like an incorrect system change, also can wreak havoc when there are no network boundaries or access limitations.

This is why network segmentation should be part of every company's industrial security strategy. Network segmentation separates your network into multiple smaller networks and allows you to establish zones of trust. This can help limit the access of outside security threats and contain any damage they cause. It can also help give employees and business partners access to only the data, assets or applications they need.

Virtual LANs (VLANs) are most commonly associated with network segmentation. These are broadcast domains that exist within a switched network. They allow you to segment your network logically – such as by function, application or organization – instead of physically.

VLANs can secure devices and data in two ways. First, you can block devices in certain VLANs from communicating with devices in other VLANs. Secondly, you can use a Layer-3 switch or router with security and filtering functionality to help to protect the communications of devices that do talk to each other across VLANs.

While VLANs are an important part of segmentation, they're only one solution. You could also use other segmentation methods across different levels of your network architecture.

One example is the use of an industrial demilitarized zone (IDMZ). It creates a barrier

between the enterprise and manufacturing or industrial zones. All traffic between the two zones terminates at this barrier while still allowing data to be securely shared.

Other segmentation methods to consider using include access control lists (ACLs), firewalls, virtual private networks (VPNs), one-way traffic restrictors and intrusion protection and detection services (IPS/IDS).

Cyber Hygiene for Food Manufacturers

Food manufacturers are reaping benefits from the convergence of operations and information technology – through increased yields and deeper, real-time insight into KPIs. They're moving into a bright manufacturing future.

However, providing access to information changes the threat landscape for food manufacturers. This territory is shaped by malicious hackers, as well as virtuous employees who are all too often unfamiliar with the impact of their seemingly everyday actions. The resulting dangers range from product contamination to loss of intellectual property.

The good news is that food and beverage companies are getting better a basic cyber hygiene. That approach starts with not just understanding what is connected on your plant floor, but understanding its attack surface. In other words, what are those assets' vulnerabilities? Then use that knowledge to patch them.

How can you secure your infrastructure, protect assets and maintain network availability?

Successfully implementing basic cyber hygiene are the first steps in building an effective cyber security program and improving your ability to defend against future cyber-attacks. To help minimize your risk, consider a security program based on four key areas:

1. Maintain an asset inventory with an emphasis on understanding the attack surface or vulnerability.
2. Manage vulnerability, patch and configuration. Have programs in place to address known vulnerabilities, patch regularly and have mature processes around how configuration changes are made and tracked.
3. Employ backup and recovery mechanisms for all critical assets to verify you have the ability to quickly pull from a known good backup.
4. Complete regular risk assessments to measure risk and manage it. Use the assessments to show your organization the level of risk they are exposed to and the resources – time, money, and people – needed to mitigate it.

Digital transformation provides an advanced network backbone, which minimizes security risks while supporting scalable execution, analytics and supply-chain connectivity. As such, an investment in IIoT technologies in compelling because it delivers insights that improve performance now, while also implementing a security architecture.

Looking at the digital journey of our customer, Hamlet Protein, provides a great example of how a successful transformation occurs.

Hamlet Protein, Inc., a mid-sized company located in Denmark that develops and manufactures soy-based functional ingredients for use in animal feeds. The company has identified seven key steps crucial to the success of their digital transformation:

1. Create and socialize **a shared company vision** among C-level stakeholders.
2. Establish a **steering committee**.
3. **Partner** with a technology provider **who** understands and **supports** your **overall business objectives**.
4. Carefully and completely assess your company's operations to **develop** an **unvarnished picture of strengths, gaps and opportunities**.
5. **Conduct a value workshop** to secure buy-in and evaluate potential gains against the picture developed in step 4.
6. Develop and socialize a **comprehensive plan and schedule**.
7. **Establish an infrastructure for change management** and inter-company communication.

Whether you're just embarking on or are already on the path of your own digital journey, you may find the following resources useful:

- Learn more, including Rockwell Automation's own journey: Journey to the Connected Enterprise
- Share your thoughts and join the discussion: Intelligent Manufacturing Institute group
- Follow us for new information and updates: https://twitter.com/ROKInfoSolution

Security Risks are Changing – Are You Protected?

●●● Greater connectivity and information sharing – enabled by technologies such as smart devices, inspired by concepts like the Internet of Things, and brought to life in **The Connected Enterprise** – are significantly transforming companies and their operations.

They're converging information technology (IT) and operations technology (OT) systems and using new technologies such as mobile, analytics, cloud and virtualization to do more than ever before.

This increased level of connectedness allows manufacturers to benefit and address challenges that more traditional models and operating practices were not able to offer. Vast data streams are acquired, processed and transmitted often in real time. However, it's these very streams of data and interconnectedness that are putting industry at risk.

Just as the nature of manufacturing and industrial operations has changed, so have the security risks. More connected operations can create more potential entrance points for industrial security threats. These threats can come in many forms – physical or digital, internal or external, malicious or unintentional.

Taking a Holistic Approach to Cyber Security

Holistic industrial security is enterprise-wide, starting at the plant level and encompassing every individual end device. Taking a holistic approach to cyber security is of paramount importance, especially in today's rapidly evolving digital manufacturing environment. It addresses risks from all sides: people, processes and technologies. In addition, it brings together IT and OT teams, both of which are indispensable in securing **network architectures**.

Forward-thinking companies use strategies and tactics to manage risk and help minimise or mitigate threats. Physical security strategies are no longer enough to protect operations. Today, manufacturers also need to understand and assess their industrial cyber security requirements and take a proactive approach to managing risks.

Proactive Threat Hunting

You may have a strong **industrial security program** in place and have implemented intrusion detection systems to avoid future incidents. But in the complex world of cyber security, you can't stop there.

Despite all your efforts, latent advanced persistent threats (APTs) are still a concern. They are slowly at work trying to find chinks in your armor and exfiltrate data, bogging down your operations, and intrusion detection isn't going to catch this activity.

Threat hunting is one of the next logical steps in your cyber security program. In its simplest form, you are searching the network for external threats or intrusions that went undetected by automated security systems. It is a very scalable exercise and can be done with varying degrees of automation, including none at all.

It can not only further protect your proprietary recipes and information, but has great potential for improving operational efficiencies as well. While this practice isn't entirely new to the IT space, it is making its way into OT environments.

Threat hunting is proactive, and takes a step back from the scanning tools, traps and future-focused infrastructure already in place. In an age of technology, it uses gray matter to uncover malicious activity and infiltrations that have been hiding in your network for months, maybe years. Further, it can find correlations not otherwise detectable between network activity and production inefficiencies.

The good news is, you likely have what you need to get started. Your HMIs and servers are already creating activity logs you can gather and analyze offline so there's no stress on the network or production interruptions. Go hunting for infiltrations before they impact your plant floor.

Protecting Critical Infrastructure

Analogous to the pharma industry, critical infrastructure such as power plants are an obvious target for security threats.

As a result, any company that generates power must be especially vigilant when it comes to understanding evolving cyber security threats. It is imperative that **power producers** keep current on the latest processes and solutions that can be implemented to combat these threats.

As cyber security threats significantly increase each year, what can you do to help protect your operations?

Security Assessment: Power producers must cultivate a deep understanding of all risks and vulnerabilities that exist within their organization. A security assessment offers a fresh and thorough review of site infrastructure nuances, software, networks, control systems, policies, procedures and even employee behaviors. It's the foundation for a successful security policy.

Key deliverables for a security assessment include:

- Inventory of authorized and unauthorized devices and software
- Detailed observation and documentation of system performance
- Identification of tolerance thresholds and risk/vulnerability indications
- Prioritization of each vulnerability based on impact and exploitation potential
- Mitigation techniques required to bring an operation to an acceptable risk state

With an assessment in hand, implementation can begin.

Defense-in-Depth Security

Defense-in-Depth (DiD) is based on the idea that if any one point of protection is defeated, additional layers will subsequently need to be defeated. Therefore, DiD security establishes multiple layers of protection through a combination of physical, electronic and procedure safeguards. A DiD security approach consists of six main components: policies and procedures, physical security, network, computer, application and device.

Trusted Vendor

Your plant's automation system is likely a small part of capital assets or costs. However, it can have a disproportionately large impact on helping you meet your security goals – similar to the impact it has on your production, quality and safety goals. Before selecting vendors for any system that will be connected to your network, request that they disclose their security policies and practices.

Rockwell Automation has a strategic partnership with Cisco to better understand evolving cyber security best practices and have defined five core security principles for designing products used in a control system:

- Secure network infrastructure
- Authentication and policy management
- Content protection
- Tamper detection
- Robustness

Power generators should look for a structured and tailored approach to meet physical and cyber security requirements. Multiple layers of protection, a highly integrated cyber security suite and other upgrades can help producers get ahead of risks already running throughout the industry. At

As cyber security threats significantly increase each year, what can you do to help protect your operations?

Latest Release of Studio 5000 Optimizes Productivity and Reduces Commissioning Time

The Studio 5000 design environment combines engineering and design elements into one standard framework that enables optimized productivity and reduced commissioning time – helping engineers design, build and commission automation systems more quickly.

The latest release of Studio 5000 includes major updates to both Logix Designer application and Application Code Manager. Logix Designer now supports AutomationML for data exchange along CAD tool chains. The enhancements for Studio 5000 Logix Designer includes a 64-bit math instruction support, new intuitive FBD Functions and Alarm Library Management improvements.

The new release of Studio 5000 Simulation Interface enables the integration of simulation tools to help build a digital twin to better design and validate systems. ControlFLASH Plus latest release allows users to manage their devices lifecycle natively and increases productivity by updating multiple devices simultaneously.

Focused on optimizing productivity, increasing efficiency and simplifying workflows, the Studio 5000 v32 software release helps you to respond more quickly to changing market and business needs while reducing total costs.

FactoryTalk Analytics for Industrial IoT Applications

Industrial organizations must be able to quickly identify ways to tighten production schedules and maximize revenue. The expanded FactoryTalk Analytics platform enables scalable analytics from edge to enterprise. The latest updates to the FactoryTalk Analytics platform include:

FactoryTalk Analytics DataView Version 2.1

FactoryTalk Analytics DataView empowers you with faster insights through self-service, and intuitive storyboards you can create with one click. It enables rapid horizontal data integration, enterprise-level security, performance and scalability combined with strong manageability in a collaborative and mobile environment.

The latest release increases visibility, improves productivity and enhances efficiency by providing quick insights to your line, shop floor, plant and enterprise. It does not matter whether data comes from one system or from multiple disparate systems like PLC, DCS, Historians, MES and Enterprise applications. Through a simple self-service four-step process, you can annotate data, add context, mash it with other data and generate storyboards to get insights immediately.

FactoryTalk Analytics Data Explorer

The first step in analytics is gathering data, aligning different data sources and preparing it to learn about a system, problem or process. Machine Learning algorithms are powerful new tools to develop useful models to improve manufacturing. However, frequently there is insufficient aligned data from diverse manufacturing systems, problems with data or significant periods that are irrelevant to the task at hand. In addition, there can be data management issues, such as excessive compression.

With FactoryTalk Analytics Data Explorer software you can visualize and graphically interact with the data to observe and detect issues. Data Explorer provides an array of tools to clean, align and interpolate, and enrich data with known concepts, and identify observable lags or helpful time-shifts in the data. An informed user can then identify useful correlations to detect new process/system influences and causes.

FactoryTalk Analytics Real-Time Optimization

FactoryTalk Analytics Real-Time Optimization (RTO) software enables process operators to consider cost to drive optimal utility equipment dispatch to support intelligent make/buy, generation and loading decisions. Energy savings on the order of 10-30 percent are typical from dispatch optimization on parallel centralized utility equipment.

RTO provides predictive optimization by modeling process behavior and applying automatic control based on defined variables and constraints within the system. Based on actual operating data, the RTO application understands the relationships between equipment selection, loading and energy costs and self-maintains mathematical algorithms to predict accurate outcomes before actual events.

FactoryTalk Analytics Edge Version 2.2

To improve decision-making, you need to gather insights as closely as possible to devices, data and those who consume them. That is when the smallest of decisions make the biggest impact on process, time and material management. FactoryTalk Analytics Edge provides data capture, transformation and analytical capabilities, including predictive machine learning, right on the edge.

Quickly assemble and organize your plant-floor data for analysis. Locate and correct sources of inefficiencies quickly to control manufacturing yield, overall equipment effectiveness and other factors that matter to your business outcome.

ThinManager Software Helps Build The Connected Enterprise

●●● ThinManager thin client software helps manage information and streamline workflows for a more connected manufacturing environment. It allows centralized configuration and management of deliverable content to any combination of user, device or location.

The latest version continues to improve visualization, security and usability by offering several new features that enhance the end-user experience and increases the security of accessed content managed by the platform. With the feature of facial recognition technology, this adds as an additional authentication method for ThinManager users.

In addition, users can activate ThinManager using the traditional method or take advantage of FactoryTalk Activation. FactoryTalk View SE users only need one client license to deliver as many sessions to a single terminal. This increases support and licensing improvements between ThinManager and FactoryTalk View SE solutions which saves our customers more time and simplifies the licensing requirements for building The Connected Enterprise.

With enhanced localization to increase usability of the platform for customers in non-English speaking regions around the globe and MultiMonitor enhancements to support up to seven monitors on a single terminal – ThinManager software version 11 easily scales to expand your digitalization efforts across multiple

Latest FactoryTalk AssetCentre Improves Productivity, Quality and Security

●●● Today's industrial environments are becoming increasingly automated and connected. With the hundreds or thousands of industrial assets in an IIoT world, there is a growing need to maintain, protect and report on the automation assets in a Connected Enterprise.

FactoryTalk AssetCentre provides you with a centralized tool to secure, manage, version, track and report automation-related asset information across your entire facility. The latest release includes an update with IPSec adoption that supports encrypted communications, and FactoryTalk Linx integration that enhances disaster recovery.

Now, you can create schedules to back up the infrastructure of your equipment with Stratix fully managed switches. Additionally, with extended third-party asset support, customers can script solutions for third-party software to execute disaster recovery remotely. With asset extended properties, you can add up to 20 custom description fields to your assets.

Downtime can be costly. FactoryTalk AssetCentre supports native disaster recovery of FactoryTalk View SE software distributed assets, allowing for version management and backup scheduling of FactoryTalk View SE software network applications.

The FactoryTalk AssetCentre v9 release is focused on improving productivity, quality and the security of your automation systems.

To support additional lifecycle content, FactoryTalk AssetCentre now includes I/O for the PLC, SLC, MicroLogix, CompactLogix and ControlLogix controllers.

Pavilion8 Software Release Includes New Tools and a Modern User Experience

●●● The Pavilion8 Model Predictive Control software provides the tools to improve the agility of your operation, giving you the capability to more quickly adapt to changing business priorities and customer demands. Leveraging a powerful modeling engine, Pavilion8 software includes modules to control, analyze, monitor, visualize, warehouse, integrate and combine them into high-value applications.

Pavilion8 Model Predictive Control (MPC) version 5.16 is the latest release of the Rockwell Automation advanced process control solution that includes the next major migration of legacy tools into a modern Windows user experience.

A major part of the original Pavilion technology platform – dataset preprocessing to merge, clean up, enrich and prepare for modelling – is now integrated with the already migrated MPC and Software Continuous Emissions Monitoring (CEM) tools into one platform with a common user interface, SolutionBuilder.

A new toolset to support, track and enhance Console reliability is an independent performance monitoring application in the latest update. Users can also track and identify the major system resource consumers and isolate issues by trends and averages of usage.

System security was improved with release version 5.15, but we remain on a planned path of enhancements, because software security is a high priority with our customers and Rockwell Automation. Pavilion8 version 5.16 is the best-in-class secure software for model predictive control and environmental solutions.

Pavilion8 software is designed to meet the most demanding needs of todays' process manufacturers and addresses industries as diverse as polyethylene, cement, ethanol, milk powder, and paper.

Rockwell Automation Introduces The Connected Mine

Mining companies benefit from improved visibility of processes, equipment performance and supply chain for smarter business decisions

Like many cyclical industries, mining is reviving, driven by steady global economic growth and an increasing demand for materials to support new technologies like electric vehicles, renewable energy and mobile devices. Despite the optimism, the industry still faces major operational challenges including process efficiencies, cost control, worker health and safety and skills gaps.

To address these challenges, Rockwell Automation introduced The Connected Mine, leveraging the latest enabling and digital technologies.

Utilizing advanced analytics, The Connected Mine helps mining companies collect and aggregate data to gain end-to-end visibility into their operations and make informed business decisions to improve mining operations.

"One mining company improved production at a mine site by almost 15 percent by implementing a simulator that provides operators real-time recovery targets that are automatically updated based on ever-changing feed grades," says Fabio Mielli, market development manager, Rockwell Automation. "The Connected Mine concept provides our global mining customers with the digital infrastructure needed to tap into exciting new technologies for optimized operations."

The Connected Mine can improve all areas of mining operations:
Extraction: Connecting and automating your mobile assets and mine infrastructure – such as mine machinery and ventilation – helps to make the extraction process safer and more efficient.
Process Management and Optimization: The Connected Mine automates, controls and optimizes mineral processes and metal refining operations, helping achieve greater throughput, enhanced recovery and better quality – all while reducing energy, water and reagents.
Material Handling: Smart machines like hoists, conveyors and stacker reclaimers improve material handling by providing unprecedented access to data that can be collected, logged and analyzed to help workers make better decisions.
Mine Electrification: A digital electrical system helps to enable seamless integration of power distribution, motor management and process control and captures the information needed for predictive maintenance and remote monitoring.
Asset Performance: Whether device-based or enterprise-wide, machine learning and scalable applications that monitor the performance of critical assets and predict failures can help reduce equipment downtime.
Worker Safety and Efficiency: Real-time mobility and augmented-reality tools deliver timely, enhanced visibility to field workers, helping to confirm the right personnel have the right information at their fingertips.
Mine-to-Market Integration: A powerful analytics platform provides full visibility of the business, removing information silos, connecting disparate systems and applications and informing better business decisions.

Rockwell Automation has combined expertise in motor control, process, power and energy management, and information solutions to deliver specific and powerful solutions that address the most critical mining operational challenges.

The Connected Mine from Rockwell Automation is built on application expertise, alliances with best-in-class system integrators, equipment manufacturers and technology providers with strong execution capabilities.

FLEX 5000 I/O Adaptors with Enhanced Communication Support and Greater Flexibility

The next generation FLEX 5000 I/O has excellent reliability and provides a flexible I/O solution in a Connected Enterprise. Hardened for applications in extreme requirements, FLEX 5000 I/O modules have the ability to operate in extremely cold arctic environments through to mines in extreme heat (-40 C to 70 C).

The new FLEX 5000 I/O SFP Adaptors deliver enhanced communication with 1 GB EtherNet/IP connectivity, which offers higher speed and increased bandwidth for improved real time operations. To provide flexibility in your network architecture, these adaptors include support for both copper and fiber-optic media, reducing the need for additional media converters. In addition, the SFP adaptors are available in both extreme (XT) and non-XT variants.

Designed for The Connected Enterprise, the Flex 5000 I/O modules help both OEMs and process operations benefit from increased productivity and security. Parallel Redundancy Protocol (PRP) and Device Level Ring (DLR) support for high-availability in Ethernet networks are available as firmware update for all Ethernet adapters. This provides highly reliable and highly available communication networks with zero recovery time for data transmission.

As part of offering the automation and safety functionality in one I/O solution, the discrete safety I/O are introduced with SIL 3, cat. 4, PLe rating and designed to fit into the standard FLEX 5000 I/O system. Apart from the 16-point discrete input and output modules, the release also includes a 4-channel relay output module.

Rockwell Automation Expands TotalFORCE Capabilities and Power Range for PowerFlex 755T Drives

●●● *Drives now available for 10 to 6,000 horsepower applications*

Rockwell Automation has expanded the power ranges and capabilities of TotalFORCE technology for its Allen-Bradley PowerFlex 755T AC drives. The drives now offer an expanded power range, helping engineers with applications from 10 to 6,000 horsepower (7.5 to 4,500 kW) improve productivity and reduce their lifecycle costs. The expansion brings harmonic mitigation, regeneration and common bus-system configurations to a wider range of high-demand applications.

Enhancements to the patented TotalFORCE technology include more powerful adaptive control capabilities, which allow the drives to monitor machine characteristics that can change over time and automatically compensate for the changes that occur. An adaptive tuning feature uses up to four automatic tracking notch filters to block resonance and vibration that can impact quality, waste energy and prematurely wear out a machine.

In addition, predictive maintenance features provide real-time information about the health of the drive. By monitoring operational characteristics such as temperature, voltage and current, the drive is able to calculate the remaining life of critical components and notify users. This allows users to act so unplanned downtime can be prevented.

"TotalFORCE technology enables PowerFlex 755T drive users to take a proactive approach in improving machine uptime. The drives can deliver information about the status of an application to the control system, which can be critical for reducing downtime and increasing productivity," said Brad Arenz, product manager, Rockwell Automation. "The drives' ability to be self-aware also enhances reliability and simplifies service."

The PowerFlex 755T variable-frequency drives were previously designed for 160 to 3,000 horsepower applications. The expanded power range makes PowerFlex drives ideally suited for large power applications such as pumps and fans requiring harmonic mitigation, and regenerative applications requiring anti-sway functionality such as cranes and hoists. The offering includes:

- **PowerFlex 755TL drive:** The PowerFlex 755TL drive uses active front-end technology and an internal harmonic filter to reduce harmonic distortion. The drive is now available from 10 to 1,800 Hp (7.5 to 1,400 kW).
- **PowerFlex 755TR drive:** Delivering power from 10 to 6,000 Hp (7.5 to 4,500 kW), the PowerFlex 755TR drive includes both regenerative and harmonic mitigation solutions. The drive helps reduce energy consumption and costs by delivering energy back to the incoming supply, resulting in a more energy-efficient solution.
- **PowerFlex 755TM drive system:** This allows users to build the system that best fits their needs for regeneration and coordination of multiple motors in common bus configurations. To optimize their system requirements and meet power-consumption needs, users can select from a series of predesigned modules with a power range from 250 to 6,000 Hp (160 to 4,500 kW) for motor side inverters and a range of 70 to 4800 kW for regenerative bus supplies.

Other new capabilities include an integrated safety module that delivers several advanced safety functions on an EtherNet/IP network, an anti-sway feature that helps lifting applications achieve greater stability and permanent magnet motor control for increased energy savings.

Combined, these new TotalFORCE technology capabilities help reduce time to commission, optimize performance and enable simplified maintenance and serviceability throughout the full lifecycle of PowerFlex 755T drives for a broad range of applications.

ArmorView Plus 7 Graphic Terminal

●●● The new ArmorView Plus 7 Graphic Terminal is a fully enclosed panel available in 12.1" size and features IP66 protection enabling a low-cost cabinet free HMI solution. It offers convenience features, including a space and cost saving design that makes an additional enclosure unnecessary, separate push buttons and low installation overhead.

This HMI is easily connected, and Ethernet I/O communication minimizes wiring. The ArmorView Plus 7 Graphic Terminal offers options to increase flexibility, such as buttons and switches that can be individually customized to meet the needs of each machine, and orientation mount options from either a swing arm, pedestal or fixed surface.

we secure

Having a robust and secure network often underlines the success of your digital transformation.

Take on this journey with ease and peace of mind, tapping into our in-depth knowledge and expertise.

Find out more at
https://www.rockwellautomation.com/en_SEA/overview.page

EXPANDING HUMAN POSSIBILITY

Rockwell Automation