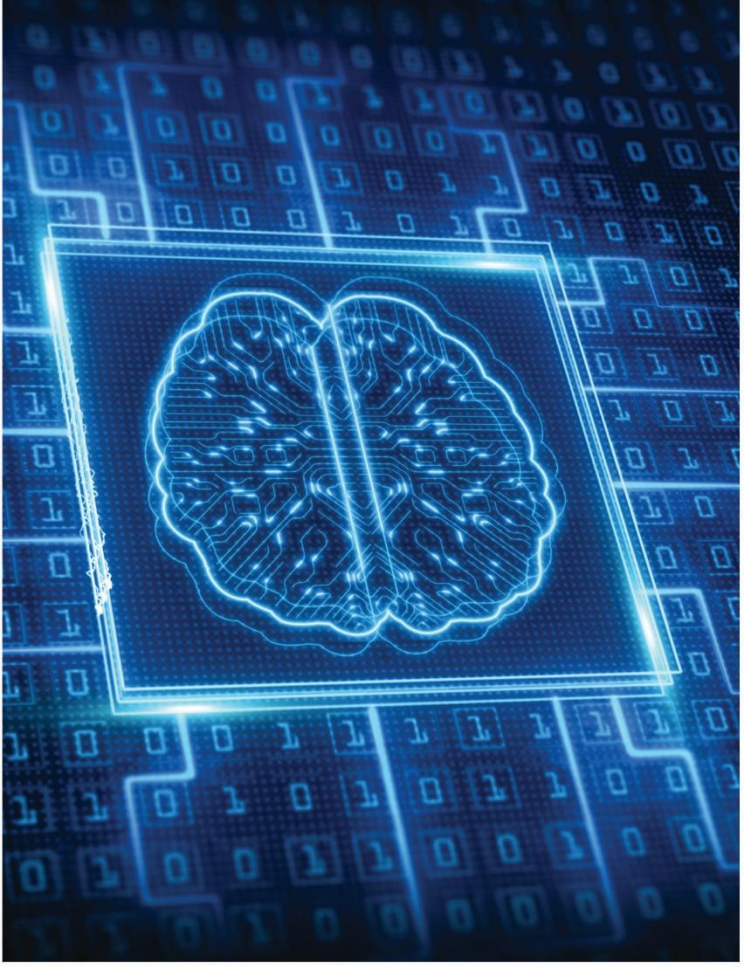


Three Ways to Embrace Industry 4.0

antaira®

making connectivity simple...

Three Ways to Embrace Industry 4.0

Global supply chains are buckling under the strain of unprecedented demand and constricted logistics capacity. Added to skyrocketing inflationary forces, it's no wonder that an increasing number of OEMs are embracing Industry 4.0 to bolster enterprise efficiency by making their manufacturing more aware, predictive, and autonomous.

The shift from Industry 3.0 to Industry 4.0 involves the convergence between information technology (IT) and operational technology (OT). Connecting OT systems to an IT network allows a more detailed view of individual equipment and creates a comprehensive view of the entire ecosystem, simplifying management and operation. Besides allowing machines to be largely operated autonomously without human supervision, Industry 4.0 creates higher value when data collected from intelligent sensors and actuators connected to equipment, leads to better decision making, as well as to the “learning” that’s now possible with artificial intelligence (AI) and machine learning (ML). These benefits are compelling and explain the explosion of interest in Industry 4.0.

For OEMs, Industry 4.0 unlocks actionable data throughout the plant and beyond, improving operational awareness in manufacturing and maintenance processes. For example, automated assembly systems that once operated in data silos can be connected with IT databases from purchasing, compliance, and customer service departments, or to data from Manufacturing Execution System (MES) and Enterprise Resource Planning (ERP), to identify trends, detect bottlenecks, and take advantage of emerging opportunities. As another example, analyzing big data collected from sensors on the factory floor provides real-time visibility of manufacturing assets to facilitate predictive maintenance in order to minimize costly downtime. In this instance, machine learning algorithms detect and target faulty parts before they wear out, rather than wait until repair work is more expensive.

Besides gaining insights from a local shop floor, warehouse, or assembly line, Industry 4.0 provides visibility into supply chains thousands of miles away where an OEM’s suppliers may be located. OEMs can be informed of where their assets are in the supply chain so they are in a better position to fulfill customer deliveries in a timely fashion. Historical supply chain data could be sent to the cloud for analysis, helping to create predictive models and develop condition-based alerts. If a delay is detected, software will alert the OEM so that it can pivot in strategy.

Antaira and Industry 4.0

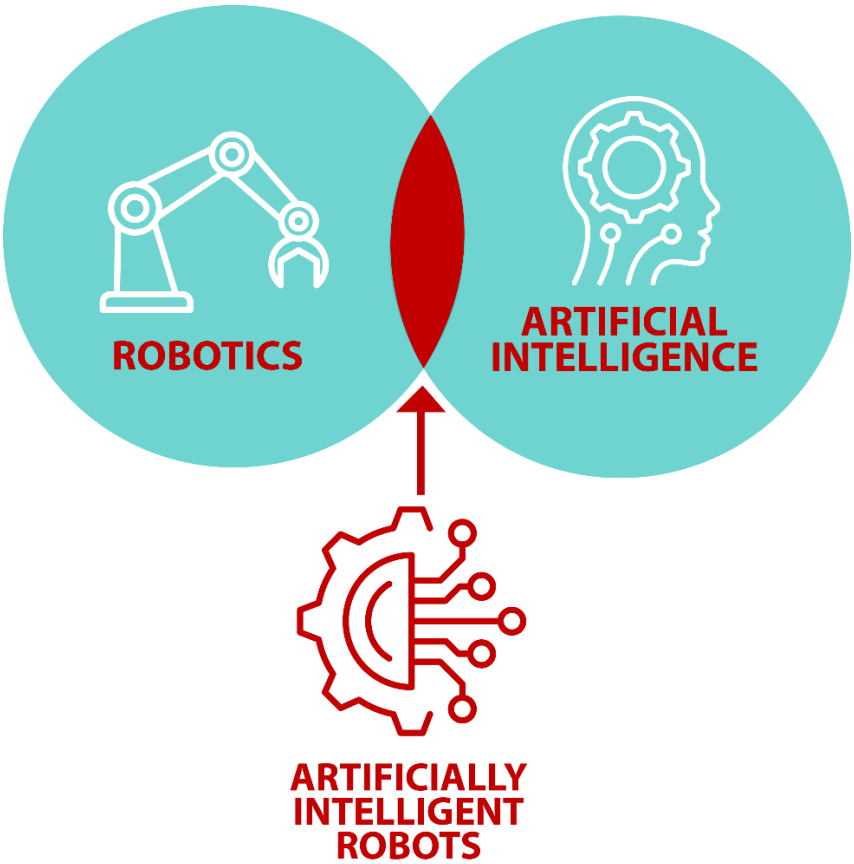
The Industry 4.0 megatrend is now being applied across a wide swath of industrial sectors where it is benefitting discrete and process manufacturing, petrochemical, mining, agriculture, and other diverse segments poised for unprecedented growth.
As an industrial networking equipment innovator, Antaira has a portfolio of tools to help you implement Industry 4.0, whether your organization is a specialty manufacturer or a multinational corporation. As an OEM, Antairia is uniquely positioned to quickly adapt to changing technology landscapes, and able to manufacture custom solutions to meet your needs.
Antaira has identified three ways to embrace this exciting paradigm shift using our industrial switches, industrial wireless devices, software and knowhow:

- Artificial Intelligence
- Network Connectivity
- Device Cybersecurity

Artificial Intelligence (AI)

AI is the simulation of human intelligence processes by computers to analyze data for correlations and patterns, and the use of these patterns to make accurate predictions about future states. AI is all around us. From agriculture applications that detect imperfections in fruits and vegetables during harvesting processes, to autonomous construction and farming machinery that use GPS technologies to navigate over predefined routes. Industry 4.0 uses AI to analyze sensor data to track equipment usage, improve workflows, streamline logistics, increase safety, and achieve higher overall efficiency across OT and IT operations.

One promising category for AI is providing intelligence for autonomous robotics. Autonomous robots are increasingly finding their way into warehousing, manufacturing, agricultural operations, and civil engineering. AI-driven “cobots” reduce labor costs and increase productivity simply by continuously working around the clock without fatigue or breaks. In addition, safety is improved in hazardous environments, and insurance and injury leave costs are reduced significantly. As AI continues to advance, problem solving and learning analytics will enable autonomous robots to be responsive to their environment with minimal human feedback. To give you an idea of what that means, think of the thousands of manned forklifts operating today in warehouses and port terminals. Forklifts are labor-intensive, expensive to maintain, and dangerous. As an alternative to a forklift, let’s say AI is applied to an automated guided vehicle (AGV). Freight is picked using a barcode reader. The AGV then automatically reroutes itself with the freight on-board to the best path through the warehouse using wireless routers and industrial switches. Sensors assure no collisions occur with obstacles or employees.



Antaira is partnering with leading companies in autonomous robotics by providing resources, technical support, and an advanced line of IEEE 802.11 a/b/g/n/ac industrial wireless devices and PoE+ 10G Ethernet managed and unmanaged switches that enable real-time processing of high-resolution, high throughput data. Antaira's industrial wireless access points, industrial routers and IoT gateways are resistant to electromagnetic disturbances, periods of voltage instability, extreme temperature fluctuations, as well as intense shocks and vibrations. Unlike many of our competitors, Antaira manufactures "industrial-grade" networking devices truly engineered for industrial environments.

Potential for autonomous robots using Antaira devices are virtually endless. In the agricultural market, for example, Antaira industrial Ethernet switches are now being deployed in robotic fruit picking devices that can delicately grasp a single strawberry without bruising. Antaira is also connecting and transmitting data in robots capable of automatically targeting and eliminating weeds using thermal energy while rolling through agricultural fields. Also, Antaira industrial managed Ethernet switches are incorporated in an upgrade kit that transforms trench excavation equipment from the likes of Caterpillar, Volvo, Hitachi, Deere and Komatsu into autonomous robots operated remotely on a laptop. For these customers and hundreds more, Antaira is delivering on the promise of autonomous robotics for a more productive, efficient and sustainable future.

Network Connectivity

With the exponential growth of Industry 4.0 technologies, operational networks are continually going through expansion processes, requiring the same type of bandwidth allocations and infrastructure support as the enterprise network counterparts. Furthermore, as Industry 4.0 is trending towards an increased focus on AI for big data analytics and cloud computing for process and control information collection, connectivity and connection points have become a critical piece in the industry 4.0 puzzle.

Ethernet — the technology of choice for operational networks, thanks to its standardization, versatility, and low cost. An all IP Ethernet infrastructure also helps to meet the imperatives of cybersecurity, determinism, and system reliability. Thanks to these advantages, legacy technologies such as analog fieldbus systems are migrating to Ethernet, allowing for communications with modern day technologies.

Ethernet thru TCP/IP–based communications now range from AI cloud-based processes to legacy bus systems, which can interconnect the smallest application using just one twisted wire pair. In a recent development, the IEEE published a standard for 10 Mbit/s (IEEE 802.3cg) important to Industry 4.0 that allows transmission distances up to 1000 meters (3280 feet), therefore holding the potential to replace virtually all fieldbuses currently in use.

One of the main components underpinning Ethernet connectivity is the Ethernet switch. Antaira managed and unmanaged Ethernet switches are staples of Industry 4.0 architectures, able to transmit data between connected devices and wider networks in a way that is secure from outside threats. While a basic Ethernet switch simply filters and forwards network packets from one networking device to another, Antaira industrial switches offer much more. As proof, consider Antaira's Ping Alive. It is a simple yet powerful feature that gives engineers and technicians control over failed communication of edge devices. Ping Alive "pings" the activity or inactivity of Powered Devices (PDs) and allows for an automatic reboot when a connected

device becomes unresponsive, saving the network engineer from visiting the site for troubleshooting.

Another example of an Antaira Ethernet switch innovation is the company's patented IEEE 802.3bt Safe PoE Disable. This hardware safety feature lets engineers easily turn on/off power to a single 802.3bt PoE port using a front panel DIP switch. Disabling the PoE port for a high powered device adds a further level of protection against possible failure when disconnecting the device while the PoE port is actively providing power.

Yet another breakthrough is Antaira's patented Persistent PoE for Managed 802.3bt switches. Antaira's Managed 90W per port industrial PoE Switches are designed with patented Persistent Power Over Ethernet (PoE) technology to support applications with PDs. It provides powered devices with uninterrupted PoE power, thus keeping the network stable while securely capturing critical moments in the event of a firmware upgrade or switch reboot.

Antaira's commitment to Industry 4.0 goes far beyond our industrial Ethernet switches. Our web-based network management suite (Antaira NMS) automatically adds Ethernet switches, both existing and newly installed, into the network topology through SNMP, eliminating the time-consuming task of manual interventions. Device issues can be remotely resolved by administrators miles away, allowing for networks to return to normal in a shorter amount of time. Administrators can also upload custom device icons and floor plans, and to decide on a preferred map layout. In addition, Antaira's Virtual Private Network or VPN system called Antaira ConnectVPN facilitates the interconnection of remote devices through the use of Antaira wireless router series for configuring, monitoring, and collecting of data.

Device Cybersecurity

The tools and software of Industry 4.0 are revolutionizing Industrial Industries. We are now seeing Smart Interconnected Gigafactory which can monitor and control every facet of "intelligent" production processes. But just as these new technologies have created the opportunities for optimization, they have also introduced new risks and security threats, creating a completely different threat vector than PC-based networks.

Industry 4.0, for all its benefits, makes "Industry" an appealing target for cyber-attacks. The expanded attack surface gives bad actors the opportunity to move laterally across a network, jumping across IT and OT systems for industrial espionage, intellectual property theft, IP leakage, or even production sabotage. For this reason, cybersecurity best practices must be acknowledged as one of the pillars to a successful Industry 4.0 strategy. Adopting this risk-based security mindset includes:

- Recognizing that every connected device represents a potential risk, therefore, maintaining a real-time inventory of all OT assets and monitoring the network to devices have not been added without authorization.
- Identifying and monitoring who can access devices. Implementing secure password policies that prioritize length over complexity will help prevent unauthorized network access.
- Taking a security-first approach to the deployment of any new connected devices. Require new devices go through verification before they can gain access to the network and proceed to communicate with other devices.

- Performing real-time vulnerability assessments and risk-based prioritizations to spot potential threats. Regularly monitoring the network will identify suspicious communications or content, malicious software, improper access, and any signs of access control manipulation.
- Fixing any outdated systems, unpatched vulnerabilities, and poorly secured files.
- Implementing multi-factor authentication whenever possible.
- Segmenting networks and restricting host-to-host communication pathways.
- Ensuring that device suppliers commit to regular security and software patches and audits.
- Involving, not just informing, the C-suite of the cybersecurity process.

Cybercriminals attack the low-hanging fruit, meaning they will go looking for easy targets and then work their way deeper inside the perimeter. In the case of Industry 4.0, the "low-hanging fruit" are your connected OT devices, including those with decades-long life cycles, an inability to patch systems due to stability concerns, and a lack of basic cybersecurity features such as user authentication or encryption. This threat environment has been further heightened by device vendors jumping into the industrial market from the IT space with little background into OT cybersecurity.

Before Industry 4.0, OT devices and systems were "air-gapped" to isolate them from risk. Antaira recognizes that is not possible today. This is why Antaira's industrial switches, industrial media converters, and wireless routers feature robust, DoD-compliant layer 2 and layer 3 security that helps manage network traffic at scale. And why our Antaira ARS-7235 NAT routers can be used to conceal the identity of an IP address block being used on a network, among the many other security features built into our industrial products. Antaira also gives administrators the tools they need to build on existing security policies and company standards, such as an Authentication, Authorization, and Accounting mechanism that can track user activities while limiting essential controls to employees who require them. Antaira Access Control Lists (ACLs) further filter accessibility by limiting network traffic to only trusted sources, while restricting management access to designated networks and allowing user access on selected machines.

To remain competitive, manufacturers of all sizes must immerse themselves in the Industry 4.0 revolution. Learn how Antaira can help you bring Industry 4.0 into your operations so you can leverage data that predicts needs, generates efficiencies, and informs smarter decisions. Visit www.antaira.com.tw or call +886-2-2218-9733 for more information.