Revolutionizing Industrial Computers: Boosting Efficiency, Security, and Automation

CONSULTING - SPECIFYING engineer® eBOOK

MOXA®

Contents

MOXA®

Navigating the Critical Role of Industrial Computers in Industry 4.0

Back to TOC

The industrial sector is in the midst of a transformative era marked by the integration of advanced technologies and smart manufacturing processes. The role of x86-based industrial computers is pivotal in this evolution, offering the necessary processing power, flexibility, and security to meet the demands of modern industrial applications. By adhering to best practices in selecting and implementing these systems, industrial automation managers can ensure the success and efficiency of their operations, paving the way for a more connected and intelligent industrial future.

The industrial landscape has undergone a profound transformation since the advent of Industry 4.0 in 2011. This revolution has introduced significant advancements in digitization, connectivity, and data processing within the manufacturing sector. The integration of technologies such as cloud computing, the internet, blockchain, sensors, analytics, and intelligence has facilitated real-time data analysis, predictive maintenance, and predictive decision-making. The synergy between human and machine interactions has also intensified, driven by innovations in virtual reality (VR), augmented reality (AR), robotics, automation, and autonomous vehicles. Furthermore, precision engineering fields like 3-D printing, renewable energy, and battery management have emerged, signaling a new era of industrial progress.

Rising Demands in the Industrial Sector

The surge in digitization and connectivity has led to an increased demand for data, processing power, and efficient industrial PCs (IPCs). Modern IPCs must offer high performance, low power consumption, and affordability to ensure a lower total cost of ownership (TCO). As we delve deeper into Industry 4.0, smart manufacturing is be-

Back to TOC

coming the norm. This trend involves integrating the Internet of Things (IoT), artificial intelligence (AI), and machine learning (ML) into industrial processes. The applications stemming from these integrations push the boundaries of automation, necessitating more extensive data collection, advanced processing capabilities, real-time analytics, security, and enhanced connectivity.

The Role of x86-Based Industrial Computers

The x86-based systems are at the forefront of this transformation due to their versatility and robustness. Analysts predict that industrial PC suppliers will increasingly focus on AI applications, driven by the rise of edge computing and the diverse requirements of operational technology (OT) environments. The OT landscape now includes various hardware components such as serial and parallel devices, managed and unmanaged switches, and network connectivity devices. Additionally, digital transformation in OT has paved the way for hardware and compute retrofits and upgrades.

Evolving Operational Technology Landscape

Industrial computers play several crucial roles within an OT topology:

- **Edge Computing:** By processing data locally, industrial computers at the edge reduce latency and enable real-time decision-making. Distributed architectures facilitate resource distribution across various locations.

- **Control Systems:** Industrial PCs act as controllers for automated processes, including programmable logic controllers (PLCs) and distributed control systems (DCS).

Back to TOC

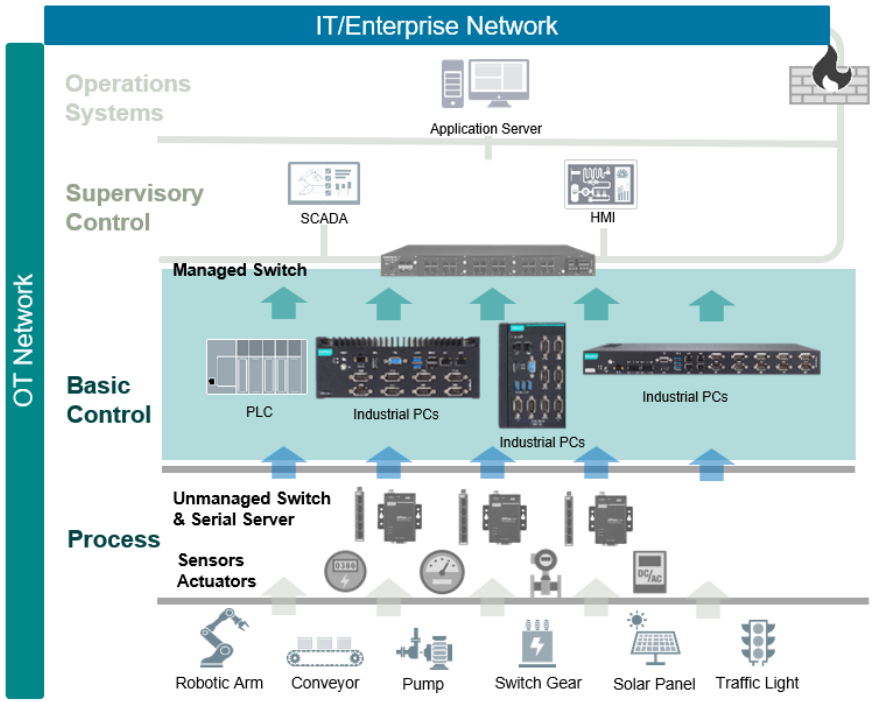
- **Data Gateways:** These computers collect data from sensors and devices, transmitting it to central systems for further analysis.

- **Human-Machine Interface (HMI):** Industrial PCs provide interfaces for operators to monitor and control processes, ensuring seamless human-machine interaction.

The integration of OT with IT is leading to more connected and intelligent systems, enhancing efficiency but also introducing challenges such as cybersecurity risks, interoperability issues, and the need for real-time data processing.

Industrial Network Topology

A typical OT network topology can be divided into four functional categories:



Back to TOC

- **Field Layer:** This includes embedded controllers, sensors, actuators, and other devices. Examples include robotic arms and conveyor belts in factories, pumps and meters in oil and gas, IEDs and switch gears in energy, and traffic control systems in transportation.

- **Control Layer:** Comprising PLCs, RTUs, and IPCs.

- **Supervisory Layer:** Including SCADA, HMI systems, and IPCs.

- **Enterprise Layer:** Connecting OT with IT systems.

New applications such as energy management, remote maintenance, predictive maintenance, and big data-based decision-making require more information from the plant floor. This trend benefits IPCs, which are better suited for data processing than traditional PLCs.

Best Practices for Selecting Industrial Computers

Choosing the right industrial computer is crucial for the success of automation initiatives. Here are some best practices for industrial automation managers:

- **Define Requirements:** Understand the specific needs of your application, including compute power, environmental conditions, connectivity, and compliance requirements.

Choose the Right Form Factor:

- DIN-Rail Type Computers: Box type, DINrail type, Rackmount type, VESA or others.

Back to TOC

Please refer to our x86 brochure or our website for detailed formfactor descriptions.

Evaluate Key Features:

- **Compute Power:** Ensure the computer can handle your application's processing demands.
- **Reliability:** Look for rugged designs with high Mean Time Between Failures (MTBF) ratings.
- **Modularity:** Opt for systems that allow easy upgrades and maintenance.
- **Scalability:** Choose systems that can scale with your operational growth.
- **Serviceability:** Ensure ease of maintenance and availability of support.
- **Ensure Security and Compliance:** Prioritize systems with robust security features and ensure compliance with relevant industry standards and regulations.

Selecting the right supplier is equally important. Choose a supplier with a proven track record in your industry, one who invests in innovation and can provide future-proof solutions that evolve with technological advancements. Also, ensure the supplier offers comprehensive support, including technical assistance, training, and after-sales service.

Three things to consider when deploying edge computing

Back to TOC

Edge computing is changing manufacturing in many ways and companies can take advantage of the many benefits it involves. Three aspects of edge computing to consider are highlighted.

Edge computing is changing analytics, artificial intelligence (AI) and machine learning (ML) applications. Substantial investments in libraries and frameworks have provided a new frontier for engineers and operations specialists to integrate these capabilities alongside process control. While the possibilities for valued applications are endless, security, management and scalability must be carefully considered during design.

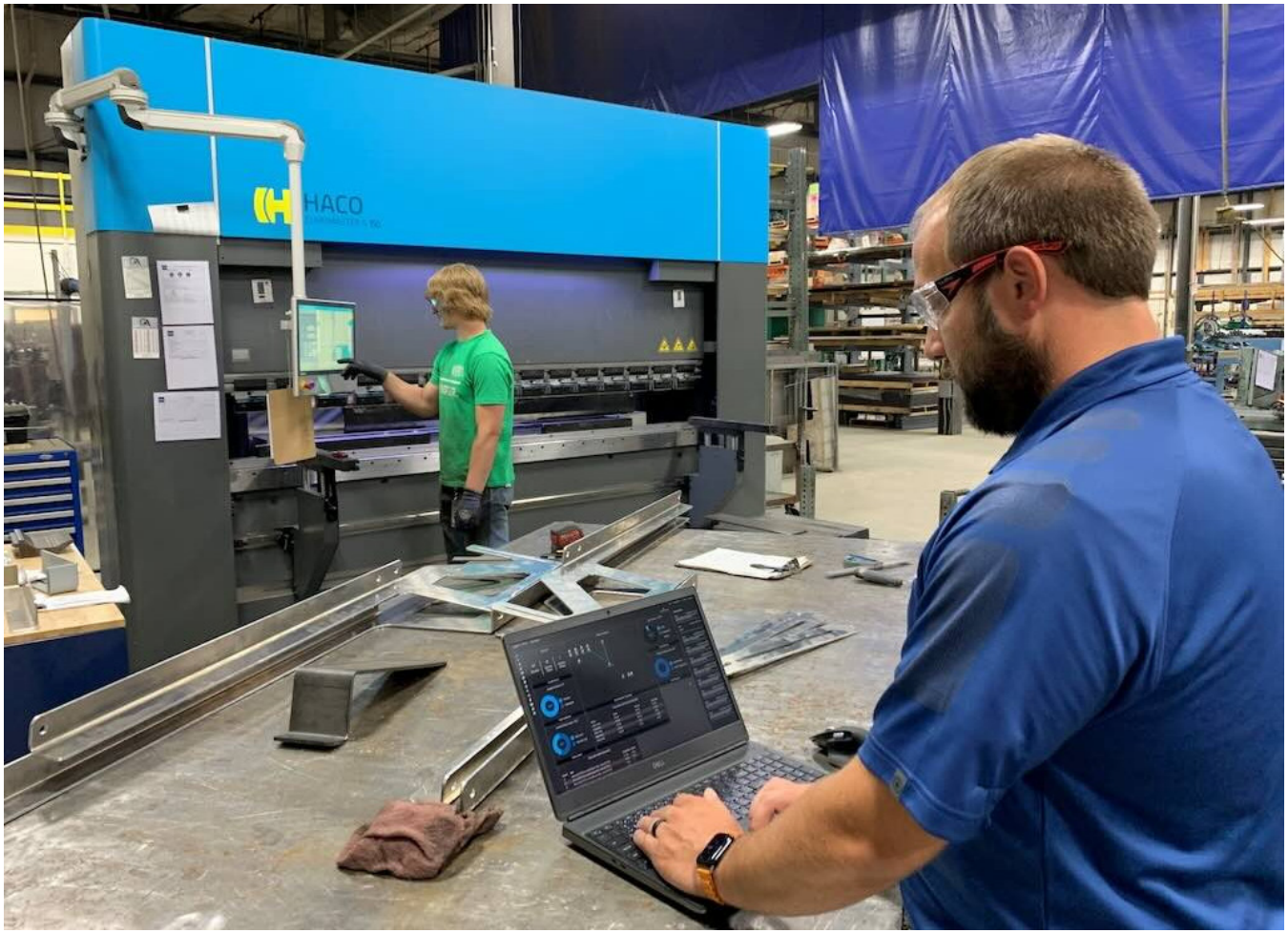
Companies looking to deploy edge solutions need to consider three primary pieces: the applications running at the edge, the infrastructure supporting the edge and the security and orchestration of edge appliances.

1. Edge computing applications

Edge computing refers to the execution of applications near controls processes or machinery. An edge device generally lives on the same network as operational technology (OT) devices and exhibits low-latency communication in data collection and response. An edge device may be a physical appliance; however, a virtual machine (VM) with low network latency to process equipment also can be considered at the edge.

One trade-off between physical devices and VMs is the preference for processing power or flexibility. The decision simplifies down to having edge virtual machines or edge

Back to TOC



physical devices. Virtual machines can be spun up or down as needed providing flexibility in resource allocation.

Companies that invest in security, orchestration and infrastructure at the edge can optimize plant operations and improve their ability to gather data. Courtesy: Interstates

However, it adds a layer of abstraction impacting processing efficiency and introducing latency. Physical devices allow low latency and substantial process power, but they lose flexibility in resource allocation and are often procured for a single application.

Back to TOC

The utilization of edge computing provides a spectrum of advantages, such as quick response times (low latency), efficient use of internet resources (bandwidth efficiency), the ability to handle data in real-time (real-time analytics scalability) and efficient application scalability. Localizing applications removes the need to send data to a central server, reducing the logical distance from data generation and data processing. When properly applied, this approach can result in near real-time solutions; applications gain the capability to make quick decisions and deliver rapid responses. Scaling edge infrastructure is crucial for increasing demands and maintaining performance and responsiveness. Scaling is done by adding an edge device to the infrastructure. The distributed workload limits bottlenecks, increases node management and improves load balancing.

Applications running at the edge are use-case specific and often purpose-built. Some examples include analytics or models to optimize process control such as reducing scrap, improving yield, reducing utility consumption, predictive maintenance and more. Data is brought locally to the edge device to be processed. Raw or aggregate data may be pushed up to enterprise servers or the cloud for further analysis; aggregating the data reduces data transfer and storage costs in the cloud.

2. Edge computing infrastructure

The supporting infrastructure for edge applications is often one of the most unknown aspects when integrating edge applications. Detailed scope of the edge application is required to understand what process parameters need to be collected, what the application's output is, and what defines success in the process.

Additional considerations, such as readiness of the process for data collection and advanced analytics, can be derived from an analytics maturity model. Advanced pro-

Back to TOC

cess analytics require investment in data collection, cleansing, contextualization and storage are supported through complementary infrastructure. Not all organizations are ready for advanced process analytics. Work with analytics experts to ensure these solutions can be supported.

As devices are deployed and applications begin to scale, the network load also increases. Understanding where data is being transferred over the network is crucial to minimizing load issues with the current infrastructure; upgrades of network switches to support larger data sizes may be required to minimize network interruptions from bandwidth contention. Consultation with plant floor network integrators during the planning phases can identify and provide solutions to mitigate network contention.

3. Edge computing security and orchestration

The security of edge devices should be considered first in the design process. Functional requirements of an edge application are used to specify the security requirements for processing data. Common examples of these security requirements may include data encryption in transit and/or rest, transport level security (TLS) communications and system patching. Orchestration platforms also can secure edge devices and manage their lifecycle as well as update devices and their respective applications. An orchestration platform also can operate at scale, providing these services to a large fleet of deployed edge devices. Management actions can be performed across the fleet of devices, such as updating application versions, pushing new analytic models or security patching.

Building solutions on an orchestration platform accelerates the development and scalability of an application. A small proof of concept or pilot solutions can be evaluated

Back to TOC

and deployed to the fleet of edge devices working alongside the process. The speed of innovation on an orchestration platform, alongside the built-in security, affords developers a powerful tool to focus on delivering solutions over managing deployments and architectures.

Edge computing, embedded with AI/ML, opens doors for new possibilities and challenges in controls engineering. Applications at the edge allow for low-latency communications and can be tailored to target various business goals. Understanding and investing in the supporting infrastructure is necessary for analytic and network readiness at scale. Security and orchestration, with a security-first mindset and robust orchestration platform, ensure edge devices are managed and protected endpoints.

Investing in security, orchestration and infrastructure can pave the way for AI/ML solutions at the edge to optimize plant operations.

Jackson Cates, Nick Malott, Tiati Thelan

Jackson Cates *is a Business Analyst at Interstates. He has worked at Interstates for 3 years and serves food and beverage clients with a focus on machine learning, image analysis, and data analytics.* ***Nick Malott*** *is a Technology Analyst with 6 years of experience at Interstates. He specializes in evaluating and designing system architectures for data collection, storage, and advanced analytics spanning a variety of industries and customers.* ***Tiati Thelen*** *is a Business Analyst II at Interstates. She has three years of experience in analytics and has been with Interstates for two of those three years with a specialty in higher analytics.*

Upgrading industrial PC cybersecurity in manufacturing

Back to TOC

Cybersecurity attacks against manufacturers and other industrial sites are growing and companies need to develop a cybersecurity plan that protects industrial PCs and other vulnerable targets that, until recently, were not connected to the internet.

It is no secret our world is more connected than ever. According to Statista, it is estimated there are 36 billion connected devices today. That amount will double by 2025. Where perception differs is whether we are becoming more or less secure. On the one hand, technologies and professional services available to improve security are growing. For example, Markets and Markets estimates that the global cybersecurity market size will grow from $153 billion to $249 billion by 2023.

On the other hand, attacks on organizations are more commonplace than ever, demonstrated by businesses increasingly purchasing cybersecurity insurance to hedge their bets. More shockingly, lists of thousands of victim companies are published online by intelligence companies, which show who has had information released on the dark web. Determining whether overall cybersecurity is getting better or worse is a complicated topic.

Industrial control systems are not keeping up

That question is less complicated when discussing the industrial control system (ICS) environment. It is a landscape held together by legacy hardware and software. Capital and operational costs for the environment is high, so equipment is often run until it fails. Industrial devices are communications are inherently insecure and unencrypted.

Back to TOC

Availability is prioritized over confidentiality and security, providing few or no opportunities for patching during downtime. In many ways, the industrial information technology (IT) infrastructure, which the control systems run on, are exact opposites of their enterprise infrastructure counterparts. The cumulative result is demonstrated in Claroty's Biannual ICS Risk & Vulnerability Report, providing data showing vulnerabilities affecting the commercial facilities sector has increased by 140% compared to 2018.

Putting these trends together, not only is connectivity and the cybersecurity threats organizations face increasing, ICS security postures are not keeping up.

The best lens to view ICS cybersecurity

The ICS cybersecurity problem is incredibly technical, the title of this article is technical and the word "cybersecurity" sounds technical. However, when considering the problem, it is best to look at it through the lens of business risk reduction and enabling innovation. Let those two objectives guide how decisions are made and allow the technical security controls and practices to fall in place behind them.

ICS cybersecurity: Business risk

From a business risk perspective, ICS cybersecurity approaches will parallel an organization's existing EH&S programs, in the sense that everybody plays a role in the cumulative security plan. It requires a mix of people, processes and technology to be effective and is a continuously improving cycle rather than a linear destination. The ultimate goal is quantifying the amount of risk tolerable to the business and then reduce it.

To provide a comprehensive framework for applying cybersecurity best practices within the ICS environment, the International Society of Automation (ISA) and the

International Electrotechnical Commission (IEC) have published a series of standards. The series is made up of 14 standards and technical reports, which address responsibilities that owners, vendors and service providers can follow. Of particular importance for system owners looking to initiate a cybersecurity program for understanding and addressing overall cybersecurity risks is the 62443-2-1 standard titled "Establishing an Industrial Automation and Control Systems Security Program."

ICS cybersecurity: Enabling innovation

The second – sometimes forgotten – lens to view

Back to TOC

Back to TOC

security decisions through is by enabling innovation. The increase in connectivity has provided an opportunity for analytics, cloud and edge computing architectures and more to be leveraged, which can make the business more efficient and agile.

However, security concerns can prevent the adoption of those technologies, and improving security can remove those barriers. Rather than viewing security improvements and being restrictive, identify which security improvements enable the implementation of connected technologies, and weigh that into the decision of security controls to implement during the overall risk management cycle.

It is imperative to think about cybersecurity holistically across the enterprise from a business risk and innovation perspective. In many cases, an organization's steps will be to understand the systems in their environment, preparing for incidents and reducing the likelihood and consequences of an incident. This is where IPS and server lifecycles and patching plays a major role.

The importance of IPC and server patching

Patching as a whole is a small piece of the overall challenge, but it is an incredibly important piece for industrial PCs and servers. In fact, the ISA/IEC-62443 series of standards is made up of 14 standards and technical reports, one of which (Technical Report 2-3) was published specifically to address patch management within the ICS environment.

The ICS environment is made up of many layers of industrial equipment, including Level 2 supervisory control devices and application, Level 1 basic control devices, MES/MOM systems, network infrastructure and more. It can be argued that if only one type of device could be patched, the wisest choice would be Microsoft Windows operating

Back to TOC

systems (OS), which are a common platform for lateral movement by attackers. They are often connected to a large quantity of devices and have the opportunity to be patched without directly impacting the industrial application running on it.

Largest quantity of industrial vulnerabilities

In fact, Level 2 supervisory control devices and applications had the largest quantity of vulnerabilities disclosed in the second half of 2020. So, considering the large amount of business risk reduction that can be achieved by patching Microsoft Windows OS, it is worth prioritizing the effort within the overall cybersecurity management cycle.

From an innovation perspective, managing the overall computing ecosystem can be simplified via consolidation onto virtualized and redundant environments or taking advantage of edge computing to eliminate Microsoft Windows OS equipment on the shop floor. That simplification also makes consistent application of access controls, user controls, resource availability and more. This makes IPC and server upgrades an opportunity for innovation advancement and risk reduction.

Due to the nature of ICS environments, there will be cases where upgrading the IPC is not practical. In those situations, there are security improvements which can be implemented. Hardening the device via shutting down unused services, ports and interfaces can reduce the devices' attack surface. The IPC also can be set up within the organization's domain, enforcing policy and making it possible for the industrial application to authenticate against the IT-managed AD. Finally, the device can be virtually or physically segmented away from other critical assets, reducing the opportunity for the IPC to be used within an attackers kill chain.

Back to TOC

Leverage existing frameworks for industrial PC security

Given the escalation of attacks and the increasing vulnerability of the ICS environment, we are behind schedule with securing the environment. When doing so, it is helpful to leverage the framework provided by the ISA and IEC have published and use business risk reduction and innovation enablement as the decision criteria for implementing security controls.

Data demonstrates that Microsoft Windows IPCs and servers are the most vulnerable, and the most targeted asset. This means managing the lifecycle, patching, and system backups is worth doing. While it is difficult, the choice between investing $1 milion per year to do so, or paying $40 million in bitcoin to a cyber gang to decrypt your devices shouldn't be a choice at all.

Jeff Winter

Jeff Winter, *senior director of strategy and marketing, Grantek.*

The Importance of Best-in Class Services and Support for Industrial PCs

Moxa

The Vital Role of Comprehensive Services and Support in Industrial Computing

In the realm of industrial operations, the reliance on industrial computers (IPCs) is paramount. These high performance and ruggedized processing devices are at the heart of modern automation and, other critical infrastructure sectors. Given the demanding and often harsh environments in which these computers operate, choosing the right IPC supplier—one who provides comprehensive services and support, extended warranties, and guarantees product longevity—is crucial for maintaining operational efficiency and system reliability.

Importance of Comprehensive Services and Support

Industrial environments are unique, often subjecting computers to extreme temperatures, vibrations, dust, and humidity. Such conditions demand robust hardware that can withstand these challenges without faltering. However, even the most rugged IPCs require dedicated support and services. This includes access to expert engineers who can swiftly address and root cause any issues that arise. This level of support minimizes downtime, ensuring that operations continue smoothly and efficiently.

Back to TOC

The value of working with a IPC supplier who has the experience and technical expertise in the Industrial operations is critical. Having accessible engineers cannot be overstated. These professionals not only address failures but can provide any insights from other installations in different verticals in the Industrial space. Whether it's updating software, installing additional hardware, solving an issue, or performing routine maintenance checks, their expertise and quick response times play a pivotal role in keeping industrial operations running without interruption.

Longer Warranty and Product Availability: A Must for Industrial Operators

Choosing an IPC supplier that offers a longer warranty period is another critical consideration for industrial operators. This not only speaks to the confidence that manufacturers have in their products but also safeguards the investment of the operator. An Industrial computer supplier can only offer an extended warranty if they have designed and tested the IPCs for Industrial use cases. The IPCs are designed for Industrial use cases and rigorously tested and approved to ensure high confidence and reliability of the devices deployed worldwide. Extended warranties ensure that any malfunctions or breakdowns are handled without additional financial burden on the facility, thereby contributing to overall cost efficiency and operational predictability.

Moreover, the availability and longevity of IPC products are significant. Industrial processes often rely on specific configurations that need consistent performance over many years. Disruptions caused by discontinued products can lead to forced and often costly upgrades. A supplier that guarantees product availability and longevity helps ensure that operators can maintain and replace their systems without the need to overhaul their entire setup, which can be both disruptive and expensive.

Back to TOC

Partnering with the Right Industrial Computer Supplier

The ideal IPC supplier does more than just sell products. They act as a true partner to industrial operators. This partnership means they understand the specific needs and challenges of their customers and can recommend custom IPC solutions tailored to meet those needs. Whether it's designing a system that can handle extreme conditions or providing a scalable solution that grows with the company, a supplier's ability to deliver tailored solutions is invaluable.

Leveraging strong partnerships with localized channel partners enables these suppliers to offer local technical support and RMA services, significantly lowering maintenance responses and costs for the Industrial customers. In addition, these relationships and partnerships provide maintaining inventory levels and readiness to deliver Configure to order (CTOS) solutions to ensure rapid fulfillment.

For industrial operators, the stakes are high, and the machinery they rely on must meet the demands of a challenging environment. Therefore, selecting an IPC supplier is not just about choosing a product but about choosing a partner who will support the longevity and reliability of their operations. Suppliers who offer comprehensive services and support, extended warranties, and assurances of product longevity not only ensure the smooth running of industrial operations but also contribute to their ultimate success. In a sector where downtime can mean significant financial losses, such assurances are not just beneficial; they are essential.

Looking for more information about Moxa's IPCs?

Check out our on-demand webinar, as we delve into the complexities of industrial environments, where selecting the appropriate computers poses unique challenges. In

Back to TOC

this on-demand webinar, we will guide you through the process of choosing the right computer for your automatic or autonomous industrial use case. From hardware selection to understanding regulatory and environmental requirements, we'll cover it all. Our exploration includes crucial factors such as scalability, reliability, serviceability, and product availability. By the end of this webinar, you'll gain valuable insights on how to mitigate downtime, prevent failures, and achieve peace of mind in your industrial operations. **Watch Now**.

You can also find out more by downloading our new x86 industrial computers brochure and learn how you can choose the best fit for your industrial applications from 75 industry-optimized models. This 8-page brochure explains how our teams and x86 industrial computer portfolios provide comprehensive solutions to enable your success in the industrial automation field. **Download Now**.

Modernize Your Industrial Automation

Moxa

Reliable Design, Exceptional Quality and Support

Modernize Your Industrial Automation With Reliable Design, Exceptional Quality and Support

Moxa introduces a new series of x86 Industrial Computers with a comprehensive range of form factors and performance options to ensure a perfect fit for nearly any industrial use case or scenario. The extensive platform is pre-formulated and designed for highly reliable, flexible, cost-effective and rapid deployment, supported by a 3-year warranty to meet diverse industrial system and application needs.

Featuring 75 basic models, the BXP/DRP/RKP Series allows users to quickly select from predefined form factors, processors, and data interfaces. Our configure-to-order service (CTOS) simplifies system assembly by offering various operating system, memory, and storage options.

By placing a CTOS order, customers can obtain a tailored industrial computer. System integrators and machine builders leverage these computers to create customized solutions, facilitating the swift and seamless implementation of automation scenarios.

Back to TOC

Adaptable

The latest x86 IPC family offers 75 basic models, enabling customers to quickly pinpoint the ideal ready-to-use solution through a 4-step selection process, reducing time to market and expenses.

- Versatile portfolio meets most industrial-automation requirements
- Configure-to-order service (CTOS) for OS, memory, and storage
- 4 simple steps to identify a best fit

Customization Friendly

At Moxa, our aim is to deliver solutions perfectly aligned with your requirements. Leveraging the modular architecture of the latest x86 IPCs, our product development team is adept at rapidly crafting tailored solutions to match your specific needs.

- Favorable customization criteria and service
- Modular design enables flexible customization
- Shorter prototyping and customization process

Reliable and Durable

Drawing from more than 35 years of experience, our dedication lies in delivering optimal value and ensuring the success of our customers with an unwavering commitment to durable quality, consistent long-term supply, and timely support services.

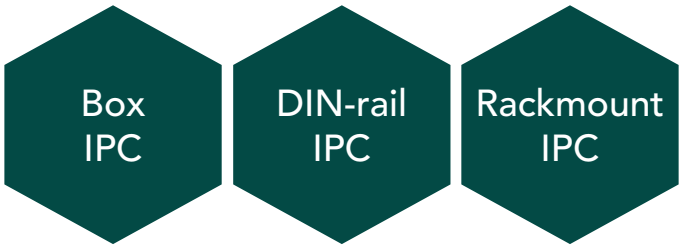
Back to TOC

- 3-year Moxa warranty for product quality
- 10-year product longevity* commitment
- Moxa's industry-renowned post-sales service

*Starting from the product release date 1 in 2023/2024

4-step Selection
BXP/DRP/RKP Series System Architecture

1. Form Factors x 3



› Filter Across 75 Standard Models

2. Interface Options

Back to TOC

3. Processor Types x 5

- Atom® Dual Core
- Atom® Quad Core
- Celeron®
- Core™ i5
- Core™ i7

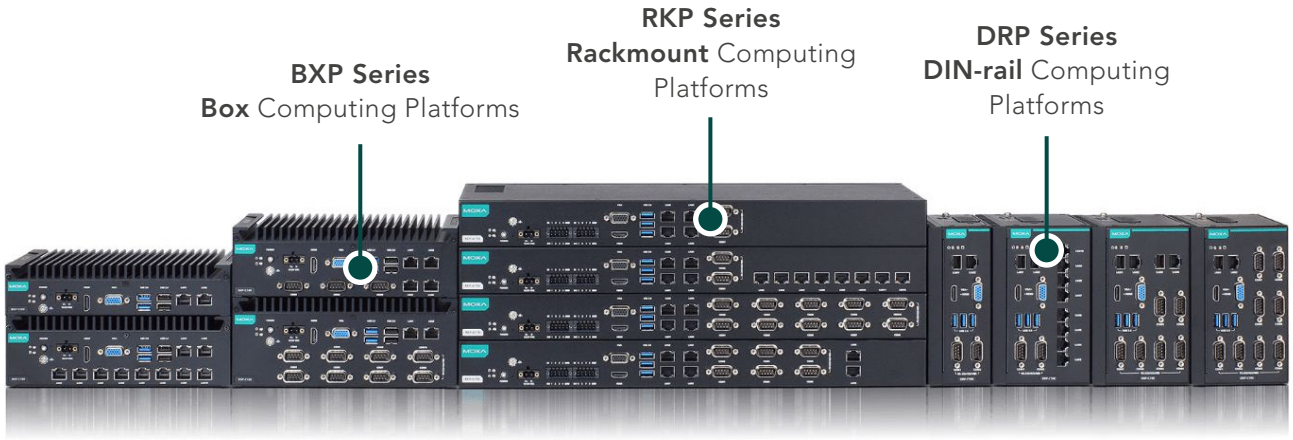
4.

- Storage (SSD)
- Memory (DDR 4)
- Linux OS (Windows)

› Configure to-order Service

BXP/DRP/RKP Series

Intel® Atom®/Core™/Celeron® Powered Industrial Computers



Back to TOC

4-step Solution Formulation for Fast System Development

Simply specify your requirements in three steps to find the computing solution that fits your application from an array of DRP/BXP/RKP Series industrial computers.

1. Select a form factor.

Which computer model can be easily installed in the current system space without requiring additional brackets?

- Box IPC
- DIN-rail IPC
- Rackmount IPC

2. Select interface combinations.

Which devices need to be connected to the computer, and what types of interfaces are necessary for these connections?

- Ethernet
- Serial
- Video
- USB
- DIs/DOs

Back to TOC

3. Select a processor.

Considering your application's data collection and processing requirements, which processor is most suitable for driving optimal performance?

- Atom® Dual Core
- Celeron®
- Core™ i5
- Atom® Quad Core
- Core™ i7

4. Select the final pieces to complete your system.

Save time and cost with our configure-to-order options that get your system ready for use.

- Storage (SSD)
- Memory (DDR 4)
- OS (Windows)

i. System Memory

- 8 GB DDR4 (built-in)
- 16 GB DDR4
- 32 GB DDR4

ii. Storage Capacity

- 64 GB SSD
- 128 GB SSD

Back to TOC

- 256 GB SSD
- 512 GB SSD
- 1 TB SSD

iii. Operating System

- Windows 10 IoT Enterprise LTSC
- Windows 11 Professional

Other interface options are also available upon request such as: CAN Bus, mini PCIe, Wi-Fi, LTE, M.2 SSD and many more.

Quality and Longevity

Our x86 computers are verified against strict industry standards for manufacturing

quality and performance to reduce failures and unplanned downtime, thereby lowering the total cost of ownership.

Back to TOC

BXP Series Box Computers

BXP-C100 Series

Box computers with a Tiger Lake 11th Gen Intel® Core™ processor and models with high-density interfaces




	BXP-C100 (Base Model)	BXP-C100 (Base + 8 LAN)	BXP-C100 (Base + 8 COM)	BXP-C100 (Base + 2 LAN / 3 COM)
Form Factor	Box computer			
CPU	11th Gen Intel® Core™ i7-1185G7E, i5-1145G7E, or Celeron® 6305E			
Video Output	1 HDMI, 1 VGA			
LAN Ports	2	10	2	4
Serial Ports	2	2	10	5
USB Ports	USB 3.0 x 2 + USB 2.0 x 4			
DI/Os	4 DIs, 4 DOs			
Power Input	12/24 VDC			
Certificates	CE, FCC, UL, BSMI			
Operating Temp.	-30 to 60°C			
Dimensions (mm)	210 x 166 x 48	210 x 166 x 65.5	210 x 166 x 83	210 x 166 x 65.5

Back to TOC

BXP-A100 Series

Box computers with an Elkhart Lake Intel Atom® X Series processor and models with high-density interfaces




	BXP-A100 (Base Model)	BXP-A100 (Base + 8 LAN)	BXP-A100 (Base + 8 COM)	BXP-A100 (Base + 2 LAN / 3 COM)
Form Factor	Box computer			
CPU	Intel Atom® Elkhart Lake, dual-core x6211E or quad-core x6425E processor			
Video Output	1 HDMI, 1 VGA			
LAN Ports	2	10	2	4
Serial Ports	2	2	10	5
USB Ports	USB 3.0 x 2 + USB 2.0 x 4			
DI/Os	4 DIs, 4 DOs			
Power Input	12 / 24 VDC			
Certificates	CE, FCC, UL, BSMI			
Operating Temp.	-30 ~ 60°C			
Dimensions (mm)	210 x 166 x 48	210 x 166 x 65.5	210 x 166 x 83	210 x 166 x 65.5

Back to TOC

DRP Series DIN-rail Computers

DRP-C100 Series

DIN-rail computers with a Tiger Lake 11th Gen Intel® Core™ processor and models with high-density interfaces

	DRP-C100 (Base Model)	DRP-C100 (Base + 8 LAN)	DRP-C100 (Base + 6 COM)	DRP-C100 (Base + 2 LAN / 4 COM)
Form Factor	DIN-rail computer			
CPU	11th Gen Intel® Core™ i7-1185G7E, i5-1145G7E, or Celeron® 6305E processor			
Video Output	1 HDMI, 1 VGA			
LAN Ports	2	10	2	4
Serial Ports	2	2	8	6
USB Ports	3 USB 3.0			
DI/Os	-			
Power Input	12/24 VDC			
Certificates	CE, FCC, UL, BSMI			
Operating Temp.	-30 to 60°C			
Dimensions (mm)	60 x 150 x 130	94 x 150 x 130	94 x 150 x 130	94 x 150 x 130

Back to TOC

DRP-A100 Series

DIN-rail computers with an Elkhart Lake Intel Atom® X Series processor and models with high-density interfaces

	DRP-A100 (Base Model)	DRP-A100 (Base + 8 LAN)	DRP-A100 (Base + 6 COM)	DRP-A100 (Base + 2 LAN / 4 COM)
Form Factor	DIN-rail computer			
CPU	Intel Atom® Elkhart Lake, dual-core x6211E or quad-core x6425E processor			
Video Output	1 HDMI, 1 VGA			
LAN Ports	2	10	2	4
Serial Ports	2	2	8	6
USB Ports	3 USB 3.0			
DI/Os	-			
Power Input	12/24 VDC			
Certificates	CE, FCC, UL, BSMI			
Operating Temp.	-30 to 60°C			
Dimensions (mm)	60 x 150 x 130	94 x 150 x 130	94 x 150 x 130	94 x 150 x 130

Back to TOC

RKP Series Rackmount Computers

RKP-C110 Series

Rackmount computers with a Tiger Lake 11th Gen Intel® Core™ processor and models with high-density interfaces

	RKP-C110 (Base Model)	RKP-C110 (Base + 8 LAN)	RKP-C110 (Base + 8 COM)	RKP-C110 (Base + 2 LAN / 4 COM)
Form Factor	Rackmount 1U computer			
CPU	11th Gen Intel® Core™ i7-1185G7E, i5-1145G7E, or Celeron® 6305E			
Video Output	1 HDMI, 1 VGA			
LAN Ports	4	12	4	6
Serial Ports	2	2	10	6
USB Ports	3 USB 3.0			
DI/Os	8 DIs, 8 DOs			
Power Input	12/24 VDC			
Certificates	CE, FCC, UL, BSMI			
Operating Temp.	-30 to 60°C			
Dimensions (mm)	440 x 230 x 43.6	440 x 230 x 43.6	440 x 230 x 43.6	440 x 230 x 43.6

Back to TOC

RKP-A110 Series

Rackmount 1U computers with an Elkhart Lake Intel Atom® X Series processor base model and high density interface models




	RKP-A110 (Base Model)	RKP-A110 (Base + 8 LAN)	RKP-A110 (Base + 8 COM)	RKP-A110 (Base + 2 LAN / 4 COM)
Form Factor	Rackmount 1U computer			
CPU	Intel Atom® Elkhart Lake, dual-core x6211E or quad-core x6425E processor			
Video Output	1 HDMI, 1 VGA			
LAN Ports	4	12	4	6
Serial Ports	2	2	10	6
USB Ports	3 USB 3.0			
DI/Os	8 DIs, 8 DOs			
Power Input	12/24 VDC			
Certificates	CE, FCC, UL, BSMI			
Operating Temp.	-30 to 60°C			
Dimensions (mm)	440 x 230 x 43.6	440 x 230 x 43.6	440 x 230 x 43.6	440 x 230 x 43.6

Back to TOC

BXP/DRP/RKP Series

Intel® Atom®/Core™/Celeron® Powered Industrial Computers

- Rich set of interfaces with expansion options to meet your application needs
- Fanless design for long-term stability and easy maintenance
- Industrial reliability with -30 to 60°C operating temperature range
- 3-year product warranty
- Configure-to-order service (CTOS) for easy assembly and faster time to marke

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 (IIoT). With 35 years of industry experience, Moxa has connected more than 102 million devices worldwide and has a distribution and service network that reaches customers in more than 85 countries. Moxa delivers lasting business value by empowering industries with reliable networks and sincere service. Information about Moxa's solutions is available at **www.moxa.com**.

Back to TOC

Made to Last, Made for You - A New Generation of x86 Industrial Computers

Moxa introduces a new generation of BXP, DRP, and RKP Series industrial computers that are specifically designed to facilitate rapid system development with reliable, adaptable, and cost-effective computing solutions.

Revolutionizing Industrial Computers: Boosting Efficiency, Security, and Automation

Thank you for visiting the Revolutionizing Industrial Computers: Boosting Efficiency, Security, and Automation eBook!

If you have any questions or feedback about the contents in this eBook, please contact CFE Media at *customerservice@cfemedia.com*

We would love to hear from you!

MOXA®