Smart Manufacturing Blueprint:
Adopting technology to take your business to the next level

MOXA®
Reliable Networks ▲ Sincere Service

Table of Contents

What is a Smart Manufacturing Blueprint?

Thank you for your interest in our Smart Manufacturing Blueprint! Before diving in, we want to share a little bit about how the blueprint can help today's manufacturers.

The manufacturing sector is no stranger to transformation and has experienced several stages of evolution throughout history. Since the 18th century, the adoption of key technologies has helped industries achieve greater efficiencies and effectiveness. These technologies have included the implementation of steam-powered machines to facilitate production, the use of electricity as the primary power source in factories, and the invention of transistors and integrated circuit chips that enable automated machines.

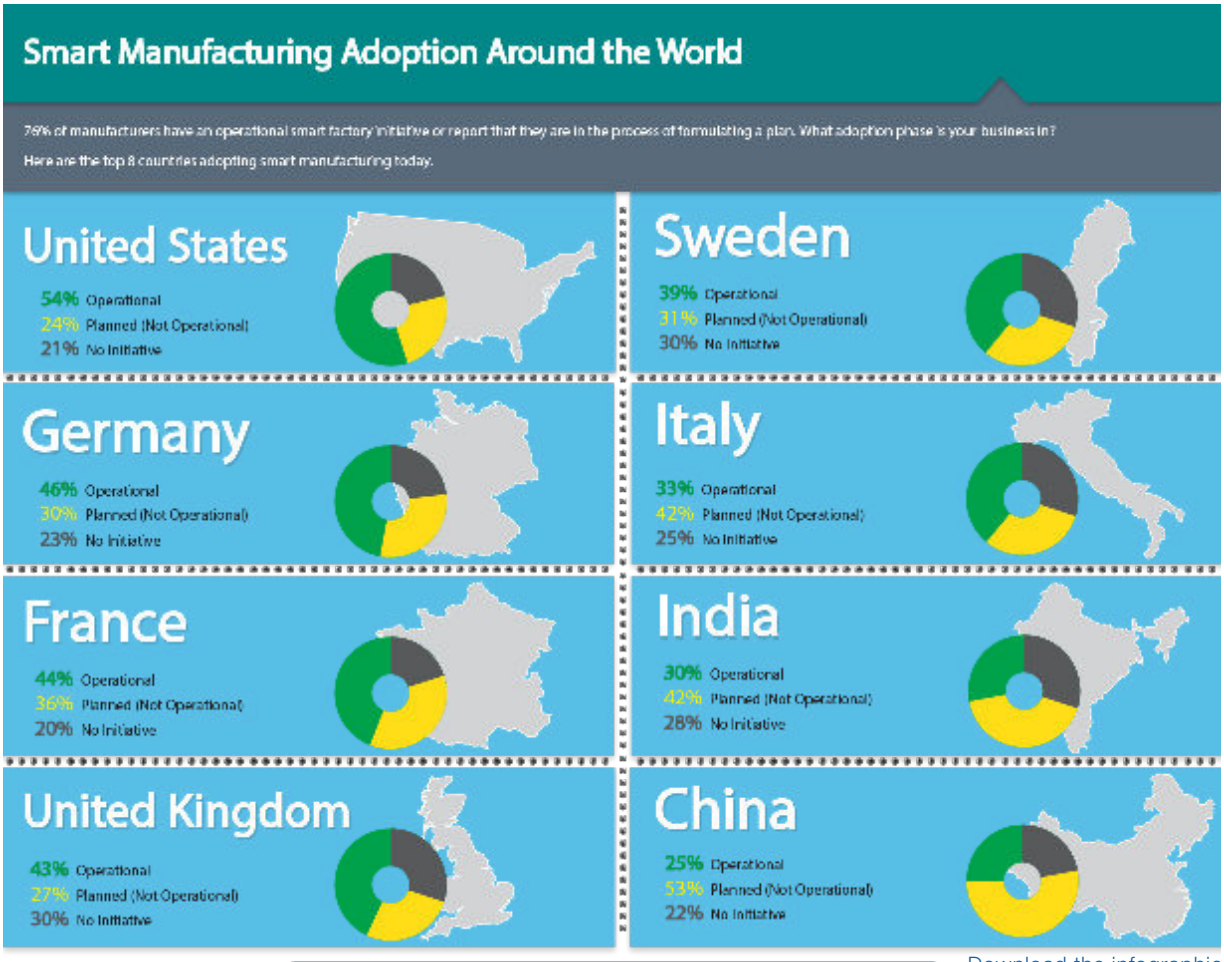
Today, manufacturers are taking operations, production line management, and order fulfillment to the next level. They are accomplishing this by utilizing the data points that are critical to their business. By doing so, a wealth of insightful information can be at the fingertips of both operators and managers, enabling them to monitor machine health, make informed decisions, take preemptive measures, and much more.

With the Smart Manufacturing Blueprint, our industry partners can identify key technologies available today to enhance production efficiencies while lowering overall costs. In fact, the term "smart manufacturing" involves much more than just the advanced manufacturing of goods, but also incorporates the end-to-end manufacturing process from raw materials to outbound logistics. Let's take a closer look at the ways technology is reshaping the manufacturing industry.

Eddie Lee
Director of Global Industry Marketing
Moxa Inc.

The Global Adoption of Smart Manufacturing

Smart factories are actively being adopted across the globe, with industrial manufacturing, automotive and transportation, and aerospace industries leading the pack with an ongoing initiative. By embracing new technologies around the Industrial Internet of Things (IIoT), big data, and AI, these businesses can reduce operational costs while increasing productivity and efficiencies in their manufacturing processes. This is achieved through the implementation of a combination of connected devices, predictive maintenance, automating tasks, and data visualization. Check out our infographic to see where your smart factory stands within its respective country.



Download the infographic

> 76% of manufacturers have an operational smart factory initiative or are in the process of formulating a plan.
>
> Click to tweet this

The First Steps to Enable Smart Manufacturing

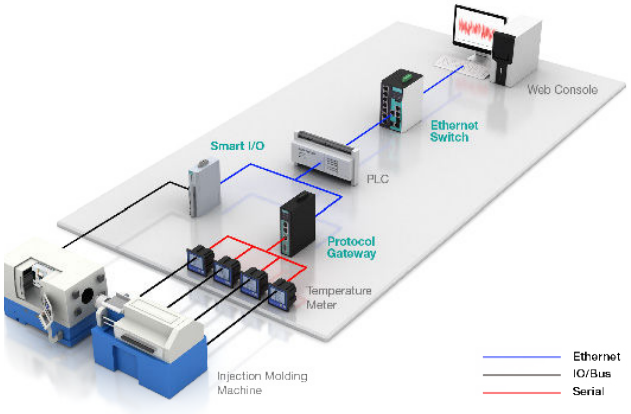
The First Steps to Enable Smart Manufacturing

The value of smart machines for manufacturing applications is real. With these machines, you can enjoy real-time data collection, remote monitoring, preventative maintenance, and apply self-learning for improved production quality. Thus, factory equipment can provide a vast amount of data. The basics of getting started to build intelligence around your machines include:

Connecting Sensors

Complete a walkthrough of your factory and take an audit of which critical equipment can offer data that is most important to your operations. This can include devices such as PLCs, sensors, temperature gauges, production machines, and more. You will need connectivity devices that can extract the information from individual sensors, gauges, and machines so that you can stay updated on their performance and any variances that are outside of your production requirements. Oftentimes, sensor data can be extracted via I/O devices. Connecting these devices to a protocol gateway will translate the I/O data to an industrial protocol that can then be transmitted through Ethernet to your SCADA/MES (Manufacturing Execution System).

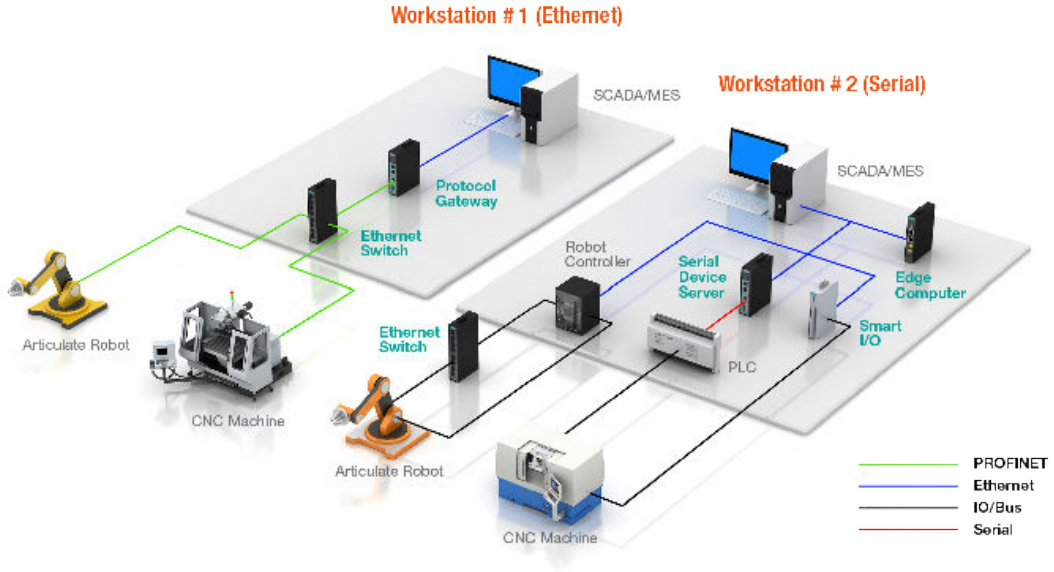
To view this data, you will need some sort of web console that presents sensor data in a format that is easy to understand and enables you to analyze by cross-referencing contextual production parameters and configurations, and make informed decisions. With this information at your fingertips, you will have the power to decide whether production is optimized, equipment needs maintenance, or whether there are conditions that create performance variances, etc. The return on your investment in machine intelligence will come in the form of increased production, higher production quality, and longer equipment lifespan, resulting in more revenue for your business.



Connecting Machines

Ethernet is the standard if you want to view data from your machines. If your factory machines do not have Ethernet connections, they should have serial connections such as RS-232/422/485. For those looking to enhance the IQ of their factory machines without a large investment in expensive Ethernet-ready factory equipment, the good news is that legacy serial equpment can still have data transmitted via Ethernet. In fact, this is the preferred method for most when adopting smart factories as it offers all the benefits of a connected factory at a fraction of the cost of purchasing new machines.

To get started, identify the types of connections and protocols your existing machines use. This includes conveyors, robot arms, CNC machines, automatic loaders, etc. If they are connected to a PLC, identify the connections and protocols those PLCs have. This is so you can plan how to bridge any potential gaps between your shop-floor equipment and your MES software. If they speak different protocol languages, you will need a protocol gateway to bridge the communication gap between the PLC and MES (i.e. fieldbus to Ethernet).



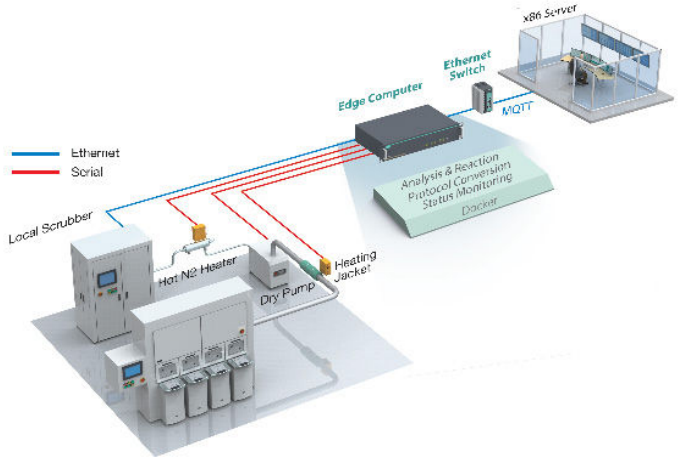
Depending on the size of your factory and the number of machines, it will help to draw a basic topology of your existing setup with connection types identified. This will help in the selection process of the proper industrial gateways, I/O devices, and Ethernet switches necessary once you start working with an industrial networking provider.

Edge Computing

Once you have figured out how to extract information from your connected sensors, machines, and other equipment, an abundance of data will now be available to you. For a single computer, it can be a burden to process all this generated data. To alleviate this issue, industrial computers are used to process localized device data before they are sent to the SCADA system. With this method, data acquisition is performed at the edge of your network (sometimes at remote locations), and only the important information you need to see is sent to the control center.

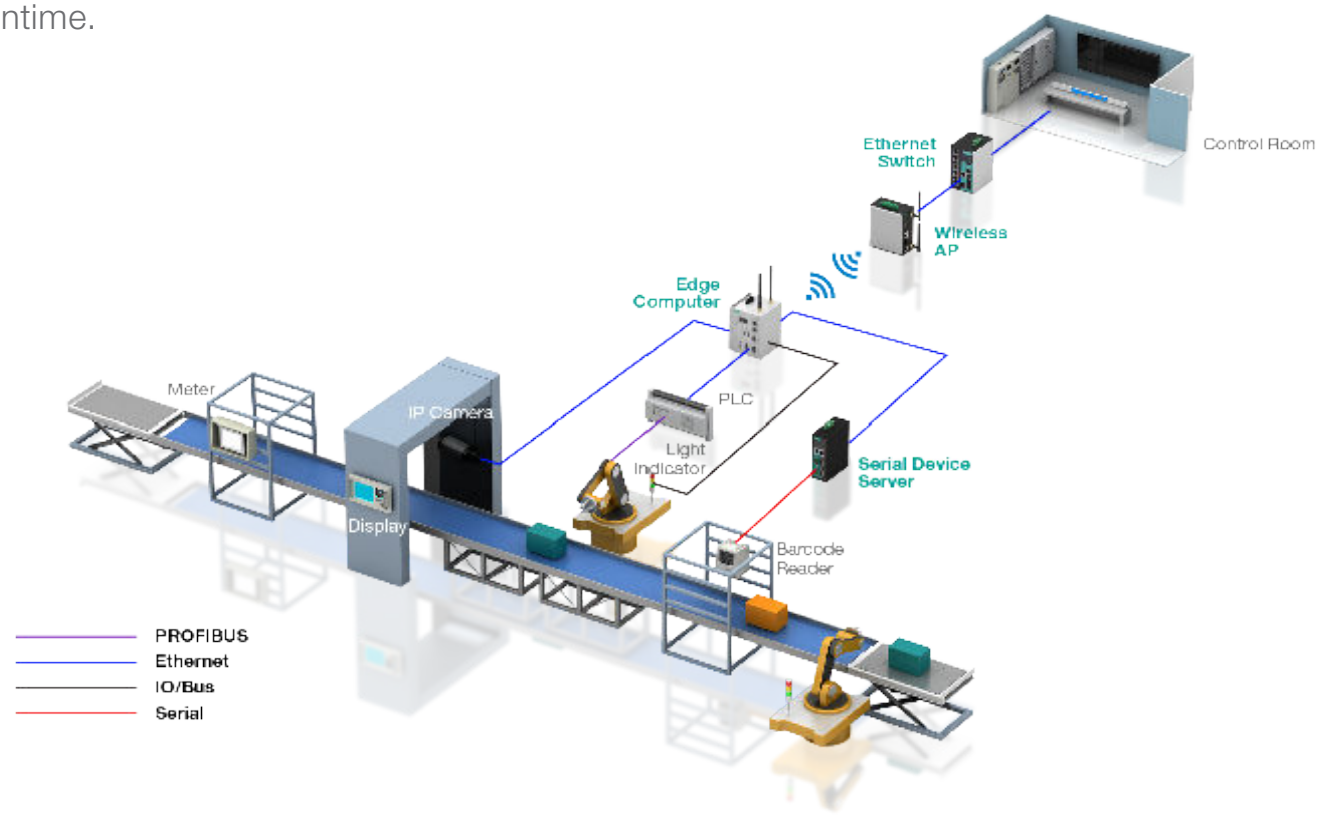
Edge computing delivers tangible value in IIoT use cases. It can help reduce connectivity costs by sending only the information that matters instead of raw streams of sensor data, which is particularly valuable to devices that connect via LTE/cellular, such as smart meters or asset trackers. Also, when dealing with the massive amount of data produced by sensors in an industrial facility or a mining operation for instance, having the ability to analyze and filter the data before sending it can lead to huge savings in network and computing resources. Edge computing also reduces latency, makes connected applications more responsive and robust, lowers dependence on MES / MI (Manufacturing intelligence) software, and helps to better manage the massive amounts of data being generated from the machines and devices.

A technology called Docker is a tool based on a smart gateway (computer or router) with industrial-strength reliability, running a combination of open Linux and Docker/ container. The tool is embedded within a vendor's own proprietary application and is touted as an ideal solution for edge computing. The Linux open platform enables easy porting of IIoT applications to IT infrastructure, while providing multivendor support and programmability.



Some solution providers are proposing a layer of abstraction between the OS and the applications to facilitate easy deployment and management of applications on the fog node. Powered by these features, a computing node can intelligently process large volumes of data received from the sensors and field monitors while only sending critical data or a summary of the data to the cloud. For example, a semiconductor application can share computing data with the sever by implementing an edge computer to complete protocol conversion, analysis and reaction, and status monitoring.

Avoiding device-to-cloud data round trips is critical for applications using computer vision or machine learning. For example, an Automated Optical Inspection (AOI) machine is an automated visual inspection of printed circuit boards (PCB) or LCD transistors. The manufacturer uses on-device machine vision to scan the device to test for both catastrophic failure (e.g., missing components) and quality defects (e.g., fillet size or shape/component skew). Performing image processing tasks through an edge computer, the AOI machine reduces the amount of data bandwidth, processing, and storage required for the inspection process by minimizing the number of image files sent over the network. In addition, by adapting more sophisticated machine-learning algorithms, the accuracy of image recognition could be improved while reducing chances of false alarms and downtime.



With edge computing, security can be improved by keeping sensitive information within the device and using edge networking equipment to reinforce security. This way, device data doesn't travel over a network and stays closer to its origin. By reducing the amount of data in a corporate data center or cloud environment, you are minimizing what is available to intruders if a system becomes compromised.

> Security can be improved with edge computing by keeping sensitive information within the device and using edge networking devices to reinforce security.
>
> Click to tweet this

Through edge computing, system architects have the opportunity to learn the benefits of distributed computing power from end to end—tapping into the capabilities of field devices, gateways, and the cloud altogether. Today, edge computers are being created with increasingly sophisticated computing capabilities, bringing "future proofing" to these systems by allowing automated updates for the device software and the list of local commands it can run. To see how KPMG enabled their smart factory, download the case study here.

The Capabilities of a Connected Factory

The Capabilities of a Connected Factory

By incorporating intelligence into the manufacturing process, system operators and managers can enjoy capabilities that bring significant benefits to the business. In this section of the blueprint, we'll explain how smart factories can lower production costs and increase efficiencies through predictive maintenance, mass customization, and smart logistics.

Predictive Maintenance Through Machine IQ

Self-monitoring is a built-in test (BIT) mechanism that allows machines to perform self-tests to discover whether they need maintenance or repair. Typical tests are for temperature, current, voltage, (motor) torque, or communication quality, for example, the decreased torque output on a robot arm or the overheating/vibration on a CNC motor. However, even after identifying potential issues, technician accessibility could be limited, and checking problems on-site during operational hours could be costly. Additionally, managers on the enterprise end of the business need systems online so that they can monitor the operational performance of assets and their availability.

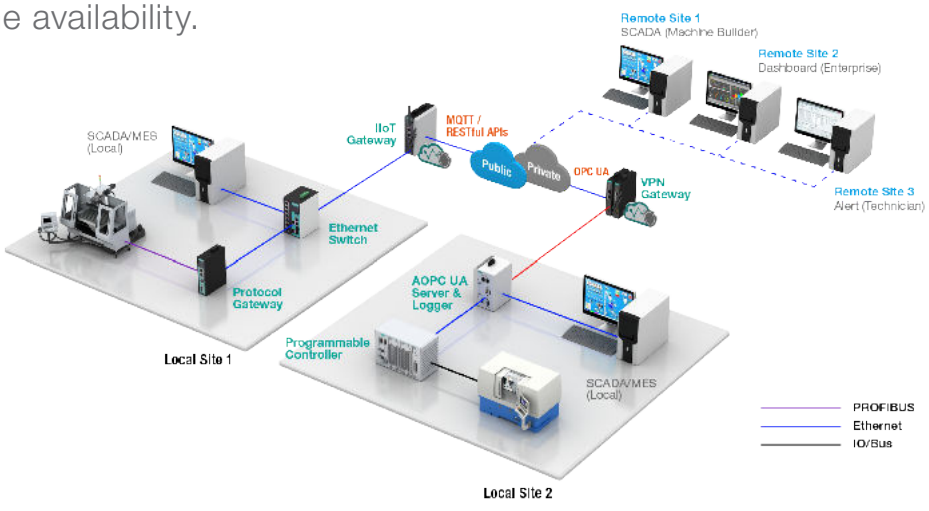
Collecting machine data and connecting systems to the cloud enable remote real-time monitoring and remote maintenance of your factory and machines. With full transparency

to machine performance, system status, and more importantly, hard data, managers are able to keep track of current machine performance. Operators can even see historical data on similar machines to predict performance variation outside of the acceptable boundaries. With this abundance of data, software engineers are able to build a mathematical model based on per-alarm occurrences to predict machine failure, so the operators can proactively schedule maintenance, improving the Mean Time To Repair (MTTR) and saving significant profit loss from downtime and repair.

Combining this real-time information with remotely connected maintenance software also allows operators to service machines remotely before costly issues can occur, and with this knowledge they can have the technician scheduled to arrive outside peak operating hours to avoid downtime. Here are two different use cases for CNC machine status monitoring:

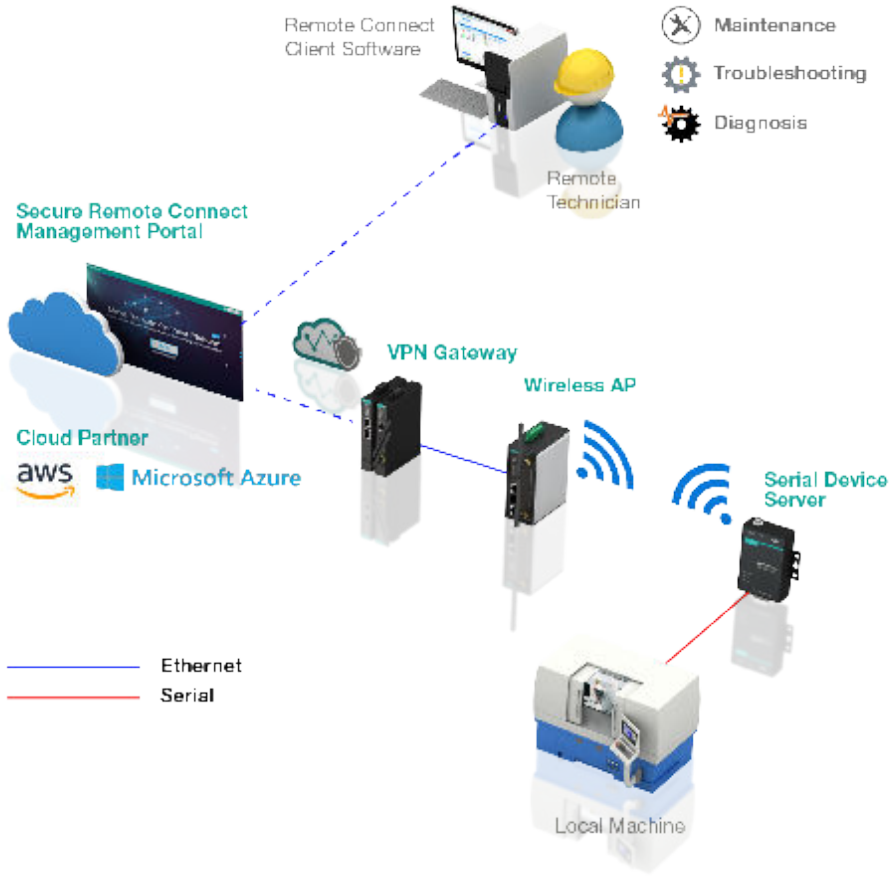
OPC UA:

The customer can use the Moxa OPC UA suite to collect production and machine data to acquire Overall Equipment Effectiveness (OEE). Temperature, current, oil level, and pressure data can be gathered and pushed to a private cloud over a VPN gateway. On the other hand, the customer can also use an IIoT gateway to collect the machine data and push it to a public cloud, such as Microsoft Azure, and perform data analysis through an Azure provided, or user-developed algorithm to find abnormal patterns. Through this approach, the machine maintenance engineer can complete predictive maintenance based on the results. As a result, unexpected machine shutdown can be avoided to increase machine availability.



Remote Access Gateways:

Remote maintenance can also be achieved by connecting equipment to IIoT-ready remote access gateways. The data is sent to MES and SCADA/Cloud Asset Performance Management software for analysis and will notify you when there are operation anomalies that affect your production quality. This can include abnormal vibration of the CNC machine, malfunction of the conveyer linear motor, or when the temperature for a reflow machine in a SMT production line drops too low. Being able to detect and take action ahead of time saves cost and time, boosting production efficiency.



If you are planning to implement predictive maintenance, Moxa can help. We offer connectivity and networking devices that bring the data from your production equipment to SCADA/MES systems. To speak to someone about how you can connect your devices for remote monitoring and maintenance, reach out to one of our industrial networking professionals.

Mass Customization

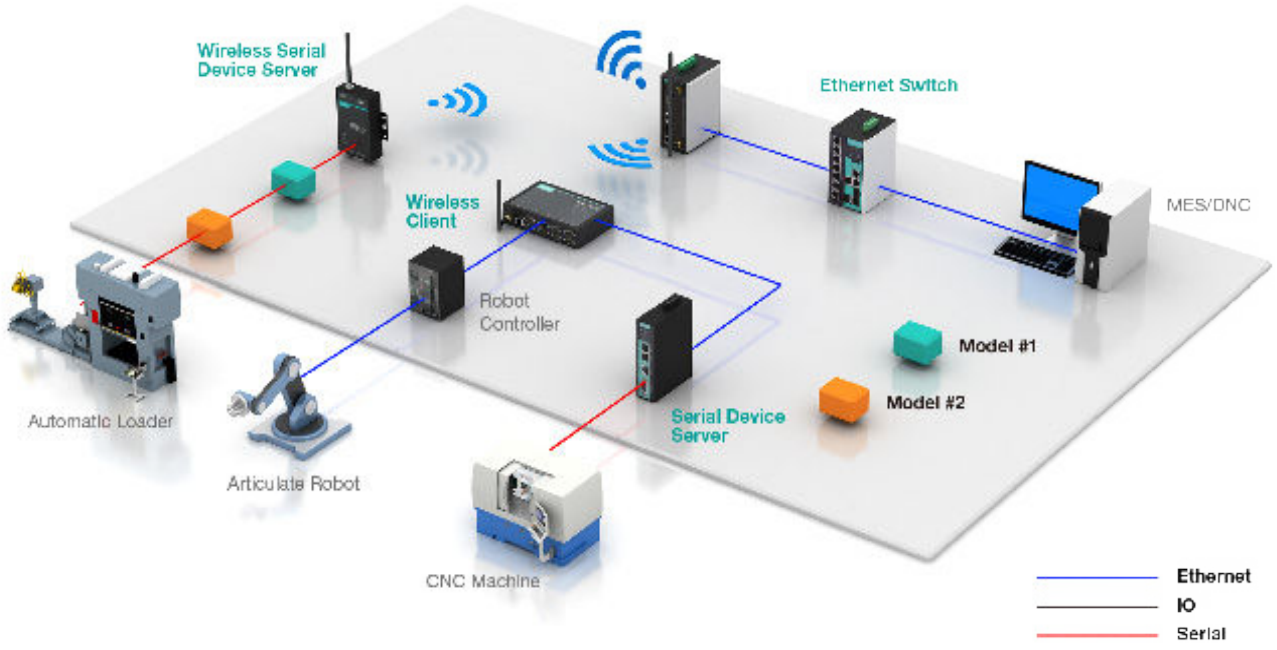
Mass customization enables manufacturers to deliver customized products to customers while keeping production costs low. To accomplish this, custom customer orders are intelligently integrated with Enterprise Resource Planning (ERP) systems or other smart applications, and mapped with the inventory system, so upstream materials can be ordered if necessary. These systems and applications will then connect to the Advanced Planning & Scheduling System (APS) and MES/SCADA systems to initiate standardization, mass production, custom production, and mixed model production.

Mass customization is achieved through smart production lines comprised of several heterogeneous smart machines to support both standardized and customized products. An increasing amount of manufacturers today need this flexibility to adjust to changing customer requirements and custom orders. OEM operators can meet these business demands by transitioning their equipment to smart machines in order to adapt to the complex production models.

By connecting factory equipment to smart sensors, PLC/edge computer and the MES, shop-floor equipment can download user/OEM developed programs to execute intelligent procedures according to the automated changeover commands. This results in minimal breaks in the production process so that business can continue.

An example of how this works is explained in the following diagram. Serial device servers and wired/wireless industrial networking devices can be connected to factory equipment to extract data such as product ID. Then, networking hardware such as wireless access

points and Ethernet switches are applied to transmit the information over to your MES/DNC (Direct Numerical Numerical Control) server. The MES/DNC sends changeover commands and G-codes over the network to each connected factory machine. This process allows CNC machines and robots to download more information to become adaptive smart machines and carry out their jobs effectively.



An adaptive smart machine can perform changeovers on the fly and reconfigure itself with different production modules on the same base machine platform. It can adapt to constant size and format changes to reduce system downtime and increase production efficiency. By enabling this adaptive intelligence, production lines remain operational and continue to produce the next order. However, in a mixed production scenario, the MES must handle more coordination commands with limited computing capability. To alleviate this extra load, edge computers play the important role of handling the partial decision-making (of the production loop) of the MES. Edge computers reduce the communication latency and any risks to production stops, by autonomously running the entire production processes of the loop in case the MES connection drops off.

Download our application note for a closer look at implementing mass customization.

Smart Logistics

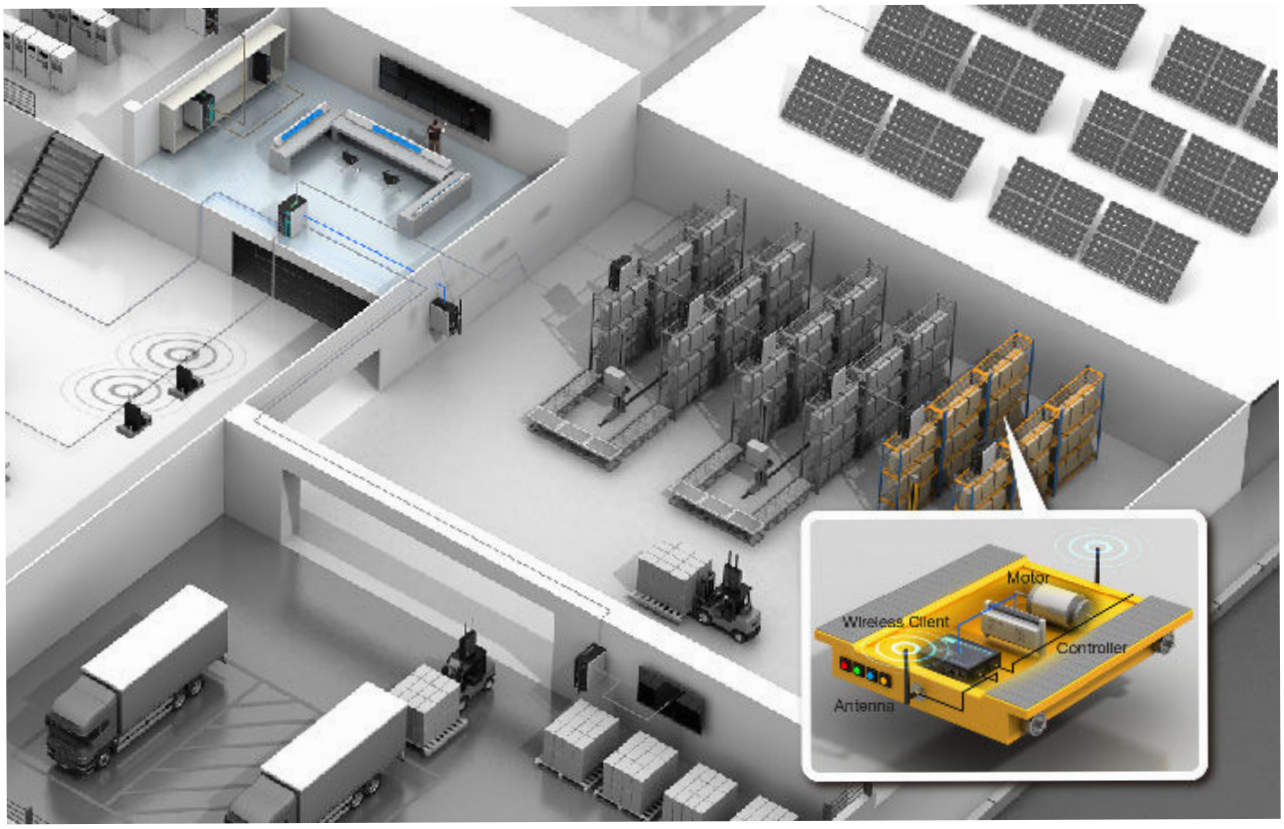
Smart logistics is all about orchestrating the internal movement of parts, incoming materials, tools across production lines, and outgoing delivery. For both standard and custom production lines, smart logistics plays an important role to ensure a smooth end-to-end process that reduces the work-in-progress (WIP) inventory and improves customer satisfaction. In this section, let's explore the different ways intelligence from big data can be used to improve internal and external logistics operations.

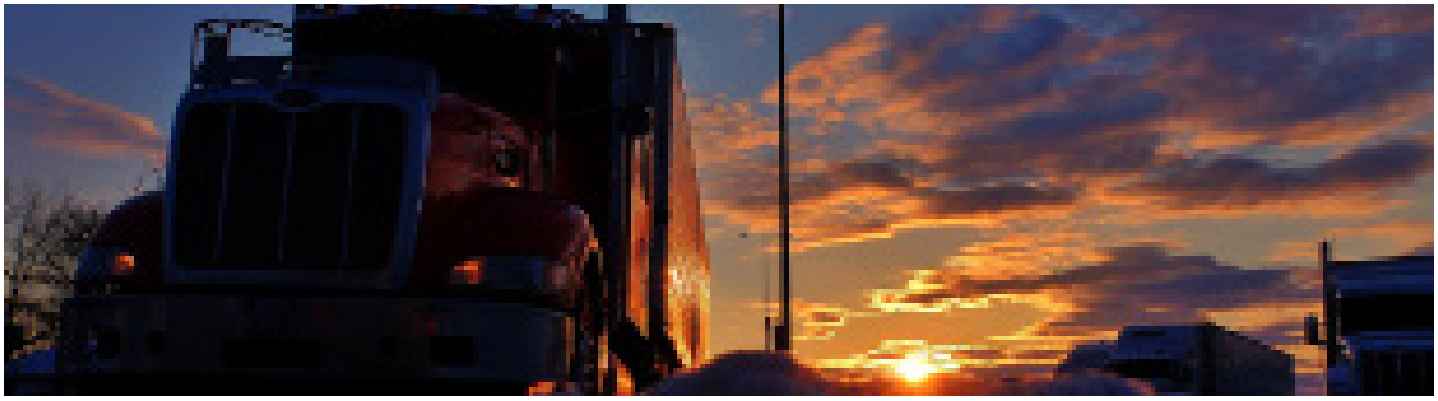
Internal Logistics

Investing in smart logistics is a natural progression after enabling smart production activities. Automatic guided vehicles (AGV) play a key role in streamlining logistical activities and it's important that the communication to and from the AGVs is reliable. Not only do your AGVs need to communicate with each other, but also your smart production line must speak to the AGV Distributing System, which is connected to the warehouse management system (WMS) or the MES. By connecting sensors, gateways, industrial computers, and wireless systems to AGVs, the AGV Distributing System can direct the AGVs to move the WIP assets to the next stage in production, therefore streamlining the process and decreasing WIP inventory.

Your shop-floor drones can move anywhere from the warehouse, auto-storage/retrieval system (AS/RS), or tooling storage to perform programmed tasks. This includes refilling or refeeding materials or replacing tools, all with seamless mobility whenever the smart production lines send material shortage or changeover signals to the MES. For the production line to communicate with the AGV distribution system, serial gateways, protocol gateways, and wireless devices are used to send the information. For this to happen, RFID is used to sense the product ID and send it to the WMS and ERP systems, which then communicate with the AGV distributing system to dispatch AGVs to the production line via connected serial gateways, protocol gateways, and wireless networks.

Once the communication takes place, the AS/RS system can pick up the product for shipment. Wireless access points are used to transmit the information back and forth between the AS/RS and AGV distribution systems to accommodate the mobility needs of the AGVs. Therefore, when designing the network setup, look for redundancy features for your wireless network so that communications are not dropped with the constantly moving equipment and potential signal interferences. By doing so, you will enhance the reliability of your internal logistics network.



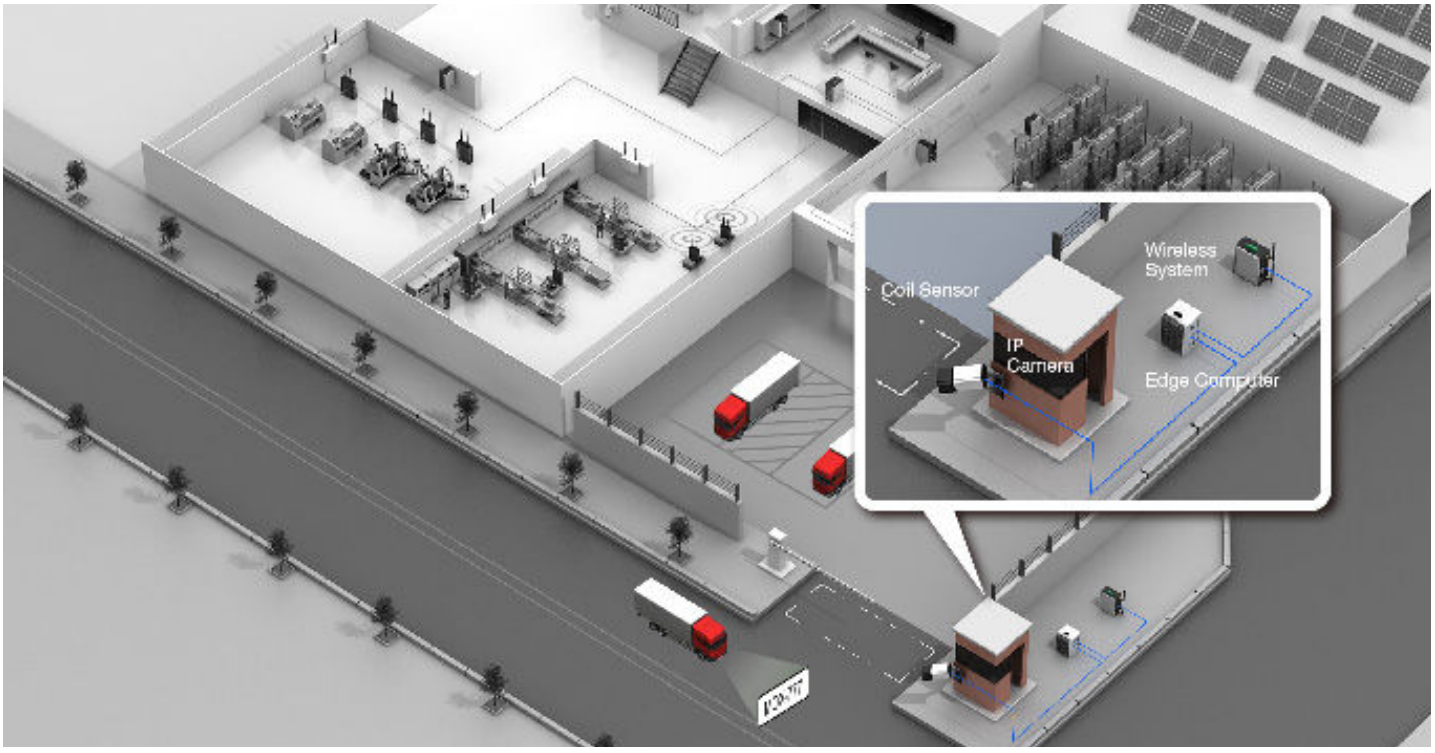


External Logistics

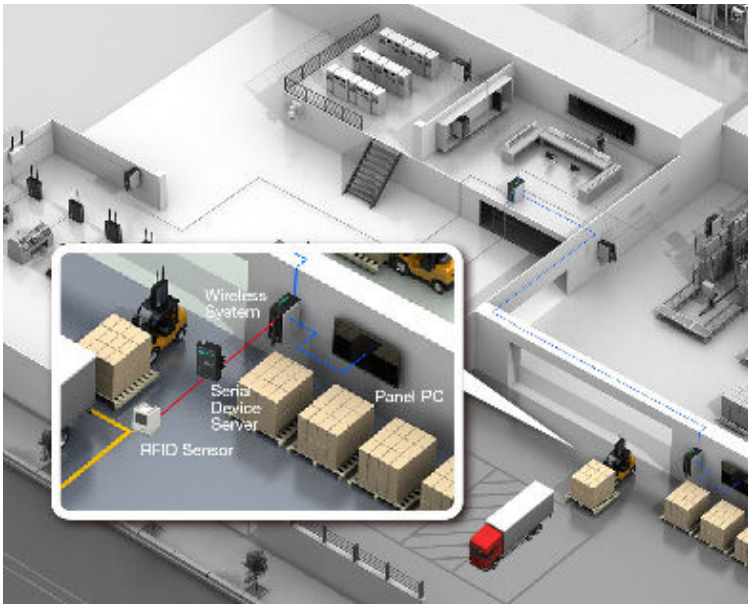
Just-in-time (JIT) manufacturing is an inventory strategy companies use to increase efficiency, decrease waste, and reduce inventory costs by receiving goods only as they are needed in the production process. In a traditional mass production model, this method requires producers to accurately forecast demand. In a smart factory with mass customization, the customer order and the inventory and supplier systems are all connected to streamline the schedule of incoming materials to be “just-in-time” for the production process. By employing JIT, outgoing deliveries to customers will also have a more reliable schedule.

To achieve the JIT manufacturing strategy and on-time delivery, your external logistics must be able to communicate to internal production activities to streamline the end-to-end process. Similar to your internal logistics, supply chain vehicles and Transportation Management System (TMS) must also communicate with the warehouse and production line. Thus, the TMS should be connected via Ethernet to other systems such as the ERP, MES, WMS, and AGV Distribution Systems. This means that your entire operations, from machines to production lines, to internal and external logistics, should all be speaking to each other and working as a team. Without this synergy, your “smart factory” will be operating as isolated units and won’t be able to work as efficiently as those that are. Once your manufacturing and logistics are working in synergy, you can auto-dispatch and coordinate vehicles to schedule incoming materials and outgoing delivery to the customers, streamline the end-to-end process, and further enhance your customer’s experience.

An example of how this can work is by connecting coil sensors and IP cameras to the industrial computers and wireless systems that control the opening of gates at loading docks. The cameras should recognize the license plates of supply chain vehicles and open the gates when necessary. The plate numbers will be verified through a plate recognition system in the control room via an Ethernet switch and wireless systems that are set up to direct vehicles to a designated dock through a panel PC that connects to the TMS.



The supply chain vehicles will then go to the designated dock where they are identified by RFID sensors connected to the WMS. A panel PC that is connected through a serial gateway and the wireless network will then update incoming and outgoing schedules for the warehouse manager while notifying the WMS to automatically request the AGV Distribution System to dispatch AGVs to receive materials for outgoing shipment.



Closing the Loop to Complete Smart Manufacturing

Closing the Loop to Complete Smart Manufacturing

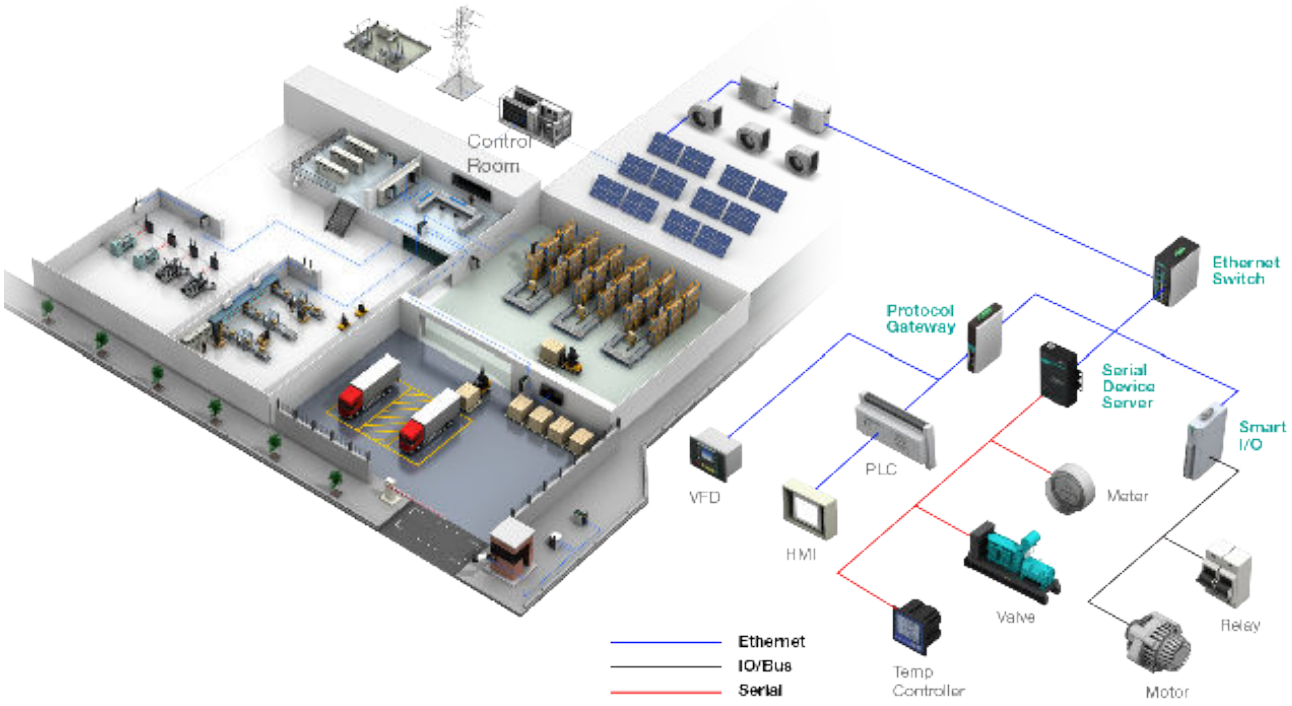
When adopting smart manufacturing, many focus on the internal operations and ways to improve production efficiency. Although these should be a major focus, additional areas that will further lower overhead costs through technology can also be explored. For complete end-to-end smart manufacturing, take a closer look at the building itself and you will find other ways technology can improve your bottom line. In this section of the blueprint, we will cover smart building solutions and why they play an important role for manufacturers.

Smart Building Solutions for Manufacturing Facilities

A connected smart building is built to support the diverse production activities with better energy efficiency, safety and security, and sustainability. With the integration of the IIoT, manufacturers are moving towards a digitalization opportunity to build a smarter, more optimized, and manageable manufacturing facility. Facilities are now being connected to deliver operationally efficient, safe, and profitable manufacturing processes.

> With the integration of the IIoT, manufacturers are moving towards a digitalization opportunity to build a smarter, more optimized, and manageable manufacturing facility.
>
> Click to tweet this

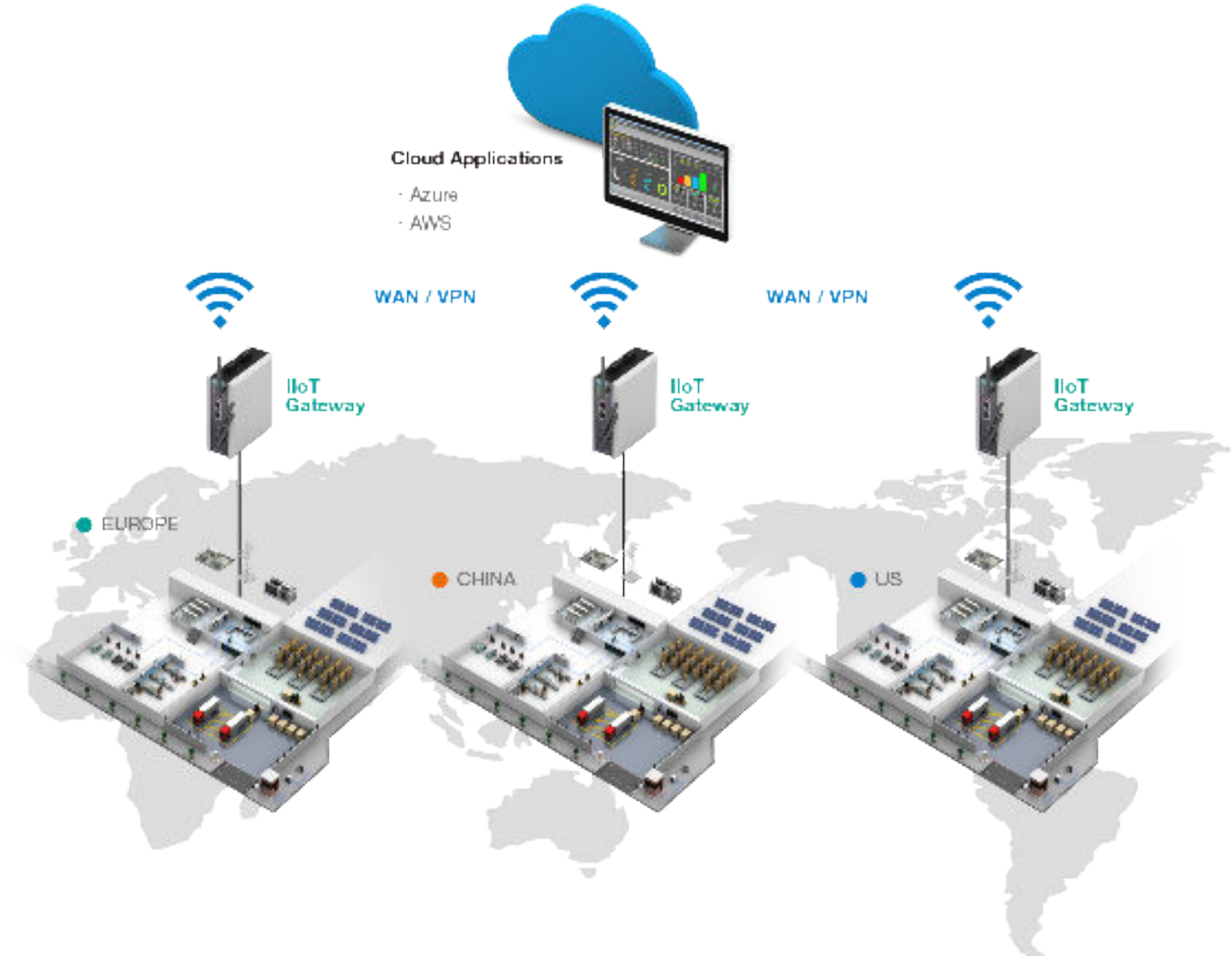
Identifying areas for energy savings is a common first step when creating a smart building. In fact, energy management is crucial for modern manufacturing facilities, as they can consume more energy than traditional plants due to the added automation and cloud computing equipment. Despite this, smart technologies are still preferred because they connect the production facilities, data center, lighting, HVAC, etc., to energy monitoring systems, which will increase overall efficiency by making adjustments based on predefined needs. More specifically, by connecting sensors, meters, protocol gateways, and IIoT gateways to production facilities (machines, pumps, boilers, air-compressors), the data center (networking devices, UPS, power distributing unit), EV charging, lighting, elevators, HVAC, and refrigerators, managers could monitor the energy consumption of the entire building and the health of all factory assets from the energy management systems based in the control room.



With the information collected, the manager can identify problems (e.g., power consumption anomalies in the data center) and deploy a smart energy management plan, such as designing the cool or hot aisle strategies for the data center, adapting geothermal heat pump technologies, auto-detecting outdoor luminescence and temperature to adjust indoor lighting and AC, regenerating power from elevator movement, or shifting energy usage with an Energy Storage System (ESS).

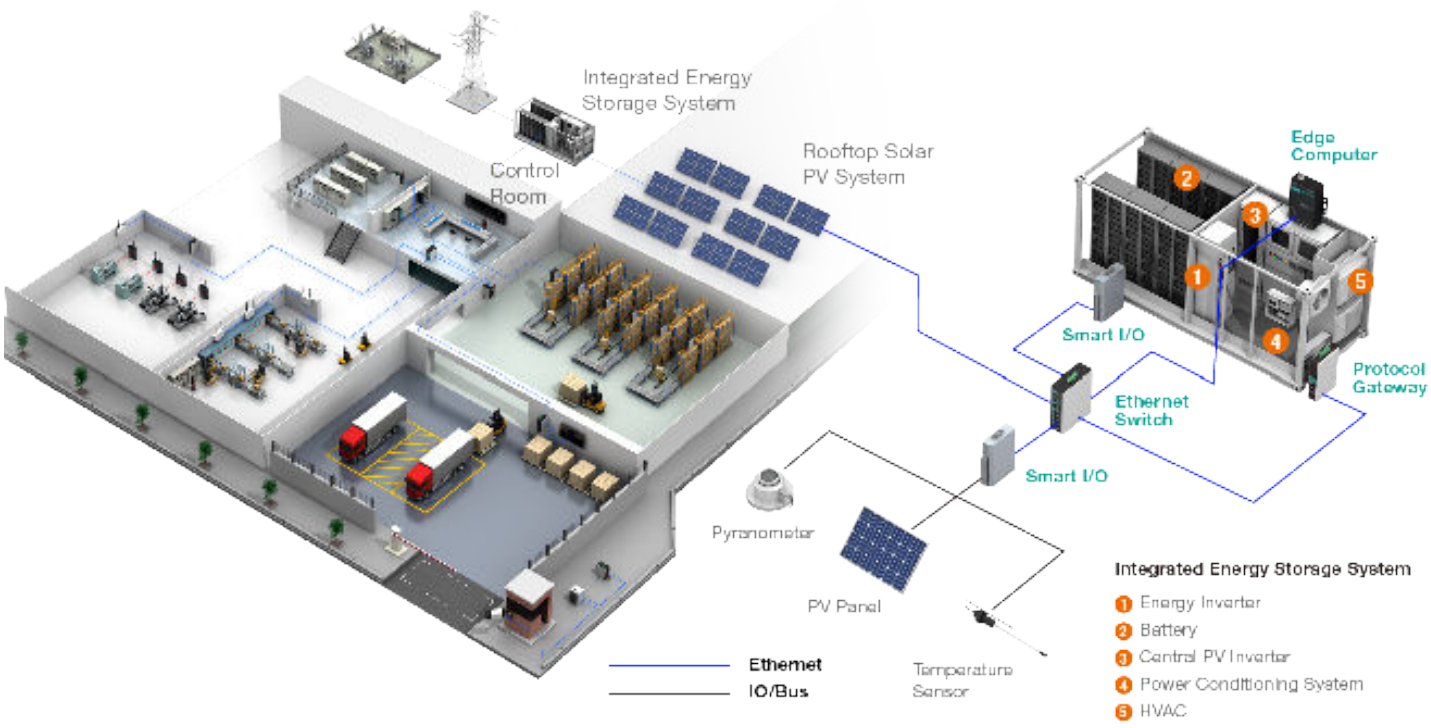
Incorporating any one of these techniques contributes to increased energy efficiency and lower operational costs. In many ways, all this is similar to designing a connected home that is optimized for energy saving. The difference is that in a commercial building, a lot more components and connected devices need to be considered. Additionally, the potential cost savings are much higher than a residential application.

By connecting IIoT gateways to multiple production sites, managers can monitor and compare the energy consumption and health of all factory assets through cloud applications. Additionally, managers can deploy different smart asset management strategies to the connected facilities or find alternative plans that increase asset performance and efficiency.



To close the loop with energy efficiency for a smart building, you need to create your own microgrid. A microgrid is a self-contained power system that has the ability to locally generate, distribute, and store energy. It also has the option to work in parallel with or independently from the main grid. This provides reliability for your business should anything happen to the main grid, such a blackout. When a microgrid is created for a manufacturing facility, it provides the energy for factory systems to operate. Depending on how much power generation the microgrid is capable of and the energy demand of the factory, you might be able to create a fully sustainable building. If this is achieved, your smart building becomes a Net Zero Energy Building (NZEB), which is a building that produces enough renewable energy to meet its own annual energy consumption requirements. The renewable energy supports normal factory operations, and the ESS ensures consistent operating power and provides the flexibility of peak shaving with the grid. Peak shaving helps commercial businesses save money because it reduces the peak demand penalty charged by utilities during high-usage periods.

In the diagram shown here, we illustrate how the inverter and energy storage system can be connected through networking equipment to provide operation managers the information they need to run an energy-efficient factory.



Cybersecurity for Smart Manufacturing

Traditional factories have long been an information silo with fewer cybersecurity concerns than enterprise networks, which typically have numerous external access points. Nowadays, smart factories involve mass customization and cloud services, which require IT and OT to be integrated by connections to sensors, machines, and production lines. Through technology, smart factories can consolidate data, making the Industrial Control System (ICS) network in these factories more vulnerable to external and internal threats, such as hacking, malicious attacks, or even malpractice by employees.

To address these issues, the top priority when enabling cybersecurity is to allow only necessary traffic on mission-critical networks. In other words, you need to create a “clean” network environment to protect smart machines, production lines, and ultimately your entire factory. This level of protection is achieved with industrial firewalls and other industrial networking devices that comply with the IEC 62443 industrial security standard. IEC 62443 defines guidelines for different parts of a network and those who perform different responsibilities on the network.

Protect Your Smart Machines

General firewalls can filter data at the IP or MAC layer to prevent any unauthorized access to critical machines and equipment. Traditionally, firewalls deny all inbound traffic and allow only one-way or round-trip traffic that is on firewall whitelists. However, whitelisting only blocks unauthorized hosts but grants access to all authorized hosts at the IP or MAC layer. As network complexity increases with smart factories connected to the IIoT, whitelisting traffic control is inadequate to provide effective network

security for industrial applications. What is needed are well-designed firewalls that can allow or deny traffic based on protocols to enable checks on control data commands at the application layer, such as Modbus TCP deep packet inspection. For more details, download our white paper on How to Choose the Right Industrial Firewall: The Top 7 Considerations.

Protect Your Smart Production Line

Mass customization production lines are comprised of heterogeneous machines that communicate in different languages (protocols). As such, it's always a challenge for general industrial users to configure security-related parameters.

In order to manage the complex network with ease and prevent unauthorized access, use a comprehensive automation profile function that supports most common fieldbus protocols, including EtherCAT, EtherNet/IP, FOUNDATION Fieldbus, Modbus/TCP, and PROFINET. Users can easily create a secure Ethernet fieldbus network from a user-friendly web UI with a single click.

Protect Your Smart Factory

To enhance the entire network security of your smart factory, the traffic that passes between the ICS and enterprise networks must be scrutinized and filtered. Cybersecurity experts believe that one of the best methods to filter traffic is to pass the data through a demilitarized zone (DMZ). By using a DMZ, there is no direct connection between secure ICS and enterprise networks, but the data sever is still accessible by both. Eliminating a direct connection between secure ICS and enterprise networks significantly reduces the possibility that unauthorized traffic can pass through to different zones, which have the potential to jeopardize the security of the entire smart factory network. For more information on industrial network security, here are 3 Aspects to Consider When Securing IACS Networks.

Technologies Behind Smart Manufacturing

Technologies Behind Smart Manufacturing

As we know, there are specific technologies required to enable smart manufacturing. Based on the topics we've covered in this blueprint, here is a breakdown of connectivity, networking, and computing hardware that ties it all together.

For more information on smart manufacturing solutions, check out our website at: https://www.moxa.com/manufacturing

Smart I/O

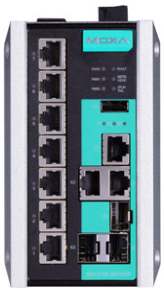
Smart I/O devices perform real-time data acquisition of connected machines and are used to collect sensory data from motors, meters, pumps, fans, temperature sensors, etc. They support IT and OT protocols to make it easy to integrate with SCADA/MES systems and push data updates either to private or public clouds for further analysis.

Serial Gateways

Serial gateways convert serial to Ethernet (or Wi-Fi) so that legacy equipment can be connected to IP systems, enabling remote management. A common use case is to connect legacy serial-based machines to CNC servers through Ethernet. This is a cost-effective way to modernize plant floor machines by making them Ethernet-ready.

Protocol Gateways

Protocol gateways translate the different languages present on industrial networks. They can be used to convert Modbus serial to Modbus TCP, Modbus to DNP3.0, J1939 to Modbus RTU/ACSII/TCP, EtherNet/IP, PROFINET, and OPC UA.



Ethernet Switches

Industrial-grade switches offer the reliability needed to create the network backbone of smart manufacturing facilities. They transmit all the data between plant floor equipment and SCADA/MES systems. More advanced switches even offer Time Sensitive Network (TSN) technology for added reliability. Reduce operational downtime by looking for fast redundancy capabilities, high MTBF specifications, and built-in security features.

Wireless Access Points & Clients

Wireless access points can be used as part of your network infrastructure in situations where Ethernet cables are difficult to run. Smart logistics systems that incorporate Shuttles and AGVs use wireless as a means of communication between devices as well as with the network.

Industrial Routers

Industrial routers are a critical part of protecting ICS networks from internal and external security threats. With increased remote access capabilities, manufacturers must enable layered security and use best security practices such as those listed under IEC 62443-4-2 standards.

IIoT Gateways

IIoT gateways are specialized edge computers that can easily connect geographically dispersed devices to the cloud, especially in outdoor or rugged environments. They serve multiple functions from protocol conversion, data process, and remote monitoring—all in a compact solution.

Edge Computers

Industrial edge computers are built with high-quality materials, innovative technologies, and thermal management features, which are requirements to work reliably in harsh environments. They come in several configurations, interface options, and form factors to serve various edge applications.

Our experts are available if you have questions about industrial edge connectivity, networking, or computing hardware for smart manufacturing systems. Contact Moxa today.

Your Trusted Partner in Automation

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With over 30 years of industry experience, Moxa has connected more than 50 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures.

Moxa Sales and Marketing Headquarters

Moxa Corporate Plaza
601 Valencia Ave., Suite 200
Brea, CA 92823, U.S.A.
Toll Free: 1-888-669-2872
Tel: +1-714-528-6777
Fax: +1-714-528-6778
usa@moxa.com

Moxa Design and Engineering Headquarters

Fl. 4, No. 135, Lane 235, Baoqiao Rd.
Xindian Dist., New Taipei City,
Taiwan, R.O.C.
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

The Americas

Moxa Americas

Toll Free: 1-888-MOXA-USA
Tel: +1-714-528-6777
Fax: +1-714-528-6778
usa@moxa.com

Moxa Brazil

Tel: +55-11-2495-3555
Fax: +55-11-2495-6555
brazil@moxa.com

Europe

Moxa Germany

Tel: +49-89-37003-99-0
Fax: +49-89-37003-99-99
europe@moxa.com

Moxa France

Tel: +33-1-30-85-41-80
Fax: +33-1-30-47-35-91
france@moxa.com

Moxa UK

Tel: +44-1844-355-601
Fax: +44-1844-353-553
uk@moxa.com

Asia-Pacific

Moxa Asia-Pacific and Taiwan

Tel: +886-2-8919-1230
Fax: +886-2-8919-1231
asia@moxa.com
japan@moxa.com
taiwan@moxa.com

Moxa India

Tel: +91-80-4172-9088
Fax: +91-80-4132-1045
india@moxa.com

Moxa Russia

Tel: +7-495-287-0929
Fax: +7-495-269-0929
russia@moxa.com

Moxa Korea

Tel: +82-2-6268-4048
Fax: +82-2-2125-5050
korea@moxa.com

China

Moxa Shanghai

Tel: +86-21-5258-9955
Fax: +86-21-5258-5505
china@moxa.com

Moxa Beijing

Tel: +86-10-5976-6123/24/25/26
Fax: +86-10-5976-6122
china@moxa.com

Moxa Shenzhen

Tel: +86-755-8368-4084/94
Fax: +86-755-8368-4148
china@moxa.com

MOXA®
Reliable Networks ▲ Sincere Service