White paper
Cisco public

Network Infrastructure for a Wireless and Secure Factory

© 2019 Cisco and/or its affiliates. Copyright © 2019 Tech Mahindra. All rights reserved.

Opportunity and size

There are 14.5 million industrial establishments worldwide. They include 10.7 million factories, 3.3 million warehouses, 500,000 oil and gas fields, 50,000 transport organizations and ports, 10,000 military bases, 54,000 mines, and 263,000 hospitals and labs (source: Harbor Research, IDC). Together they hold more than a billion assets worth $4.5 trillion. Industry 4.0 is creating an opportunity to optimize these assets.

However, only 3 percent of the factory data is used for Industry 4.0 use cases. One of the top reasons for this underuse of data is a lack of an adequate and reliable industrial network infrastructure. This white paper examines the characteristics required in such an infrastructure.

© 2019 Cisco and/or its affiliates. Copyright © 2019 Tech Mahindra. All rights reserved.

Introduction

The factory of the future, Industrial Internet of Things (IIoT), robotics, remote monitoring and diagnostics, edge analytics, and traceability solutions have already started to transform the manufacturing supply chain. The next key step in the journey toward Industry 4.0 and smart manufacturing is to industrialize these solutions.

The key component in achieving the factory of the future is the network infrastructure, which acts as the backbone and is the single biggest factor for empowering the manufacturing process.

We believe that the millions of industrial establishments becoming network enabled will move toward wireless networking technology (Wi-Fi, 4G LTE, 5G), together with deploying better wired networks across different layers in the manufacturing IT/OT space.

Factory equipment holds a great deal of meaningful data. This data is key to any successful Industry 4.0 project. It must be collected from multiple sources and delivered to the right application at the right time—otherwise, little optimization can happen.

© 2019 Cisco and/or its affiliates.
Copyright © 2019 Tech Mahindra. All rights reserved.

The network in the factory of the future: Moving toward wireless connectivity (Wi-Fi, LTE, and 5G)

The rapid growth and ubiquitous use of cellular technology during the past 20 years has fundamentally changed the way we live, work, and connect with each other—locally, regionally, and globally. Technology that began with device connectivity and mobility for voice services quickly evolved to a broad range of data services, use cases, and associated business models. The 5G ecosystem promises a connected mobile society that will drive a socioeconomic transformation by extending the internet to machines and devices on a massive scale, with varied access connections.

Industry stakeholders and standards organizations have identified several potential use cases for industrial 5G, with very diverse requirements. Most of these fit within three primary categories:

- **Enhanced Mobile Broadband (eMBB):** eMBB provides more bandwidth and higher speeds for densely populated urban areas and event locations, such as stadiums.
- **Ultra-Reliable Low-Latency Communication (uRLLC):** uRLLC enables real-time interactions for mission-critical communications, such as autonomous driving, robotic control for industrial automation, drones, and remote surgery and medical care systems.
- **Massive Internet of Things (mIoT):** mIoT serves billions of low-cost, long-range, ultra-energy-efficient devices, machines, and things that need connectivity from remote locations as well as cloud applications with periodic, infrequent communication.

In addition to cellular advances, Wi-Fi networking is getting major upgrades. And while these technologies will each feature individual improvements, they will also work in tandem to fill in gaps in environments where the other technology may not be ideal.

The Wi-Fi Alliance is referring to the IEEE 802.11ax specification as Wi-Fi 6, because it's the sixth generation of Wi-Fi. (The existing standard, 802.11ac, will be known as Wi-Fi 5.)

One of the oft-cited benefits of Wi-Fi 6 is the speed boost over previous iterations. In addition to delivering greater speed, Wi-Fi 6 splits network capacity among a group of devices. That will be immensely important as the number of devices proliferates.

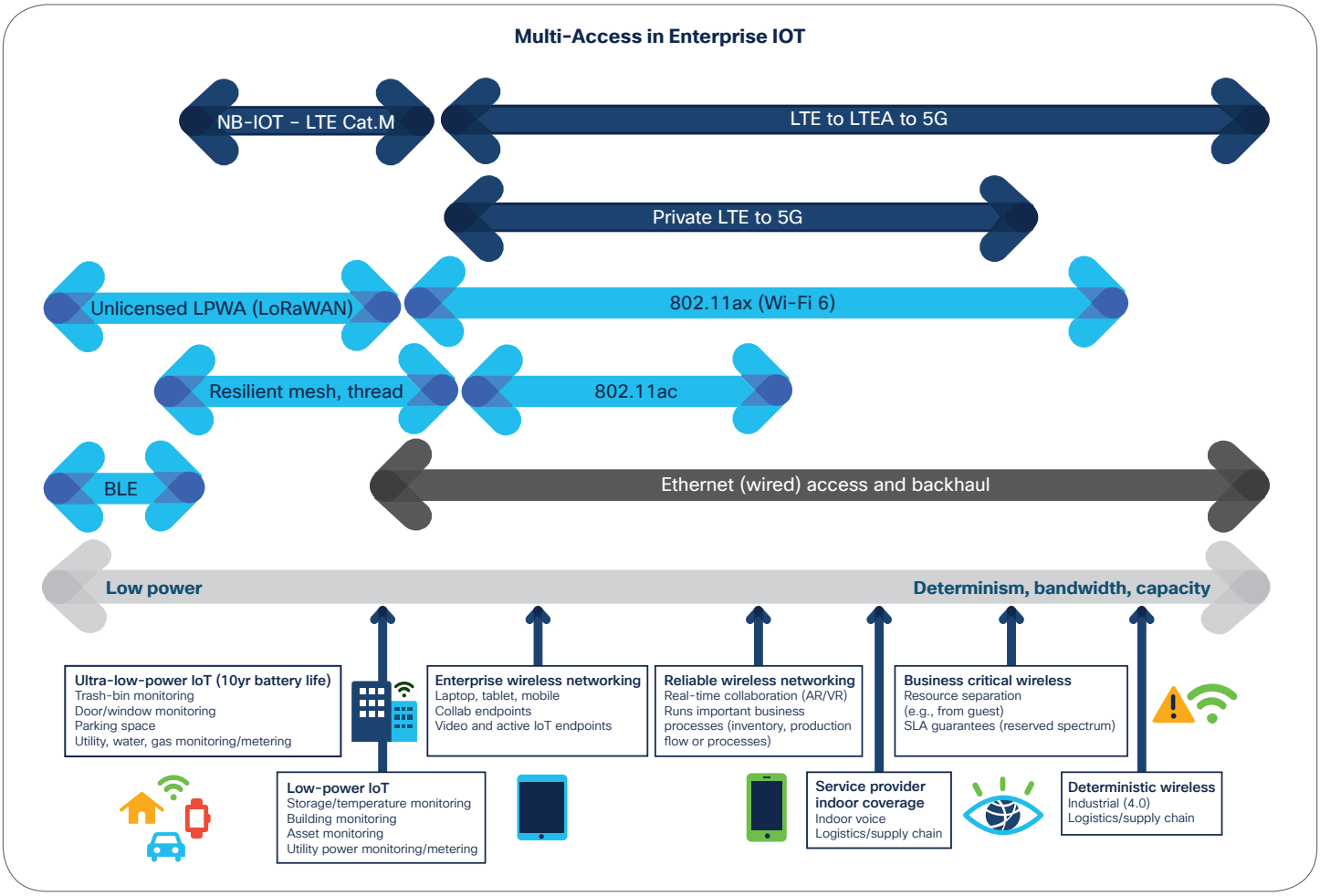
But Wi-Fi 6 and 5G speeds will depend on a variety of factors, so real-world application won't necessarily match these theoretical maximums. Factors include the number of devices connecting to a single 5G cell and the distance and obstructions between a 5G-connected device and the 5G tower.

However, we believe that 5G and Wi-Fi 6 will coexist and serve different needs. The interoperability between these two technologies will provide the maximum benefit to enterprises from a cost to performance perspective.

It's also important to note that 5G will not replace 4G immediately. Carriers will use a combination of WAN and other networks to deliver 5G services, coexisting with other legacy architectures into the next decade. In fact, carriers are deploying 5G radio (new frequency bands) with their 4G packet core (in non-standalone mode).

Figure 1 shows how the Industry 4.0 use case requirements of sub-millisecond latency, accurate location, high reliability, and very high bandwidth can be leveraged across multiple technologies.

Figure 1 Multi-Access in Enterprise IOT



Source: Demystifying 5G in Industrial IoT. Cisco white paper.

Mapping use cases to networking technologies

We believe that wired and wireless networks will coexist and that different use cases will be enabled on either or both technologies. Figure 2 shows a few Industry 4.0 use cases that we have mapped, with the critical networking features required for each one. We see many use cases moving toward wireless and further on to mobile technology. Examples include materials handling and automated guided vehicle (AGV) solutions, augmented reality and virtual reality (AR/VR) solutions, and smart products and tools.

© 2019 Cisco and/or its affiliates. Copyright © 2019 Tech Mahindra. All rights reserved.

Figure 2 Network requirements for selected Industry 4.0 use cases

Use cases–network features mapping ... moving to wireless

Use case	Description	Low latency	High bandwidth	Reliability	Advanced analytics	Edge and fog computing	Wireless (Wi-Fi)	4G LTE/ 5G
Machine connectivity, remote monitoring and diagnostics (RM&D), and statistical process control (SPC)	Integrate communications modules with machine programmable logic controller (PLC), enabling process parameter data extraction. Develop a remote monitoring system application for real-time alerts for parameters exceeding threshold limits. Use SPC-based predictive analytics for failure prediction. Provide dashboards and reporting in mobile clients.		•	•	•	•	•	
Digital overall equipment effectiveness (OEE), mean time to resolve (MTTR), mean time between failures (MTBF)	Measure and improve actual productivity of plant, production line, and equipment by integrating production, quality, maintenance, and control systems.		•	•		•	•	
Predictive maintenance	Measure and improve actual productivity of plant, production line, and equipment by integrating production, quality, maintenance, and control systems.		•	•	•	•		
RFID-based track and trace	Track material movement and storage with auto-ID technologies (RFID and barcode) from material entry into production to dispatch and track across the value chain, reducing errors.	•		•		•	•	•
Smart assembly tools	Connect power tools and make them smarter. Making them smart involves efficiently tracking and tracing these tools to ensure their proper use and prevent their misuse. Collect data on tool usage and status through remote connectivity.	•		•	•		•	•
Connected sensors for utility management	Manage energy use by integrating sensor data and exception management for specific consumption deviations, leading to savings in water/air/gas/electricity/ steam (WAGES), avoiding pollution, and responding faster through alarm management.	•		•		•	•	•

© 2019 Cisco and/or its affiliates. Copyright © 2019 Tech Mahindra. All rights reserved.

Use cases–network features mapping ... moving to wireless

Use case	Description	Low latency	High bandwidth	Reliability	Advanced analytics	Edge and fog computing	Wireless (Wi-Fi)	4G LTE/ 5G
Material handling effectiveness	Efficiently move, protect, store, and control material and products throughout manufacturing, warehouse, distribution, consumption, and disposal.	●	●	●	●	●	●	●
Safe Work 4.Zero	Use digital E2E electronic processes that incorporate work permit and equipment isolation management, resulting in increased worker safety and knowledge management for executing maintenance and turnaround work.		●	●			●	●
Vision-based inspection systems	Use cameras for vision-based applications to guide the operators in inspections, assembly operations, and error proofing, both online and offline, to improve quality and prevent errors.	●	●	●	●	●	●	●
IT/OT integration	Integrate IT systems used for data-centric computing with OT systems used to monitor events and processes and devices and make adjustments in enterprise and industrial operations through networking and communication technologies.		●	●		●	●	
Augmented reality and virtual reality	Use AR/VR technologies to train operators to perform complex assembly tasks, and for machine and tool troubleshooting and repair, such as repair of robots, machinery, and conveyors.	●	●	●	●	●	●	●
Paperless factory	Replace traditional paper-based communication in manufacturing operations with information systems such as eLogbook and Digital Asset History Card. Provide electronic work instructions on mobile devices for operations and maintenance crews.		●		●		●	

© 2019 Cisco and/or its affiliates. Copyright © 2019 Tech Mahindra. All rights reserved.

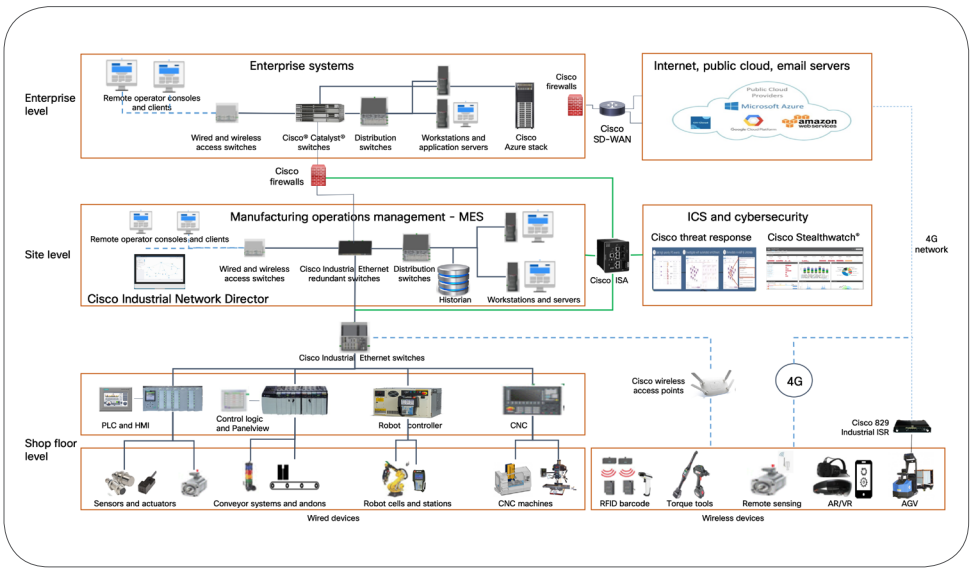
Architecture

To enable different business use cases and applications across different manufacturing IT/OT layers, Cisco and Tech Mahindra have developed a joint architecture, which is shown in Figure 3. It is the modern industrial network configuration of an industrial setup, with a unified view of secure wired and wireless connectivity. Unified wired and wireless helps simplify network management and enables you to deliver smart mobile connectivity, gain insights from your network, and connect wirelessly to control systems or I/O in challenging areas.

As factory floor infrastructure and workforce needs have become more mobile, a secure and reliable wireless infrastructure is afforded by 4G LTE moving to private 5G.

The integrated connected factory architecture acts as a blueprint for a factory design that incorporates various types of connectivity to ensure that devices are interconnected with each other, data centers, the cloud, other factories, and the IT networks reliably and securely.

Figure 3 Reference architecture



Networking and automation—a few key technology trends

Industrial switching

Industrial switching has been static, capable of providing wired connectivity only to the equipment and systems. While there have been tremendous advancements in enterprise switching, the benefits have not always extended to industrial switches.

Cisco recently extended its digital networking architecture capabilities to industry switches as well. With these new capabilities, factory plants can have deeper insights into the data that is traveling through the network, use machine learning capabilities to analyze the data, have a view of health of the entire network, and also get information on exactly where issues are occurring, with remediation guidance. These capabilities dramatically increase the performance of the network and reduce downtime significantly.

The network has security built into it, as well the ability to identify normal and abnormal traffic patterns. If it detects any abnormality, it can immediately contain the affected area and isolate it. It also has automation capabilities built in that enable networks to be built quicker and changes to be executed faster.

All these capabilities reduce the overall operational costs significantly, plus network uptime is higher, with fewer errors due to manual processes.
The wired and wireless architecture makes the entire factory network a unified platform with a single pane for management.

© 2019 Cisco and/or its affiliates.
Copyright © 2019 Tech Mahindra. All rights reserved.

SD-WAN

Traditionally, manufacturing has used WAN functions to connect users at the plant level to the enterprise applications hosted on servers in the data center. Typically, dedicated Multiprotocol Label Switching (MPLS) circuits were used to help ensure security and reliable connectivity. However, this arrangement no longer works in a cloud-centric world. As businesses race to adopt the use of software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS) applications in multiple clouds, the application experience deteriorates. That is because WANs designed for a different era are not ready for the unprecedented explosion in traffic that IoT and cloud adoption brings. Software-defined WAN (SD-WAN) is a new approach to network connectivity that lowers operational costs and improves resource usage for multisite deployments. Network administrators can use bandwidth more efficiently and can help ensure the highest level of performance for critical applications without sacrificing security or data privacy.

In environments in which a large number of connected factories are spread across multiple geographies, the cost of connectivity and the reliability of communication between the factories and the applications hosted either in the cloud or in data centers should be evaluated. The benefits of secure SD-WAN and the cost benefits of internet links instead of the expensive MPLS/leased lines could lower operational costs significantly. In addition, SD-WAN increases the reliability of SaaS and analytics applications in the cloud.

Fog and edge computing

Fog computing brings intelligence to the shop floor network, as shown in the reference architecture in Figure 3 (at the shop floor level), processing the data in a fog node or IoT gateway. And edge computing brings intelligence, processing power, and communication capabilities to an edge gateway or directly into devices such as programmable automation controllers (PACs).

The data from the control system program is sent to an OPC server or protocol gateway. This converts the data into a protocol such as MQTT or HTTP that internet systems understand. The data is then sent to another system, such as a fog node or IoT gateway on the LAN, which collects the data and performs higher-level processing and analysis. This system filters, analyzes, processes, and may even store the data for transmission to the cloud or WAN at a later date. Fog computing's architecture relies on many links in a communication chain to move data from the physical world of our assets into the digital world of information technology.

IPv6

An important inflection point occurred in 2008, when the number of things connected to the Internet surpassed the human population. An interesting trend contributing to the growth of the IoT is the shift from the consumer-based IPv4 internet of tablets and laptops—that is, information technology—to an operational technology-based IPv6 internet of machine-to-machine interactions. This IPv6 internet includes sensors, smart objects, and clustered systems and is one of the most important enablers of the IoT, as it is not possible to add billions of devices to the IPv4 internet. IPv6 remedies the depletion of the nearly 4.3 billion IPv4 32-bit addresses with a theoretically endless supply of unique 128-bit addresses.

However, the transition to IPv6 needs to be planned well and requires an in-depth analysis of the current factory environment. We recommend that you first check with your ISP about IPv6 support, and check your equipment's operating systems and applications to see if they are compatible. Your transition strategy should be based on these results. Some of our recommendations would then include the following:

- Start by using a dual-stack technology to combine native IPv6 and IPv4 systems
- Apply a transition mechanism to connect through your dual-stack systems to IPv6 resources over an IPv4-only network
- Use translation services to connect IPv6 users who need to access IPv4 content
- Add security for IPv6. The processing and configuration of IPv6 initially presents compatibility issues and security risks that must be addressed by software and configuration updates
- Deploy incrementally and test

© 2019 Cisco and/or its affiliates. Copyright © 2019 Tech Mahindra. All rights reserved.

Security in the factory of the future

While factories of the future will empower the manufacturing business and processes, the connected nature of smart factories exposes them to a variety of potential cyber threats. This exposure is the biggest bottleneck in the adoption of digital technologies in production environments. It makes security a vital component that needs to be addressed for continual success.

A smart factory's system includes countless pieces of equipment and devices that are connected to a single network. Vulnerabilities in any one of those devices can create a gap in the network that could open the system up to security threats. Factories of the future will have to build a comprehensive cybersecurity plan that includes the following:

- Threats from IT/OT convergence
- Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
- Man-in-the-middle attack
- Stolen data due to gaps in the manufacturing process
- Anomalies based on human behavior
- Critical system access to third-party contractors
- Legacy programmable logic controllers (PLCs), remote terminal units (RTUs), supervisory control and data acquisition (SCADA) servers, and historians integrated with IoT devices
- Lack of adequate visibility and cyber resiliency

From a factory viewpoint, OT systems have predominantly been isolated from external networks for many decades. However, due to the advent of TCP/IP and Ethernet communications within OT environments, the OT elements have become susceptible to cyber attacks in the past few years. Driven by automation and IoT, factories of the future present an industrial utopia with incredibly low downtimes, high levels of customization, and real-time data transparency—all leading to a more profitable and error-free production process.

To circumvent cyber attacks, several guidelines and standards, such as IEC-62443 and NIST 800-82, have mandated security controls on industrial control system (ICS) networks. Regular assessment of active components, including PLCs, field devices, RTUs, human-machine interfaces (HMIs), historians, and SCADA servers, is highly recommended to rule out

any security vulnerabilities. Besides migrating from flat networks, VLANs to segmented networks would minimize the security risk in ICS networks.

Preventing external communication is also highly recommended. Such communication should be allowed only on an as-needed basis by introducing data diodes, application whitelisting, and two-factor authentication. In addition, we recommend introducing military-grade deception technology to prevent adversaries from reaching the crown jewels. Further, we highly recommend bringing in a tamper-proof blockchain-based identity and access management layer on top of existing password-driven active devices while communicating over the edge, distribution, and core layers of network.

Human behavior-based anomalies and insider attacks constitute more than 70 percent of attack scenarios in ICS networks, besides industrial cyber threats and vulnerabilities. In light of this, continuous monitoring for industrial cyber threats and human behavior-based anomalies, correlated on a security information and event management (SIEM) platform, would facilitate incident response management and reduce the mean time to resolve any critical incidents.

In short, the above measures, with continuous threat monitoring of ICS, would help prevent cyber threats, including ransomware attacks such as WannaCry and malware insertion into ICS networks. Convergence of IT and OT security is highly recommended to combat sophisticated adversarial attempts. ICS governance should exercise caution when letting removable media into operational areas, and scanning of USB is strongly recommended.

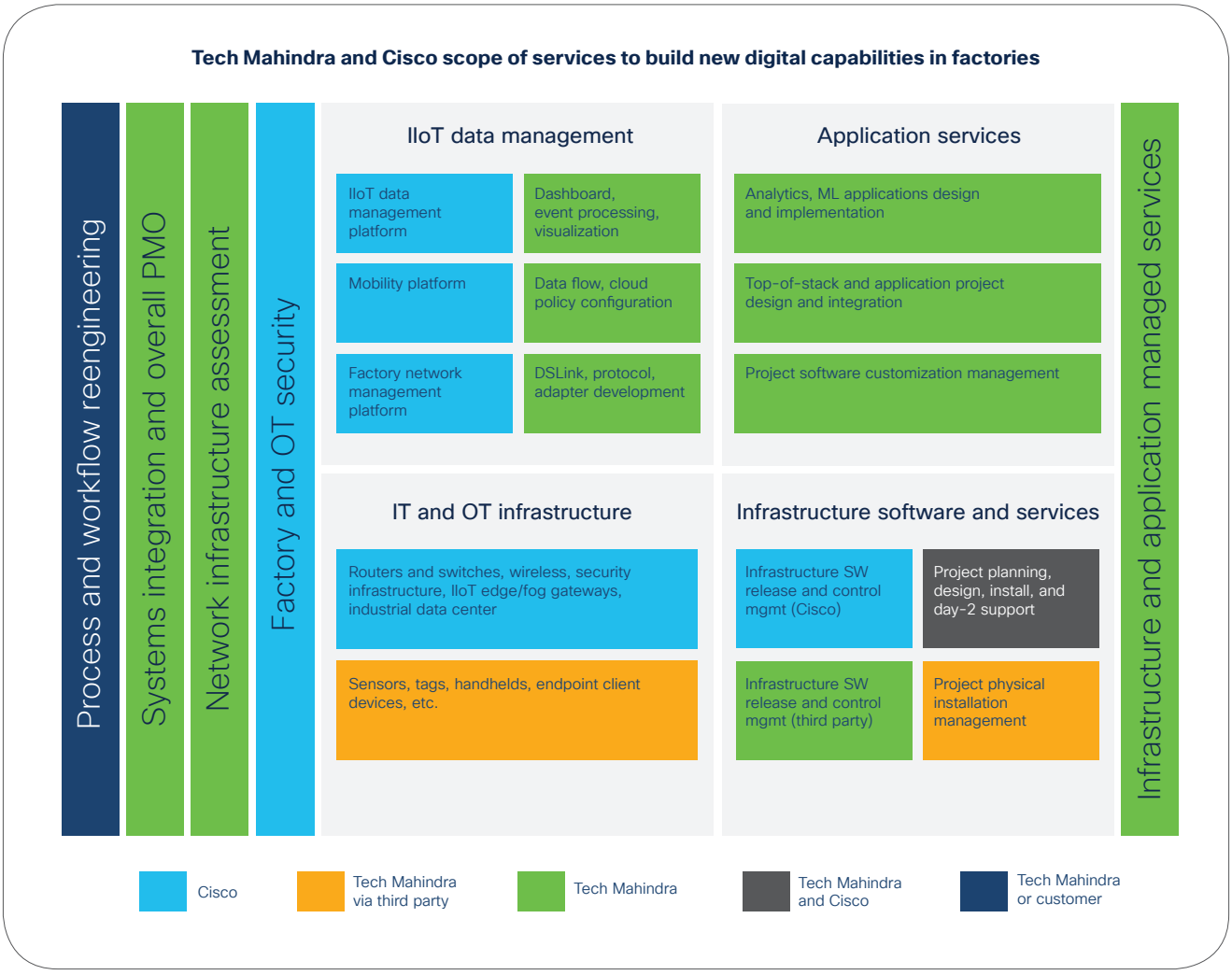
© 2019 Cisco and/or its affiliates. Copyright © 2019 Tech Mahindra. All rights reserved.

Cisco and Tech Mahindra's solutions and services

Cisco and Tech Mahindra solutions provide end-to-end business and technology solutions in the factory infrastructure space, making it possible for manufacturers to move toward their Industry 4.0 goals. The partnership spans various business, functional, and technological areas, and key highlights of the alliance for the factory infrastructure space include:

- Network infrastructure assessment and consultancy services that provide a complete assessment of the current infrastructure and roadmap development, from your factory infrastructure needs to the factory to enterprise connectivity
- Implementation in IT/OT areas, including sensorization, data collection, analysis, and providing closed-loop feedback
- Design, plan, implementation, and management of infrastructure services, factory applications, and security services

Figure 4. Solutions and services offered by Cisco and Tech Mahindra



Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R) Copyright © 2019 Tech Mahindra. All rights reserved.