Allied Telesis

Network Solutions Guide

MANUFACTURING

Data is crucial to your manufacturing network, so moving it securely, reliably and quickly is essential to your success. We have the solutions, the products and the experience to help.

The Era of the Industrial Internet of Things

Smart Technology Pillars

- Industrial IoT
- Horizontal and vertical integration
- Cybersecurity
- Autonomous robots
- The Cloud
- Big data and analytics
- Simulation
- Augmented reality
- Additive manufacturing

The Internet of Things (IoT) refers to the network of physical objects made "smart" with electronics, sensors, software, and network connectivity, allowing them to collect, process and exchange data. These objects can also use data processing insights to influence physical processes, by using actuating and control functions.

IoT is a global infrastructure for the information age, enabling advanced services by interconnecting both physical and virtual things, using existing and evolving interoperable information and communication technologies.

Industrial organizations soon realized the benefits of IoT and coined their own taxonomy, characterization of application, and use cases. Thus the Industrial Internet of Things (IIoT) was created—and is now the most valuable IoT market.

IIoT technology allows organizations to directly access plant, manufacturing, and remote industrial device data. As more organizations move to adopt IIoT, operational technology (OT) and information technology (IT) are converging. Technology convergence hinges on developing a unified strategy for traditionally separate groups such as facilities, security, safety and IT. This convergence enables the virtualization of production processes and their configuration via flexible IT services, rather than low level OT processes.

OT consists of machinery, physical plant equipment, and remote industrial software and hardware. OT professionals focus on systems used for monitoring and control. They are adept with Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Human-Machine Interfaces (HMIs), Supervisory Control and Data Acquisition (SCADA) systems, and embedded computing technologies.

IT includes any use of computers, storage, networking and other physical devices, and the infrastructure and processes that create, process, store, secure and exchange all forms of electronic data.

OT is progressively adopting IT-like technologies, so the convergence of IT and OT will bring clear advantages to companies, including cost and risk reductions, and enhanced performance and flexibility.

What is Smart Manufacturing?

Smart manufacturing is focused specifically on peer exchange and communication between businesses, people and physical things, as equal entities. The digitization of complex production processes and value chains is within companies, across companies and sometimes across industries. There is a vision for a high degree of digital technology and automation to empower manufacturing—with improved efficiency, intelligent production, reduced energy consumption, better production quality, advanced collaboration modes, new business models and much more.

In smart manufacturing, the synergy of systems enables self-regulating processes via machine learning, artificial intelligence and cognitive computing. Data leads to actionable insights, including early warning algorithms, predictive models, decision support, workflows and dashboards. Smart manufacturing transforms isolated automated cells into fully integrated facilities communicating with each other to reduce the mean time between failures (MTBF), increase the overall equipment effectiveness (OEE), and optimize supply chain management, productivity and quality at reduced costs.

Manufacturers and their suppliers recognize that standard communication and uniform networking of industrial systems is the key to optimized services, greater visibility, and lower total cost of ownership. As such they embrace standard information technology, particularly Ethernet and IP networking, for industrial automation and control environments. IP adoption enables integration with the company network and allows a cloud approach for critical applications.

Adopting Ethernet and IP networking technologies enables the flow and integration of information between the factory plant and business systems. An IT/OT converged physical network removes redundant network infrastructure controls such as conduit, cables, switches and UPS, to allow interoperability and security compliance.

Taxonomy

Smart manufacturing is a collective term for the technologies and concepts of integrated computer networking, and the physical processes that enable production process digitization.

Machine learning provides the ability learn from data and create foresights based on this data.

Artificial Intelligence is when machines exhibit human-like traits such as self learning and problem solving, leveraging on advanced information analysis and correlation.

Cognitive computing utilizes self learning or deep learning algorithms at scale, to operate in a manner similar to the way the human brain works when attempting to solve problems.

IT/OT convergence means IT systems support OT needs, consolidating data streams to enable digitization of OT processes and intelligent decision making across industries.

Why Allied Telesis?

In 2021, **20%** of top manufacturers will depend on a secure backbone of embedded intelligence, using IoT, blockchain, and cognitive analysis, to automate large-scale processes and accelerate execution times by up to **25%.**

Source: Gartner Research, 2019

Allied Telesis is an industry leader in networking solutions. With a proven history of delivering highly reliable and feature-rich advanced network solutions, more and more manufacturers are turning to Allied Telesis to achieve their objectives.

Allied Telesis has been implementing leading-edge manufacturing networks for many years and supply advanced cutting-edge network services to tomorrow's generation.

Allied Telesis provide network connectivity functions for both locally and globally distributed manufacturing sites. Our unified network fabric enables guaranteed high performance, quality, reliability and strict latency for data exchange, providing high application performance.

Allied Telesis Industrial Ethernet switches provide enduring performance in harsh environments and offer high throughput, traffic management and policy enforcement, such as security, remote access, Quality of Service and multicast management. With a fanless design, a wide operating temperature range, shock and vibration resistance, appropriate EMC, lighting and surge immunity, they tolerate demanding environments such as those found within a factory plant.

Our advanced high-value product portfolio provides the security, mobility and performance you need for your network, both now and well into the future. A set of management tools simplify and automate many daily activities, minimizing the human effort required.

Let's look at how Allied Telesis meets the challenges faced in manufacturing, and provides solutions that facilitate an advanced business approach.

IoT and Edge Computing

Internet of Things (IoT) enables the extraction of insights from data in real-time so decisions can be made rapidly. Data acquisition and analysis at the edge provides more business agility and lower costs.

Digital Video for Analytics and Security

A dedicated product portfolio securely and reliably transports any kind of video stream across the IP network. Security camera video streams give physical security, and production line video allows advanced process quality analytics.

Unstoppable Segmented Network Access

Provide complete access anytime ensuring that your network is up and running. Fix link or network equipment failures without the need for human intervention.

Industrial-Grade Infrastructure

Devices are designed to provide enduring performances and tolerate harsh industrial environments.

No Compromise Wi-Fi

Ensure reliable, high-performance Wi-Fi connections everywhere they are needed. High device density support, for manufacturing equipment and user access.

Total Autonomous Networking

Automate network management with a single smart tool to add intelligence, security, easy management, risk reduction and lower costs.

IOT AND EDGE COMPUTING

Manufacturing processes are under continuous review, aiming to optimize production time and cost, minimize material wastage and achieve excellent quality. Process optimization is crucial—it has a direct impact on the final product quality and consequently on revenue.

The level of process optimization is directly related to the ability to control each step of production. All devices, sensors and equipment must be monitored to collect important information for any process improvements.

With the advent of IoT technology, today's modern production plant is equipped with hundreds of sensors capable of providing information in real time. A vast amount of data moves across the network and reaches the servers that analyze it to find important correlations, improve processes and proactively predict equipment failure or malfunctioning.

This complex process, called elaboration, is simplified by the IoT data analytics platform provided as cloud services. All collected data is delivered to the cloud IoT platform where it is analyzed to provide useful information and predictions.

The Impact on Bandwidth

The cloud approach requires that all collected data is delivered over the WAN link to the cloud server. The dynamic power of cloud processing is easily able to manage the data, but the cost of this elaboration process, as well as the cost of the WAN link, can be high.

The Edge Approach

IoT sensors are usually basic devices that simply collect information and send it to the server. A temperature sensor, as an example, continuously measures the temperature, sending it to the server every few seconds. This results in a continuous stream of the same information repeated until such time as it changes.

The process is the same for the large majority of sensors. This generates a tremendous amount of background traffic which overloads the WAN interface and the elaboration process.

To minimize background traffic, edge devices are used to pre-elaborate the information and to communicate only the important changes, optimizing both WAN and cloud usage.

Edge devices are located near sensors, enabling real-time actuation and control processes. Locally storing sensitive information enhances privacy control, avoiding sharing sensitive data within multiple network devices.

DIGITAL VIDEO FOR ANALYTICS AND SECURITY

Video Inspection

Automated video inspection is a diffused technology within almost any manufacturing process, from small party assembly lines to very large plants.

Maximizing production quality and avoiding the use of defective parts involves many elements—quality checking production components, correct placement of devices and parts, compliance of finished goods, and completeness of final packaging.

Machine vision systems can decide in real time if a part should be accepted or rejected, and will raise an alarm if there is a problem. In addition, recently introduced machine-learning techniques perform a background analysis of the information coming from different assembly equipment and from different production lines, providing predictive failure prevention information.

The machine video inspection is based on a large number of visual inspection cameras that retrieve real time information and work with high quality images. Machine learning processes do not have the same real-time requirements, but need to manage the entire plant's video streams.

Different requirements are reflected in the network characteristics, which must be designed with the video stream in mind.

Video Security

Strong plant security requires dedicated video surveillance, connected to an appropriate access control system.

To reap the full benefit from the machine learning process, all video data coming from environmental and security cameras must be analyzed, adding a new video stream to the network.

> We have wireless network access covering the entire factory, so secure access is now possible anywhere, which is extremely helpful and convenient.

Mr. Hajime Nakajima

Manager, Manufacturing/Engineering Group
Yokote Plant & Management/Administration
Div. NHK Precision Co., Ltd.

Video Streaming Over Ethernet

The Ethernet network used in a production plant must provide a highly reliable implementation to minimize service interruption. Any problems in video transmission will affect the machine video system, preventing it from detecting any faulty parts or from passing quality assessments. Since it is not possible to put production on hold, the risk of failed units at the end of the production line grows.

Adopting industrial low voltage devices—which are centrally managed and developed for harsh environments—maximizes network quality and improves the reliability of the whole system.

UNSTOPPABLE SEGMENTED NETWORK ACCESS

Factory devices communicate with each other to synchronize the production process and provide the necessary reports and data for process optimization. Communication amongst factory equipment is migrating, from industrial-dedicated protocols using a dedicated network, to protocols running over a shared IP-based infrastructure.

IP adoption enables integration with the company network and allows a cloud approach for critical applications. This migration requires original infrastructure with very low jitter and latency, implemented over an IP network designed with real-time operations in mind.

The production line is the most critical part of any manufacturing business—any interruption has a direct impact on revenue. The high availability and accessibility of the IT infrastructure is vital to the entire production process.

The unstoppable Allied Telesis network access solution has been developed to ensure that any network can survive multiple faults, while still maintaining the connectivity in a wide range of network architectures—providing a high-availability solution.

Network Equipment Power Supply

Power supply continuity must be guaranteed with a battery backup and an automated generator. Networking equipment must be designed with redundancy in order to withstand the event of an internal PSU failure. Allied Telesis produces a wide range of equipment with redundant PSU systems so that when one of two units fails, the equipment can still remain fully operational—even during a blackout.

Segment Access Network

To minimize infection between devices, network segmentation with a firewall between each of the segments is mandatory in a factory environment. The Allied Telesis solution's Self-Defending Network approach avoids threat proliferation and production problems.

Virtual Stacking with VCStack™

Multiple Allied Telesis switches can be connected to form a single virtual switch. Allied Telesis VCStack with Link Aggregation provides a resilient solution that can survive link or equipment failure.

Ring Protection

When the distance between devices is large, a network ring topology is the optimal solution. Allied Telesis provides ring protection protocols to save your network from link failure whilst providing a truly resilient infrastructure.

VCSTACK

VCStack and link aggregation provide a solution where network resources are spread across the virtual chassis members, ensuring device and path resiliency.

VCStack can be spread over long distances, with fiber connectivity. A long distance VCStack is perfect for distributed network environments or data-mirroring solutions.

EPSRING

Allied Telesis Ethernet Protection Switched Ring (EPSRing™) solutions provide high performing, reliable, flexible, scalable distributed network cores.

The recovery time when links or nodes go down is extremely fast—as low as 50ms, making this solution ideal for manufacturing networks.

Redundant Core and Disaster Recovery

Should a further degree of resiliency be required, Allied Telesis also provides core switches with an optimally redundant configuration for a disaster recovery architecture. This is accomplished by a virtual stack, with network devices located in different rooms or even buildings.

INDUSTRIAL GRADE DEVICES

Networking equipment for manufacturing networks differs from equipment designed for enterprise use. Standard enterprise devices are designed to be installed in 19" racks, with standard AC power supply and deployed in controlled temperature environments. The conditions for factory devices are completely different. Devices developed to withstand harsh factory environmental conditions are called Industrial Ethernet devices, and they have specific characteristics:

Extended Temperature Range

Factory temperature is not always controlled—cabinets placed in outdoor areas or in large warehouses can reach temperatures ranging from -40° to 75°. Commercial equipment with a temperature range of between 0° and 50° cannot survive in this specific environment. Industrial devices are built to support this temperature range.

Ingress Protection (IP)

Industrial Ethernet devices are usually placed in cabinets, and located in production areas. These devices, together with the cabinet, need to be protected from ingress of water and object intrusion. This kind of protection is called Ingress Protection (IP). Industrial devices that need to be placed in a cabinet usually require code IP30.

DC Powered

In the factory cabinet the power supply is low voltage DC. Industrial Ethernet switches must support a DC power supply, as well as dual PSUs for redundancy.

Dust Protection

Industrial environments are not protected from dust, and network equipment fans collect dust, obstruct air flow and can cause equipment damage. Hence, Industrial Ethernet devices must be fanless to avoid dust damage.

DIN Rail

Standard cabinets in industrial environments provide a DIN rail capable of hosting devices with DIN rail attachments. Industrial Ethernet devices to be placed in cabinets must be designed to be mounted on a DIN Rail.

Time Synchronicity

Factory protocols require synchronization between equipment. Once an IP network is used, the Precision Time Protocol (PTP) synchronizes the endpoint. Industrial Ethernet devices must therefore support PTP transparent mode to enable synchronization.

Ingress Protection (IP)

The IP code is composed of the "IP" prefix and two digits.

The first digit in a range from 0 to 6 indicates the protection against solid objects of different sizes. 0 means no protection, while 6 means protection up to dust particle size 6mm.

The second digit in a range from 0 to 8 indicates protection against liquid. 0 means no protection, while 8 indicates protection up to 1 meter immersion for long periods.

IP30 indicates protection against objects with a diameter larger than 2.5 mm and no protection from water.

In an industrial installation, the system IP is provided by a combination of the device protection and the cabinet protection.

DIN Rail

A DIN rail is a metal rail of standard size dimensions widely used for mounting circuit breakers and industrial control equipment inside equipment racks.

INDUSTRIAL INFRASTRUCTURE FOR MANUFACTURING

IE340 Series

Ruggedized switches built to provide enduring performance in harsh environments, such as manufacturing, transportation and physical security.

IE340 Series switches:

- Offer high throughput, rich functionality and advanced security features.
- Are ruggedized to meet the latest industrial Ethernet standards.
- Provide highly stable and reliable network switching, with recovery in less than 50ms.
- Use Allied Telesis Autonomous Management Framework™ Plus (AMF Plus).

The reference model for computer-integrated manufacturing splits the network into different zones, to improve security and clearly define the equipment needs in terms of mechanics, ingress rating, climate, and electromagnetic compatibility. The zone dedicated to the factory production area is called "cell/area" and is the most demanding in terms of device characteristics.

The cell/area zone is the functional area within the manufacturing plant that includes systems and devices with a role in the production process.

Cell/area devices are industrial-grade, designed for harsh environments. They have some common characteristics:

- a wide operating range
- high electromagnetic and surge immunity
- mechanical robustness against shock and vibration
- dual power input for Mains and UPS
- appropriate ingress protection and, if required, protection against the destructive effects of temperature, humidity and gaseous pollutants
- DIN rail or rack mount

Allied Telesis Industrial Ethernet switches are designed to operate reliably and consistently under extreme conditions.

IE340 Series

Industrial Ethernet Gigabit Layer 3 Switches

IE220 Series

Industrial Ethernet Layer 3 PoE++ Switches

IE210L Series

Fanless Layer 2 Switches

IE510-28GSX Series

Extended Temperature Gigabit Fiber Stackable Switches

IE200 Series

Industrial Ethernet Layer 2 Managed Switches

IS130 Series

Industrial Ethernet Layer 2 Unmanaged Switches

NO COMPROMISE WI-FI

Within a factory, communication between autonomous guided vehicles requires a stable wireless network to ensure real-time information access.

The large amount of objects moving within a production site or warehouse causes a continuous change in the wireless signal reflection and coverage, impacting the connection stability.

To avoid these problems, an uninterrupted roaming wireless solution is ideal for manufacturing.

Wireless connections are also used for non-factory automated communication, and the no-compromise Wi-Fi approach avoids interference caused by non-production related traffic—adding reliability to the entire network solution.

Despite the wireless standard improving overall performance, there are still limitations that require technical skills in order to implement a stable wireless network.

In a wireless network, client disconnection and slow communication are typical problems, usually caused by more than one technical issue. The main reasons for wireless issues are interference between radio channels, an external wireless source not under IT control, and a lack of Access Point (AP) signal strength.

In a dynamic environment, there is a crucial need for a continuous network, requiring monitoring and skilled IT resources to maintain the installation to provide a valuable wireless service.

No Compromise Wi-Fi

The Allied Telesis No Compromise Wi-Fi solution ensures reliable, high-performance Wi-Fi connections everywhere they are needed by minimizing human intervention.

By analyzing signal coverage gaps and Wi-Fi AP interference, Autonomous Wave Control (AWC) automatically delivers a high-quality wireless experience. It reduces your dependency on skilled network engineers and results in lower operating costs.

In critical environments like factories and warehouses, AWC Channel Blanket (AWC-CB) enables control of hybrid APs that simultaneously provide single and multi-channel Wi-Fi connectivity.

AWC

Allied Telesis Autonomous Wave Control (AWC) is an advanced network technology that utilizes Artificial Intelligence (AI) to deliver significant improvements in wireless network connectivity and performance, while reducing deployment and operating costs.

AWC-CB

Allied Telesis AWC Channel Blanket (AWC-CB) is the Single Channel solution for Allied Telesis wireless APs.

All APs operate on the same channel with the intelligent controller managing the access mechanism.

Together with a traditional Multi Channel approach this provides a complete wireless access solution for any environment.

TOTAL AUTONOMOUS NETWORKING

Increasing network complexity significantly raises demands on network management and specialized resources. Implementing an automation solution makes life more simple, and more affordable.

Vista Manager EX is a plugin-based single-pane-of-glass approach to network management. A dashboard shows network details, status and events on a topology map, and highlights critical issues, alllowing for timely problem resolution.

With a series of plugins to control wired networks, wireless devices, and WAN links, our modular automation tools make networking easy.

Allied Telesis Autonomous Management Framework™ Plus (AMF Plus)

Reduce network operating costs with added intelligence and automation. Centralized management, automated services including firmware upgrades, backup and recovery, and zero-touch provisioning are just some of the AMF Plus benefits that minimize the effort and cost required to manage a complex manufacturing network.

Autonomous Wave Control (AWC) - Plugin

Analyze and optimize the performance of complex wireless networks with AWC. Install and forget your wireless network with an autonomous tool that analyzes traffic patterns and automatically configures APs to meet demand.

Self-Defending Network

Unauthorized access to factory data, ransomware and other types of attacks affects production and puts company assets at serious risk.

The Allied Telesis Self-Defending Network solution provides an integrated approach to network security, automating manual IT

VISTA MANAGER™

Vista Manager EX delivers state-of-the-art monitoring automatically by creating a complete topology map of switches, firewalls and wireless APs.

VLAN mapping and creation between devices, traffic monitoring and WAN mapping enables effortless management of many, if not all, network devices at once.

For more information please visit **alliedtelesis.com**

operations and protection from threats coming from both wired and wireless access devices. Without the need for endpoint agents or software, the Self-Defending Network can automatically respond to threats once they are identified.

Enabling a Self-Defending Network that helps organizations avoid lost time and unnecessary disruption to network services, the AMF-Sec Controller is key to our innovative and award-winning AMF security solution.

Software-Defined WAN (SD-WAN)

Centrally manage and automatically optimize inter-branch traffic.

Multiple connections with different performances and costs require continuous attention. The SD-WAN orchestrator centrally manages branch office connections for reliable and secure application delivery. Set acceptable performance metrics, automatically optimize and load-balance application delivery, and easily monitor WAN performance.

ABOUT ALLIED TELESIS

For nearly 30 years, Allied Telesis has been delivering reliable, intelligent connectivity for everything from enterprise organizations to complex, critical infrastructure projects around the globe.

In a world moving toward Smart Cities and the Internet of Things, networks must evolve rapidly to meet new challenges. Allied Telesis smart technologies, such as Allied Telesis Autonomous Management Framework™ Plus (AMF Plus) and Enterprise SDN, ensure that network evolution can keep pace, and deliver efficient and secure solutions for people, organizations, and "things"—both now and into the future.

Allied Telesis is recognized for innovating the way in which services and applications are delivered and managed, resulting in increased value and lower operating costs.

Visit us online at **alliedtelesis.com.**

AMF-Sec

The Allied Telesis AMF-Sec Controller enables our state-of-the-art network management and security solution. It provides exactly what enterprises need—reduced management costs, increased security and an improved end-user experience

AMF PLUS

AMF Plus is a scalable network management platform.

It supports Allied Telesis switching, firewall, and wireless products, as well as a wide range of third-party devices—including video surveillance cameras and IP phones—for truly inclusive network automation.

© 2024 Allied Telesis, Inc. All rights reserved.

Manufacturing sg RevC