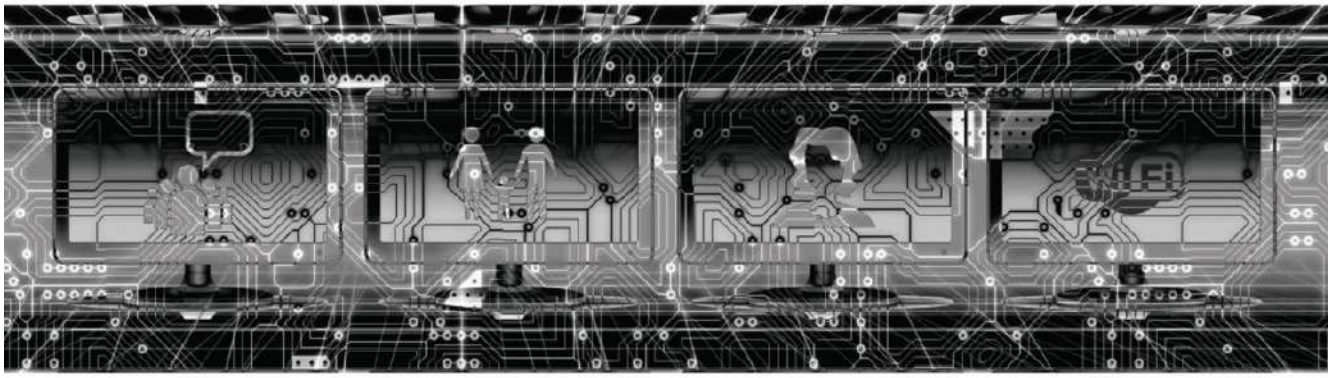


Blow Molding and the Connected Factory

By Tom Craven,
VP of product strategy
RRAMAC Connected Systems

Blow molding applications are both cost-sensitive and complex. Maximizing profits in blow molding equipment is a balancing act between increasing machine throughput and minimizing raw material costs while maintaining quality. These factors make blow molding an ideal candidate for Industry 4.0, which leverages the ability of machines, devices, sensors and people to connect and communicate with each other via the internet to reduce costs and maximize productivity.

Industry 4.0 can help blow molders:

- connect to equipment suppliers that can assist with machine troubleshooting, optimization and upgrades;
- implement predictive maintenance strategies to minimize unplanned downtime;
- optimize machine throughput by using software programs that provide process simulation and artificial intelligence (AI) and can track overall equipment effectiveness (OEE);
- automatically order raw material based on actual machine usage and history;
- leverage smartphone apps and web dashboards to provide real-time data such as equipment status, downtime alerts, predictive-maintenance alerts, production rates and production totals;
- and automatically order replacement parts based on failure alerts or predictive maintenance notifications.

For example, a recent case study involved a customer that was experiencing nozzle clogging that resulted in an increase in downtime, scrap and labor hours. By sharing sensor data with a trusted partner, the customer was able to access a model to predict nozzle clogging in real time and alert operators when needed. The solution reduced nozzle changes, eliminated nozzle clogs and improved quality. From contract to completion was four or five weeks, including integration, and the project produced an annual cost savings of about $450,000. (See case study on Page 11.)

Some will argue that software that provides process simulation, AI and OEE calculations can be installed at the end-user facility without the need for internet connectivity. The difficulty in this approach is that these types of software packages must be adapted to fit each user's specific requirements and most end users do not have the time or expertise to properly configure, maintain and continually optimize these software packages.

Hosted solutions for simulation, AI and OEE can be quickly implemented and maintained by the software provider for a fraction of the cost of installing, configuring and maintaining software packages in-house. Consequently, the return on investment (ROI) is far more attractive with a hosted solution.

The obvious concern for many users is the security of the internet connectivity. In this respect, the Industrial Internet of Things (IIoT) is like fire — dangerous if used carelessly, but incredibly valuable if used safely and properly for a specific purpose. This article explores several software architectures that allow companies to optimize blow molding equipment while keeping both the plant floor and the company's intellectual property safe from cyberattacks.

The 'Trust No One' Security Model

Many companies still take the approach that the plant floor should have absolutely no connection to the outside world. This is a perfectly understandable approach, but it does not guarantee that you are secure from cyberattacks. The industrial automation market is being flooded with products that offer some form of internet or wireless connectivity. You may choose not to use them, but the connectivity is waiting for someone to enable or configure it.

In a 2013 presentation, Theresa Payton, a former White House chief information officer and one of our nation's leading experts on cybersecurity, pointed out, "'Zero risk' does not exist." Instead, she advised, "Make sure 'managed risk' does."

Payton stated that most security breaches are caused by well-meaning employees who are simply trying to do their jobs. According to Payton, insider threats can happen when "Mr. Incredible" breaks your defenses.

"I tell organizations that their biggest threat may actually be their 'Mr. Incredible' employees. These are the people that will do whatever it takes to work for you: days, nights, weekends and holidays."

On the manufacturing floor, "Mr. Incredible" might be the engineer trying to fix an issue that can be quickly resolved with a temporary internet connection. This might be done in order to perform a software or firmware upgrade or allow an equipment manufacturer to remotely troubleshoot the system.

There is also an infamous story about hackers stealing a casino's high-roller database through a thermometer in a lobby fish tank. We'll talk about preventing these types of attacks in the Cyber AI section, but the point here is that zero connectivity or the "Trust No One" approach is no longer a realistic expectation.

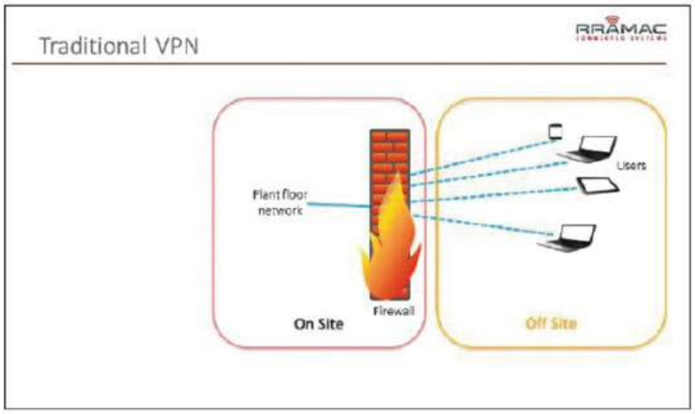
Why a Traditional VPN Is Not the Solution

A Virtual Private Network (VPN) is designed to connect an external user to a network. A VPN is great at allowing employees to access the company network when they are out of the building but is not the best option for allowing outside suppliers or cloud-hosting companies to access your equipment. A VPN requires a hole in a network's firewall, which is unacceptable to almost all IT groups. If allowed in through the firewall, VPN users are free to browse your company network unless your IT group takes the time and effort to restrict access for each user. This means IT personnel have to set up rules for each external user to allow each user access to specific equipment.

There are two conversations you do not want to start with your IT department or your customer's IT department:

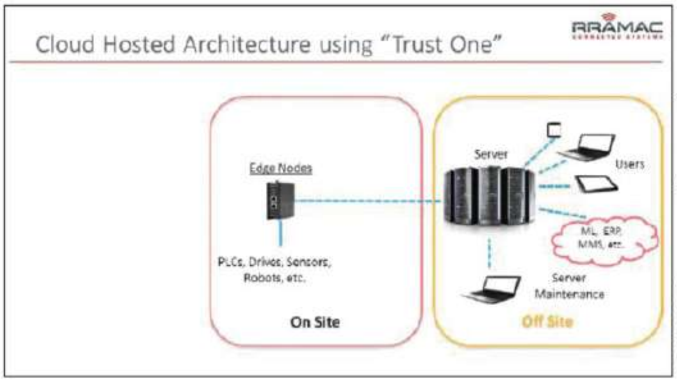
1. I want to break your security policy by putting a hole in your firewall; and

2. I want you to do a bunch of extra work on my behalf.


Traditional VPN

A Virtual Private Network (VPN) is designed to connect an external user to a network.

IT personnel are often quick to reject any request for remote connectivity, because they assume that the solution will be based on a VPN. Ultimately, plant management or other financial stakeholders will drive the decision to invest in an Industry 4.0 solution. IT personnel will be far less likely to prohibit the connectivity once they understand that they will not be required to permit and manage external VPN users.


Cloud Hosted Architecture using "Trust One"

RRAMAC Connected Systems illustrations

The "edge node" used in this diagram is a Secomea SiteManager, provided by Secomea.

'Trust One' Security Model

A simple, cost-effective alternative to the "Trust No One" approach is the "Trust One" approach. This approach allows secure, managed connectivity without the VPN requirements of firewall holes or custom IT configuration. The connection is initiated by an "edge node" within the plant that can collect data from sensors, PLCs, drives, etc., and push it over the internet to a cloud-hosted server. The edge node is located inside the company firewall but is able to connect through the internet using an open port or a proxy server. There is no publicly exposed IP address and no ability to accept an inbound connection. The connection to the cloud server uses Transport Layer Security certificates and data encryption.

External users can then access the information they need via web interfaces, smartphone apps and email or text notifications. Account administrators can grant users access to specific equipment or processes. All user activity can be monitored and tracked in an audit.

The specific type of edge node can limit access by remote users. Access possibilities may include:

- read-only access to data collected by the edge node;
- read/write access to specific variables on PLCs or other devices configured on the edge node;
- and programming access to PLCs or other devices configured on the edge node.

Case Study: Connectivity Saves Money

Issue

A manufacturer of high-performance aftermarket automotive parts was having problems with its two-part reaction injection molding (RIM) mixing nozzles clogging. The situation led to excessive costs in increased downtime, waste and labor.

Solution

Lone Star Analysis, a Dallas consulting company that provides predictive and prescriptive analytics, built a model to predict nozzle clogging, so that operators could be alerted when needed. Additionally, Lone Star's solution monitored other criteria and was able to help identify the root cause of issues affecting quality.

Results

With Lone Star's solution, the manufacturer eliminated clogs, experienced fewer nozzle changes and improved part quality, reducing scrap. Lone Star's simulation model required the use of relatively few sensors and led to insights that reduced raw material consumption by increasing the time between material purges and reducing purge volumes.

Annual cost savings approximated $450,000 with about a 7 percent increase in machine performance. The manufacturer achieved a return on investment in less than one month. ●

For more information
Lone Star Analysis
Dallas
972-690-9494, http://lone-star.com

All of these features can be enabled or disabled on the cloud server. Read/write access and programing access, if available at all, are limited to specific users and are fully audited.

Three key factors distinguish this approach from a traditional VPN:

1. The connection is outbound to a server, not inbound into the plant network.

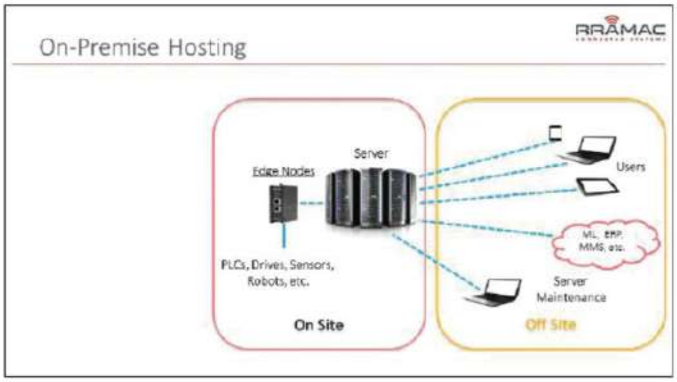
2. Remote users have access to information on the edge node device, but do not gain access to the plant network.

3. No firewall holes/exceptions are required.

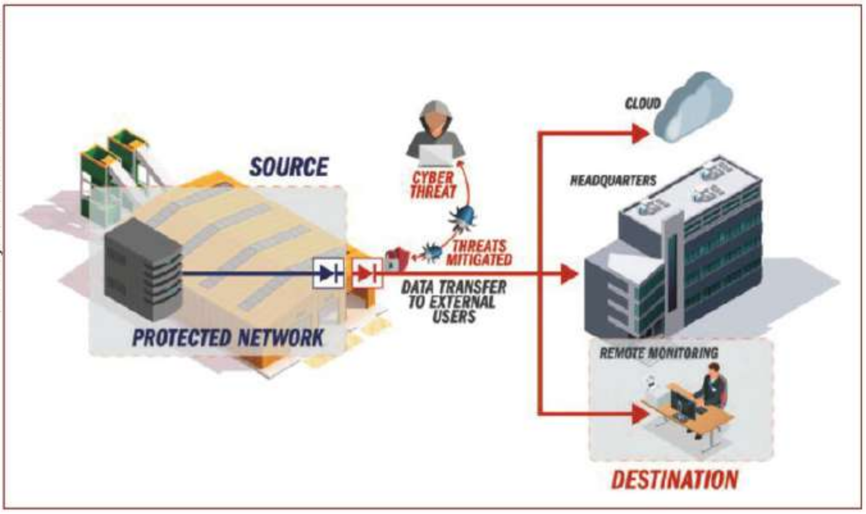
Little or no work is required by the plant IT department, other than providing a proxy server account if required for outbound internet access.

On-Premise Hosting

For companies requiring that all data or a portion of data remain within the walls of their buildings, a solution hosted on-site can provide a better outcome than managing the software in-house. In this scenario, the software-service provider configures software to run on a dedicated server on the customer site. The architecture strongly resembles the previously described cloud-hosted architecture with the exception of the physical location of the server. The software provider requires remote access to the server for initial setup and periodic maintenance, but the outside connection can be switched off entirely most of the time. Maintenance, upgrades and enhancements can be performed periodically or on an as-needed basis and can be scheduled and monitored by the end user.


On-Premise Hosting

The edge node in this diagram is also Secomea SiteManager.



Owl Cyber Defense Solutions LLC

Data Diodes

A data diode is a special type of edge node that allows outbound data from the plant while physically preventing any inbound traffic. The data diode consists of two network ports, each with its own processor. The "upstream" side of the data diode communicates with the plant floor, while the "downstream" side communicates with a remote server over the internet. The two sides are connected to each other through a fiber-optic signal. While most fiber-optic signals include both a transmit line and a receive line, the data diode has only a single fiber that transmits data from the plant side to the remote connectivity side.

The data diode may include a physical switch that would enable bidirectional communication in order to allow outside vendors temporary access for troubleshooting or maintenance purposes. Data diodes are a great option for on-premise-hosted solutions because they can allow outside users to access information without any chance of connecting into the plant. The physical switch feature provides a way for the software vendor to perform periodic upgrades wtih a temporary, user-specific connection.

Cyber Artificial Intelligence

As mentioned previously, a "Trust No One" or a zero-connectivity policy will not guarantee that there will be no outside access at your facility. Regardless of how secure your company network is, the possibility still exists that someone will attempt to try to sabotage your network or steal your data. This is where cyber AI systems come in.

Cyber AI solutions continuously monitor your network and alert you to suspicious network activity that may be associated with a cyber threat. The system will also learn the data traffic on your network and establish normal usage patterns. When the network traffic pattern changes, the system will alert you of the unusual activity and provide details. Regardless of whether you choose to allow some level of remote connectivity, cyber AI gives you added assurance that your equipment and data are not at risk.

Recommendations

Industry 4.0 has the potential to reduce material costs and increase throughput for blow molding applications, and, while cybersecurity concerns are a major consideration, they are not insurmountable. The key is to weigh the benefits against potential risks.

The following are recommendations for starting an Industry 4.0 project in blow molding applications:

1. Identify projects that could result in significant revenue if the throughput or quality were increased, or labor or scrap reduced.

2. Select a pilot project with significant measurable revenue or cost savings.

3. Obtain bids from Industry 4.0 providers for the project.

4. Evaluate the total cost, including upfront costs, recurring costs and any internal resources required for setup or ongoing maintenance.

5. Calculate the ROI.

6. If the ROI is justified, set up a meeting between the Industry 4.0 provider and your IT group to review the security architecture before proceeding. ●

For more information
RRAMAC Connected Systems
Plymouth, Minn.
844-477-2622, www.rramac.com