ZIVARO

BRILLIANT IT

Innovations in Industrial IoT Networking

Joe Blazon
Director Solutions Operations

INTRODUCTION

For several years now, modern enterprises have been digitizing their businesses and developing their Internet of Things (IoT) initiatives. Finally, it is the time when the promises of IoT become a reality and solve many of the problems that organizations have faced. In a rapidly-changing technology maelstrom of cloud computing, evolving protocols, wireless connectivity, and bandwidth demands, IoT networks have struggled to keep up. The administrative burden of deploying, configuring, and maintaining far-flung industrial networks has posed considerable challenges. The fear of IoT security vulnerabilities and compromises have caused many organizations to delay, postpone, cancel their projects or isolate them so heavily they are ineffective. And once the IoT network is established, the data processing, analysis, and analytics challenges have made it difficult for organizations to realize the benefits of these costly industrial networks.

Innovations in industrial networking capabilities have solved many of these problems, alleviated the administrative burden, reduced deployment and operational costs, future-proofed the technology, and made it easier than ever to securely capture the valuable data and allow it to be effectively processed reducing the time-to-benefit for the enterprise.

HISTORIC CHALLENGES

Organizations have encountered many challenges of building and maintaining Industrial and IoT (IIoT) networks. The rapidly-changing protocols, devices, and cloud affinity have made this a difficult IT realm to "stay up-to-speed on". Shifting personnel work responsibilities has caused skills gaps requiring engineers to learn how to deploy and operate these IoT environments via "on-the-job" training.

Organizations have experienced a high administrative burden building out IoT environments and maintaining these large-scale networks with numerous sites and devices. Enterprises experience difficulty managing devices spread across a geographically dispersed set of facilities. It isn't easy trying to manage wireless IoT devices in far-flung locations that aren't easily reached physically. Challenges of managing large numbers of devices manually makes zero-touch provisioning, deployment workflow, and streamlined operations a must. However, today, much of the configuration work is performed manually.

Evolving needs of organizations makes it difficult to architect and design for the future. The

expandability of industrial devices may not exist as many IoT networking hardware lacks expandability. When an IoT deployment starts, 4G WAN services may initially be sufficient, but as applications change, more data may be streamed as the volume, veracity, and volatility of data grows. Soon 5G services (and other types of industrial interfaces) will be required and if the hardware wasn't adaptable, this could necessitate a complete hardware refresh and require site visits to upgrade every location.

Security of remotely-located devices is a primary concern for enterprises. The physical security of lights-out facilities is often weak and access to networking equipment in industrial facilities is unsecure. There is a constant concern about default configurations, default passwords, that can lead to a system-wide compromise. This common problem occurs when there are shared access credentials that many administrators use the same login username/password. When there is turn-over, organizations seldom go back to each and every device to remove access, or change the passwords.

The physical world of the industrial data network is a messy place. Locations where manufacturing, energy extraction, processing and generation, or transportation occurs are subject to many external threats. Extreme temperatures, dirt, dust particles, water, salt-water, oil, power fluctuations, vibration, shock, and even fire can threaten the fragile digital computing devices out in the field. These are not the places for a delicate piece of networking equipment or a finely tuned server.

Retrieving data from the industrial edge networks can be difficult. That data is on the very tip of the edge of the enterprise network. Organizations need digital networking at the edge and get it securely back to the data center or the cloud. Not only gathering IoT data can be challenging, but analyzing the data collected can be a huge task. Business analytics cannot occur until the data is received from the physical world and the data must be filtered and pre-processed before it can be used by a big-data application. A wide variety of datapoints across manufacturing, energy consumption, transportation, and other applications needs to be retrieved, synchronized among various compute systems. The data modeling and data management of IoT data are also on the critical path to making any of these digital business initiatives a reality.

One cannot overlook the security concerns of industrial networks and IoT devices. In recent years, compromised IoT devices have sourced DDoS attacks, malware infections have disrupted major services, human errors have led to data integrity issues, and these security flaws have impacted system continuity and compromised public safety. The security of the data coming streaming off the IoT devices themselves must have secured transit, and the IoT devices must be defended against these malicious attackers.

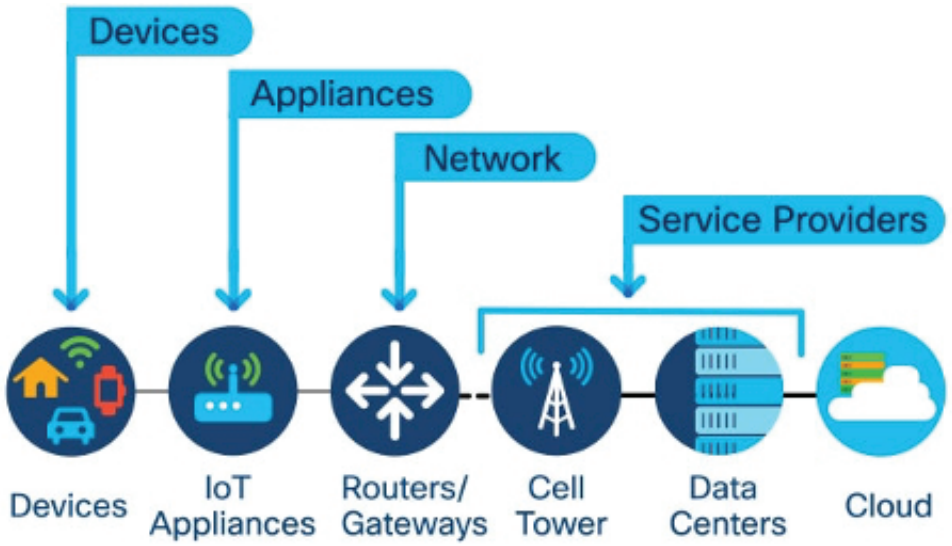
BACKGROUND

The IoT transformation has brought together the Information Technology (IT) world of networks, computers, cyber security and the Operational Technology (OT) world of Industrial Control Systems (ICS) and heavy machinery. IT teams are familiar with routers, switches, firewalls, servers, storage, hypervisors, running on AC power, 19-inch racks, and cloud computing infrastructure.

OT teams have decades of experience with Supervisory control and data acquisition (SCADA), Advanced Metering Infrastructure (AMI), Distribution Automation (DA), Industrial Automation (IA), Programable Logic Controllers (PLCs), Remote Terminal Units (RTUs), relays, contacts, sensors, serial interfaces, Din-Rail and DC power. These worlds are coming together in Industrial IoT (IIoT). This integration sometimes creates friction between diverse backgrounds, but can also result in functional, innovative, and transformative solutions that improves our world.

Legacy industrial networks were serial based, hard-wired bulky closed systems with gateways and isolated data stores. In the brave new IIoT world the potential of the data is being unlocked and shared on premises and with cloud infrastructures. Wired WAN connectivity is not always feasible in in many industrial locations. In recent years, the importance of 4G LTE wireless service provider connectivity was well understood, but bandwidth needs continue to grow. Now 5G broadband wireless services are becoming feasible, and even required for some applications. There are unique characteristics of 5G services that support IoT applications. Mobile Network Operators (MNOs) offering 5G networks have enhanced traffic management that allow them to support the numerous IoT devices and give them prioritized traffic transmission. Two of the primary use cases of 5G networks are: Ultra Reliable Low Latency Communication (uRLLC), and Massive Machine Type Communication (IoT) (mMTC). uRLLC services are applicable to manufacturing networks, autonomous vehicles, and first-responders needing FirstNet connectivity. mMTC services are useful for IoT applications that need to conserve battery life and conserve energy but don't have high bandwidth needs.

IoT devices can often be located in a "walled garden". Their remote location and lack of abundant power (constrained battery power) limits their ability to send data to the data center or out to the cloud. IoT sensor and control networks often use a Field Area Network (FAN) with wireless communications, sometimes in a mesh topology, and use low-rate wireless protocols like IEEE 802.15.4, 6LoWPAN, LoRaWAN, Thread, and Zigbee. These non-Internet Protocol communications must use some type of translation or gateway function to be able to share their OT data with the traditional IT networks running IP. The development of "edge computing" allows a gateway computer to gather the data from the IoT sensors and controllers, aggregate the data, pre-process it, perform local processing and analysis, then share it broadly with other computing systems. IoT systems often have an affinity to cloud applications and the edge compute node is the bridge between these two worlds.



Graphic Source: https://www.cisco.com/c/en_sg/solutions/computing/what-is-edge-computing.htm

ZIVARO

BRILLIANT IT

SOLUTIONS & ANSWERS WITH CISCO IOT

The IoT world has evolved over the past decade, so too has the solutions available from the leading manufacturers. Cisco continues to innovate and expand their network devices making them purpose built for industrial networking and IoT connectivity. Cisco has developed new routers and switches with capabilities that uniquely support IoT applications. The security, expandability, configurability, and ease of data gathering and analytics capabilities in Cisco IoT offerings have blossomed. These new industrial network devices are flexible, secure, and simple to work with.

Cisco's industrial routers, like the Integrated Services Router Rugged IR 1101 have a modular design that allows for expandability. They are also very compact, energy efficient, and can run on a variety of power sources. These routers have gigabit capabilities, which have not been available in previous generations of IoT edge routers. The routers have 1Gbps Ethernet interfaces and Small Form-factor Pluggable (SFP) interfaces for a variety of optical connectivity cabling options. These routers can connect to many different types of serial interfaces, GPIO pins, SCADA connections, and are well-suited to a variety of IoT device interfaces. The routers can have local data storage and are edge computing enabled. The flexibility of these routers lengthens their useful lifespan helping organizations maximize their investment by allowing the device to adapt to changing requirements.

Cisco industrial routers are "ruggedized" to endure physical threats in an inhospitable industrial environment. These routers can endure hostile environments and withstand vibrations, shocks, dust, dirt, humidity, and can operate down to -40oC (-40oF) and up to 75oC (167oF). These routers also help protect itself from electrical power service issues, like Electrostatic Discharge (ESD), with Volt-Var optimization and EMC protection. IR 1101s can run in secondary power substation harsh environments with their IEEE 1613 and IEC 61850-3 hardware specs for DA applications. These routers are small, are field replaceable and repairable and have low average power consumption (~10 watts). Cisco's Catalyst IE3x00 switches are also ruggedized and support wired network connectivity, with Power over Ethernet (PoE and PoE+) in hostile operating environments. The modularity and physical strength of these switches and routers provides investment protection.

Cisco's industrial routers have different modular Long Term Evolution (LTE) interfaces, including Citizens Broadband Radio Service (CBRS), and support a wide variety of mobile carrier connectivity. Cisco IR 1101 routers use LTE-MNA pluggable interface modules for emergency, public safety, and first responders who need specific 4.9GHz and FirstNet connectivity. These routers can be easily upgradable to 5G WAN services, when the services are available at the router's location, for higher bandwidth applications. The 5G interfaces can be connected to a MISP (public and private networks, Multi-PDN (Multi Packet Data Network)), using different SIM cards providing dual-active LTE interface redundancy and security of the sensitive data being forwarded.

For many enterprises, administrative burden and reducing technical dept are overriding requirements for industrial networks. Cisco's IoT routers are simple to deploy and configure and are easy to operate. They run the same Cisco IOS software that network engineers are familiar with and have decades of experience operating. Cisco's industrial routers can be integrated into an Software-Defined Wide Area Network (SD-WAN) environment and support Zero-Touch Provisioning (ZTP) which makes them easy to deploy by field teams without the use of a laptop, a console cable, and typing in configuration commands in the field. Cisco IOS-XE allows for network programmability with RESTCONF, NETCONF, YANG data models, and Python scripting which allows for automation of numerous routers with ease. Cisco's IoT Field Network Director (FND) is the management solution for effectively operating IoT Field Area Networks (FANs) allowing for zero-touch provisioning of IoT gateways and millions of IoT nodes.

The range of Cisco industrial network equipment support Internet Protocol version 6 (IPv6). IPv6 helps future-proof the network, removing the need for IPv4 NAT rules, improved global connectivity to clouds, partners, vendors, suppliers, customers, and everyone. IPv6 offers a plentiful supply of globally unique IP addresses and has optimizations like multicast communications and optimized Neighbor Discovery Protocol (NDP) for IoT devices with constrained battery power. IPv6 support on these routers allows for Proxy Mobile IP (PMIPv6) and Network Mobility (NEMO) protocol requirements needed in transportation applications. One example of how IPv6 can help unlock the potential of an IoT network is found in the BC Hydro Canada smart meter deployment using Cisco industrial routers. BC Hydro deployed millions of ITRON smart meters running IPv6 in an IEEE 802.15.4/RPL mesh network that allows for Automated Metering Infrastructure (AMI), Distribution Automation (DA) and smart-gird applications.

Cisco's IoT routers can provide security for these vulnerable industrial applications. Having an IOS-based Cisco router at the IoT edge can encrypt the data traffic in transit and provide advanced filtering of threats targeting the IoT devices. The IR 1101 routers have hardware-accelerated encryption processors to facilitate secure connectivity and use Cisco Trust Anchor Technology ensuring device authenticity. IR 1101s can be configured with network segmentation using Multi-VRF, VLANs, and VPNs to protect sensitive application data. Combining these router's capabilities with Cisco Cyber Vision to give deeper insight into the Industrial Control Systems (ICSs) are a powerful defensive combination. Cisco Cyber Vision can integrate with Cisco Identity Service Engine (ISE) and TrustSec to create dynamic security groups for IoT asset inventories to allow for enforcement of security zones and encrypted connections. Cisco Cyber Vison helps develop granular "least-privilege" security policies integrated with Cisco Talos Threat Intelligence to protect the Industrial IoT (IIOT) networks.

Cisco Edge Intelligence helps securely capture the valuable data from the IoT edge. Retrieve the correct data elements from the IoT devices and get it securely back to where that data will be processed. Cisco Edge Intelligence can gather the data, extract the data, filter the data points, transform the information, to facilitate the distributed data analysis. The Cisco Edge Intelligence Control Plane runs as a SaaS application that provides a dashboard to extract, transform, govern, and deliver IoT data to on-premises and cloud data analysis environments. This reduces the time-to-value of this valuable IoT information available at the edge compute gateway and make it actionable.

Frequently, enterprises need to reach out to a trusted partner with industrial networking experience to help them with the planning, design, architecture, and end-to-end integration of these applications. Having an integrator with these unique capabilities can save CAPEX investment by creating a future-proof solution while saving OPEX investment by creating an industrial network that is easy to deploy and operate over the long term.

Zivaro's decades of Cisco networking experience combined with capabilities with cloud application deployment leverage the combined affinity with IoT solutions. Zivaro's customers in the geologic resources (oil, gas, mining), manufacturing, governments, electric utilities, regional and municipal water utilities have tapped into Zivaro's ability to integrate the IT and OT disciplines. These customers each have their own unique IoT environments, but they all require reliable, consistent, secure infrastructure with advanced data analysis across a wide geographic footprint.

Zivaro leverages their SD-WAN and Network Programmability experience as key capabilities when deploying thousands of network devices. These capabilities can be combined to create a zero-touch provisioning for network devices being deployed in remote locations (often lights-out industrial facilities) that reduces operational costs. Zivaro's security practice can help proactively secure the IoT devices and protect the confidentiality and the integrity of the data gathering and analysis.

Zivaro's cloud services can also help clients create secure landing zones for the processing and analysis of the IoT data. Zivaro can help enterprises start off on the right foot when deploying scalable cloud networking, computing, storage, and application environments using industry best practices and cloud service providers well-architected frameworks. Zivaro's cloud team will reduce the mean-time-to-value by rapidly creating the secure cloud environments needed for these IIoT applications.

CONCLUSION

Choosing the right technology partners before embarking on an IoT deployment is the critical first step. Building in flexibility, upgradability, and future-proof the design with modularity will reduce the large initial investment. Industrial environments are harsh and organizations can protect their investment by choosing devices that are durable and suited for severe conditions.

Organizations will end up maintaining for the next decade so that administrative cost must be reduced using network programmability and network automation. Organizations can reduce their management costs by selecting solutions that are quick to deploy and easy to operate.

It pays dividends to first consider security in the architecture and design phase making sure the industrial network provides the reliable availability, preserving the confidentiality and integrity of the data, and protecting the IoT devices and infrastructure from attack. The goal is to address security in the design and leverage the best practices that give visibility and control to the IoT assets and their communications patterns.

The data is the most valuable result of an industrial network and having the ability to collect the information, process it, analyze it, and gain valuable insights and turn it into actionable business intelligence is the true value of the entire system.

Cisco and Zivaro can eliminate the challenges of industrial network deployment and operations letting enterprises focus on their business and realizing the benefits of their IoT technology investment.

REFERENCES

Cisco IR1101 Integrated Services Router Rugged
https://cisco.com/go/ir1101
https://www.cisco.com/c/en/us/products/routers/1100-series-industrial-integrated-services-routers/index.html
https://www.cisco.com/c/en/us/products/collateral/routers/1101-industrial-integrated-services-router/datasheet-c78-741709.html

Cisco IR1101 named 'Best of Show' in the Industry Network Category at Interop Tokyo 2020!
https://blogs.cisco.com/internet-of-things/the-route-stuff-interop20-tokyo-names-cisco-ir1101-best-of-show

Cisco Catalyst IE3x00 Rugged Switches
https://www.cisco.com/c/en/us/products/switches/industrial-ethernet-switches/catalyst-IE3000-rugged-switches.html

Cisco IoT Blogs
https://blogs.cisco.com/internet-of-things

Cisco IoT Networking
https://www.cisco.com/c/en/us/solutions/internet-of-things/iot-network-connectivity.html

Cisco IoT Routers and Gateways
https://www.cisco.com/c/en/us/solutions/internet-of-things/iot-routers-and-gateways.html

Cisco IoT Security
https://www.cisco.com/c/en/us/solutions/internet-of-things/iot-security.html

Cisco IoT Field Network Director (FND)
https://www.cisco.com/c/en/us/products/cloud-systems-management/iot-field-network-director/index.html

Cisco Edge Computing Solutions
https://www.cisco.com/c/en/us/solutions/service-provider/edge-computing.html
https://www.cisco.com/c/en_sg/solutions/computing/what-is-edge-computing.html

Cisco Cyber Vision
https://www.cisco.com/c/en/us/products/security/cyber-vision/index.html

Cisco Edge Intelligence
https://www.cisco.com/go/edgeintelligence
https://www.cisco.com/c/en/us/solutions/internet-of-things/edge-intelligence.html
https://www.cisco.com/c/en/us/solutions/collateral/internet-of-things/at-a-glance-c45-743263.html

BC Hydro IPv6 Smart Meter Project
http://blogs.cisco.com/energy/bc-hydro-cisco-and-itron-a-powerhouse-in-canada
http://www.cisco.com/c/en/us/solutions/industries/energy/utilities/smart-grid/gridblocks-architecture/bc-hydro.html