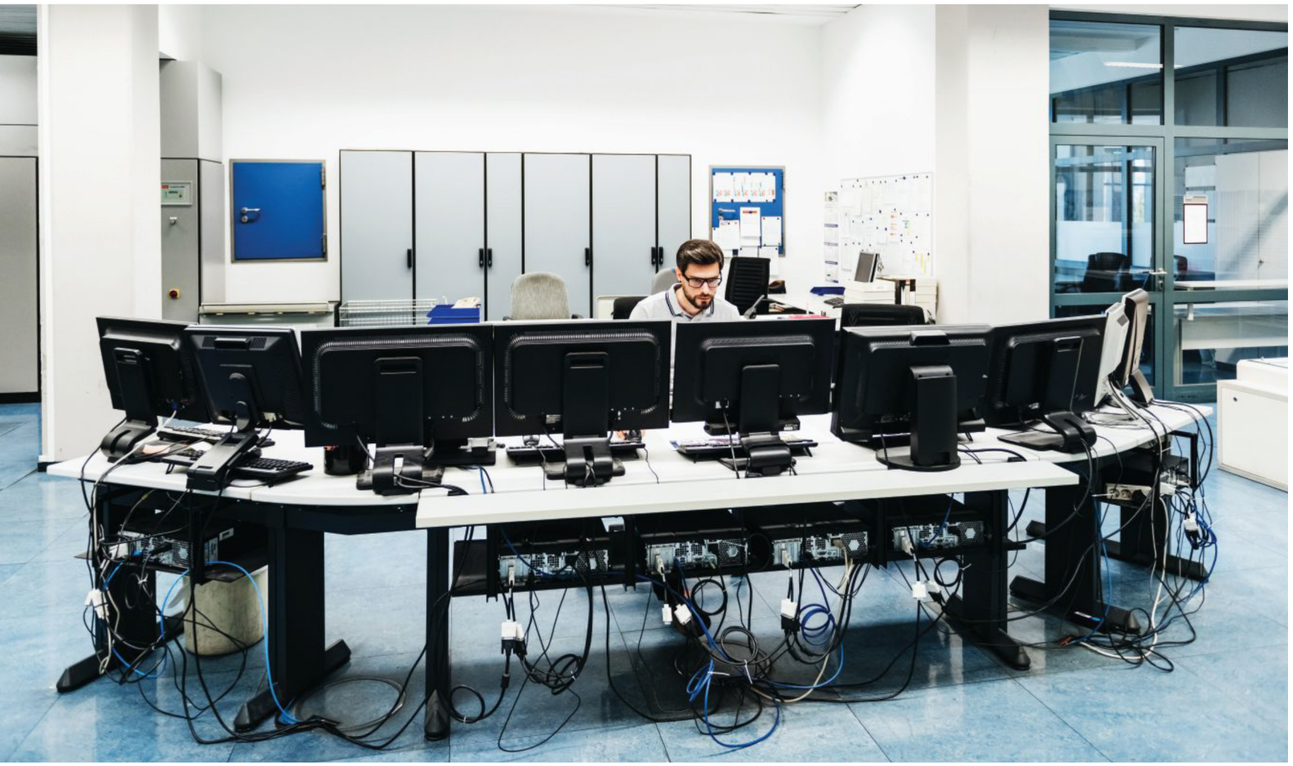


THE STATE OF INDUSTRIAL CONTROL

Senior-level leaders join our roundtable on industrial control systems to sound off on legacy equipment, device lifespan and controls project planning

BY KRISTINA URQUHART

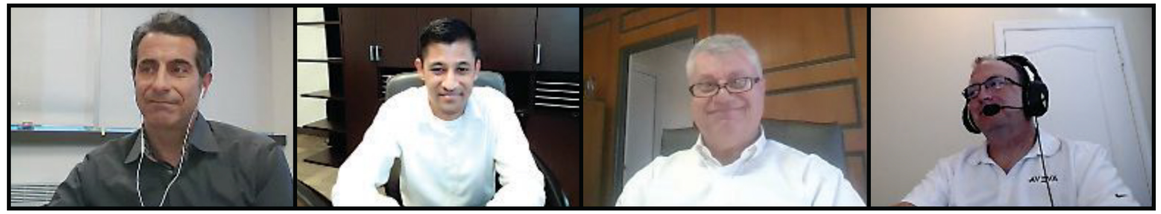
Upgrades to industrial control systems (ICS) are one of the biggest investments a company can make. Industry 4.0 offers many new capabilities for ICS, but how can a manufacturer convert their control systems while maintaining uptime, ensuring security and minding cost?

Last month, we asked several industry experts to share their insight and advice on making a change to control systems and devices such as SCADA, HMI, PLCs and MES at our online Industrial Control Systems Roundtable. (You can watch the recording via automationmag.com/industrial-control).

The advantage of modern control systems is they can connect to automated machines and store reams of data that can be sent to edge or cloud services for analysis, noted Vic Briccardi, president of RTS Consulting – Automation. Using artificial intelligence and machine learning, that data is then used to optimize operations and drive value.

"In the past, systems were very much set it and forget it," said John Krajewski, senior director of product management, monitoring and control at AVEVA. "Now, control systems are living and breathing – we're constantly commissioning new things and decommissioning old things."

Over the course of about two hours, our roundtable participants discussed how COVID-19 has impacted that value, and how profitability, data optimization and security factor in to any new controls project. Here's just some of what they had to say.



The Industrial Control Systems Roundtable panelists, from left: Christian Perrier, PCI Automation; Sanjith Singh, Schneider Electric Canada; Vic Briccardi, RTS Consulting – Automation; and John Krajewski, AVEVA.

"Don't get caught in the trap of getting a fancy new control system but using the old legacy control philosophy."

Using the ICS for crisis management

The COVID-19 crisis has put more stress on legacy ICS – particularly those that were not yet connected to the internet or equipped with the capabilities to enable remote access. As workers moved from their usual places of work early in the pandemic, there were restrictions on what they were able to access, said Krajewski.

In addition, support for hardware, software and service has been challenging throughout the pandemic, with people working from home, off sick or reluctant to travel, said Briccardi. Without connectivity, "users of existing and legacy control really lacked or had limited visibility and control of production operations," he said. "Total access to operations, anywhere at anytime, is paramount to supporting the operation."

Sanjith Singh, vice-president, industrial automation at Schneider Electric Canada, said that automation was a "godsend" for plants that didn't have enough workers onsite to maintain and run equipment. Plants that had upgraded their PLC, HMI and SCADA systems were better equipped to pivot for production of critical medical devices and supplies needed in the fight against COVID-19.

The bottlenecking in supply chains caused by the pandemic has highlighted a bigger need for networked systems, said Singh.

"As we see the demands of consumers becoming greater, there's a greater need for traceability throughout the supply chain," he said. "You don't just track and trace the finished product [anymore], you now need to trace the supply chain – so the suppliers' suppliers – almost to the point [of] the component level right up until to the produced level."

With supply chain, production and logistics requiring traceability to gain full visibility, the industry is moving from a "smart factory" idea toward a more holistic "smart manufacturing" approach.

"From that perspective, control systems are really helping to connect those dots, and connect the supplier to the raw material," said Singh. "It's almost a farm-to-fork mentality using the control system."

Considering cost vs. value

When is right time to upgrade? It comes down to several factors, Singh said, and greatly depends on a manufacturer's desire to embrace new technologies as well as the funding they have available – though there are a variety of solutions available now to fit most budgets.

But the maturity of the equipment should be of concern, as should access to parts. "As control systems age, there is a risk of failure and fatigue at the component level, which results in downtime," said Singh.

Manufacturers are hesitant to invest in new technology because they do not fully understand the risk if they don't, said Christian Perrier, president of PCI Automation. He finds leaders reluctant to move data outside of their current setup. But prolonged maintenance of control systems can only go so far until repairs get too complex and too costly to do. "It raises the risk of longer downtime," he said.

The availability of systems also prevents manufacturers from moving on upgrades, shared Krajewski. For example, some of his clients can only afford one to two hours of scheduled downtime per year, and don't want to have to run two systems at once in order to do an ICS changeout.

"So very often you see these guys trying to change the engines on the airplane while the thing is still in flight," Krajewski said. "The monolithic nature of a lot of the old systems actually led to this – to touch anything, I had to bring everything down. We're starting to see things become more segregated."

This means that while one part of a control system is down, another part can still be running – or the cloud can be used to upgrade certain components on the fly. This approach is enabling more manufacturers to move to a hybrid model, whereby they can bring systems that are not mission-critical fully into Industry 4.0 and leave critical processes alone, tacking on additional connectivity solutions as needed.

"Extending the reasonable life of assets has become a huge thread," said Krajewski. Artificial intelligence and machine learning can help operators learn the value of an asset "so that you can understand – do I need to replace it, or do I need to maintain it? Can I just continue to let it do its job?

ICS

For this roundtable, we defined industrial control systems (ICS) as the devices, instrumentation, software and networks used to operate industrial processes, particularly when it comes to manufacturing.

"Very often you see these guys trying to change the engines on the airplane while the thing is still in flight," Krajewski says.

Ultimately, the capital expenditure that can be preserved is gold. There [may be] no reason to have to buy it again or rebuild it."

Briccardi pointed to a recent example when his company worked on a 1960s injection molding machine. Because it was not connected to the internet, it had no metrics or KPIs to indicate its health. The client did not want to move data to the cloud, but was willing to have analysis on site. With a $600 PLC attached to the machine, Briccardi's team was "able to strategically pick points to be monitored so that we had visibility into things like cycle time and idle time and mold changeover time," he said. The company was able to "get definitive numbers on how well the machine was performing compared to the latest and greatest technology, which then allowed them to make some strategic capex decisions on new machines."

Planning a new controls project

As they're considering an upgrade, some of the common things senior decision makers want to know include the availability of hardware, if there are resources to support the team during downtime, if data will be able to be shared and integrated with other parts of a plant, and if the ICS will be able to communicate with other controllers in the plant, said Briccardi. A key part of planning for an upgrade is creating a strategy or roadmap for the future, even if it won't be used for several years.

"Sometimes, direct cost-benefits are not enough to make a project go," said Perrier. "Initially, your project may not be profitable in itself, but if you consider integrating it into your full picture, it takes on a lot more value."

To ensure the success of a new controls project, Briccardi advised beginning with a business goal such as improved financial performance or increased productivity, as well as an expected outcome. Identify high-priority initiatives that bring maximum value, then conduct a gap analysis to ensure those goals can be achieved.

Once an upgrade is underway, steer clear of old ways of thinking, said Singh. "Don't get caught in the trap of getting a fancy new control system but using the old legacy control philosophy," he said. "You become less efficient, because you've spent a lot of money and your return on investment has been pushed out."

He suggested looking beyond the project's goals to the company's goals. If sustainability is a corporate goal, then energy consumption should be a key indicator on a new ICS. Once you've mapped out what you want to achieve from a macro level, you will know what hardware makes the most sense for your application.

Optimizing performance using data

A key feature of modern industrial control systems is the streamlining of data collection so that the data can be contextualized and used to improve performance, Singh said.

In the past, manufacturers had their devices hardwired throughout a plant – and this system is still in place at most plants today. But with wireless networks or connected devices, data can be collected more easily, and used in exciting new ways that move beyond simple graphic representations and into preventative and predictive analysis.

"One of the biggest limitations we have is our imagination," said Krajewski. For example, a PLC might not be the best place to obtain information for a certain application. "If an operator sees falling output pressure on a pump and knows the seal needs to be replaced – when was the last time that information was maintained? That information is not in the PLCs. Do we have any spares in the inventory? That information is not in the PLC."

Indeed, PLCs are powerful tools that now incorporate office-centric communications protocols like SQL, MQTT and others, which helps with their integration into reporting software, Perrier said. But they're not the only control device from which data can be gathered.

The latest tools for data analysis, which include modelling, correlation analysis and statistical process control, can provide ways to optimize production in real time, said Briccardi. In order to facilitate that analysis, control systems can move the data from machines to a database for computation. Ideal performance targets are then fed back to the edge.

That real-time data feedback is paramount to modern-day ICS, said Singh. "Clients are looking for speed. How quickly can I get data?" he said. "From a manufacturer perspective, or from an analyst perspective, if there's a component failure, you want to know the second of the minute of the day that it happened. So you need real-time data transmissions."

Speed will be further enhanced by 5G wireless networks, which are forthcoming to the industrial sector over the next few years. With lower latency and increased network capacity, Briccardi noted that 5G will allow manufacturers to reliably connect devices inside plants on segmented networks, allowing for private transfer of information.

Securing industrial control systems

Cyber attacks are an increasing problem in manufacturing – and industrial control systems are a major target for criminals. The roundtable panelists unanimously agreed that their clients don't take cybersecurity seriously enough.

For manufacturers without a cybersecurity plan, "once you get locked out of your production facility, you could go days or weeks before you open it up," said Singh. "Instead of paying for protection, you have to pay after the fact and then spend possibly millions of dollars because your production line is down.

"We really need to start thinking about what [this means] for our plant. If I were to get locked out of my plant today, what would it cost me? And is that cost greater or less than what it would be for me to actually invest in having a good cybersecurity plan?"

$600

Using an inexpensive PLC that cost $600, Vic Briccardi at RTS Consulting was able to bring a 1960s machine online so that decisions could be made about the equipment's health and longevity.

Singh advises against maintaining the status quo on a legacy ICS, even if connected systems bring higher risk.

With many cybersecurity incidents kept under wraps to protect the reputation of the affected company, awareness isn't as strong as it should be, Perrier said. "It causes other customers to have a distorted picture of the situation and the potential threat," he said. "One [attack] I heard about stopped production for three days on six job sites. Another caused a company to stop functioning for maybe two to three weeks, everything from customer service to production floor."

He stressed that losses are the biggest consequence of a cyber attack – not only in terms of production, finances and intellectual property, but also potentially human life. If an attack on a connected machine results in it operating in a different or unsafe manner than its original use intended, a worker could be injured – or worse.

"[Companies] say, 'I don't know that I can balance that risk against availability' – until it hits them. And then they realize how important it was," said Krajewski. "Be honest with yourself – make sure you have a clear and documented topology of your system so that you understand what the attack vectors are."

There are various areas of entry for a cyber attacker to compromise an ICS, and thus varying levels of risk, said Singh. He suggested contracting a company experienced in cybersecurity to provide an objective assessment of hardware, software and systems. He also advised against maintaining status quo on a legacy ICS, even if moving to connected systems brings higher risk.

"If we don't do something because we are worried about the risk of typically what could happen, then we're never going to move forward," Singh said. "Mitigate your risk. Because we know there is risk. Do the right things, put the cybersecurity measures in place."

That includes ensuring secure access to industrial control systems through encryption, authentication and restrictions on user activity, said Briccardi. Remote access works for some employees, but it can also introduce errors in programming if operators and engineers are accessing control systems without being present in the physical environment.

Perrier pointed out that there's an additional, rarely considered element that can help to ensure security – if employees are well compensated, they will care more about the health and security of the company.

Another way to minimize risk is to work with vendors that are specifically certified to make components or provide services. This is especially important at a time when everyone is experimenting with IIoT solutions that can provide additional access points for cyber criminals.

"Startups may not have that maturity," Krajewski said. "If you're working with a startup, they may have some brand-new fancy technology, but very often they haven't gone through the level of maturity where they've established the security practices to ensure they are ready for primetime."

Singh agreed. "Cheap is not always better," he said. "Sometimes, there is a reason why something is cheaper."

Thanks to our sponsor, Schneider Electric Canada, for their assistance in putting together the roundtable. Watch the roundtable recordings and see more videos from our panelists at automationmag.com/industrial-control. | **MA**

What's new in industrial control?

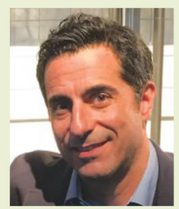
Roundtable participants shared the control trends that excite them moving into next year.

Vic Briccardi, president and founder, RTS Consulting - Automation

Briccardi said he is excited to see where AI goes, because it is a boon to productivity in the factory, and integral in ensuring maximum performance of assets with no waste. "I think we're heading toward a future where we'll have conscious factories driving the supply chain," he said.

John Krajewski, senior director, product management, monitoring and control, AVEVA

Client attitudes on change are shifting, Krajewski said, which makes conversations about upgrading easier. "I'm seeing a willingness to take that chance." Mission-critical legacy systems can co-exist with new AI, cloud, and machine learning solutions – and Krajewski said he's looking forward to seeing how that continues to evolve given the demands COVID-19 has put on the industry.



Christian Perrier, president, PCI Automation

"I like the way PLCs are now talking in languages once only seen in office software such as SQL, OPC and MQTT," Perrier said. "This really elevates the integration level." He also enjoys seeing how artificial intelligence is being used to enhance machine vision, as well as the automated logistics solutions that are now available for warehouses and distribution centres.

Sanjith Singh, vice-president, industrial automation, Schneider Electric Canada

"The trend I see is there's a shift away from buying products and turning to integrated solutions," Singh said. "People aren't looking at where they are today, they're looking at where [they're] going to be in three years or in five years. And I think that thought process is developing a trend of the connected world – and the connected product inside the industrial control system."