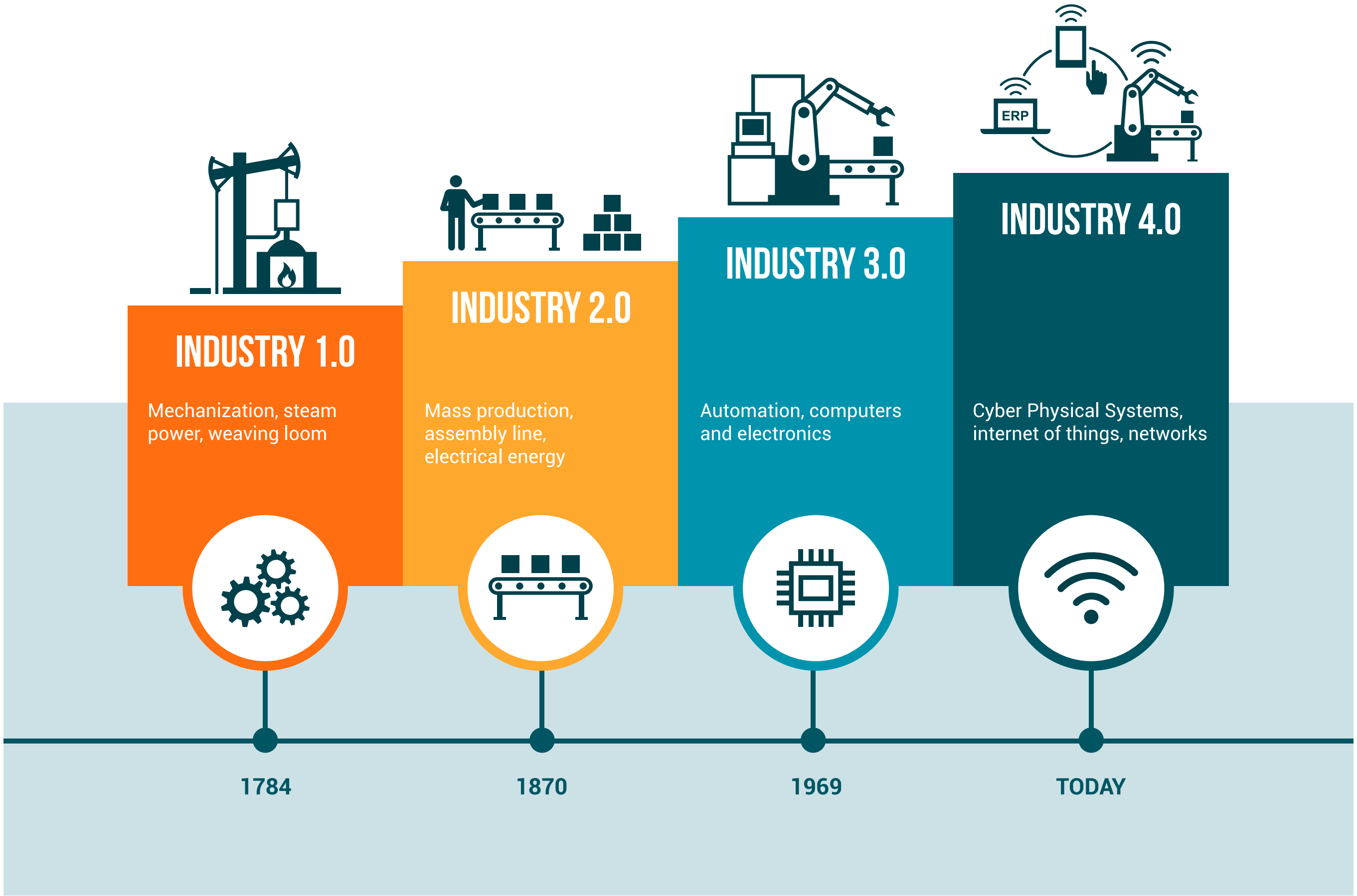
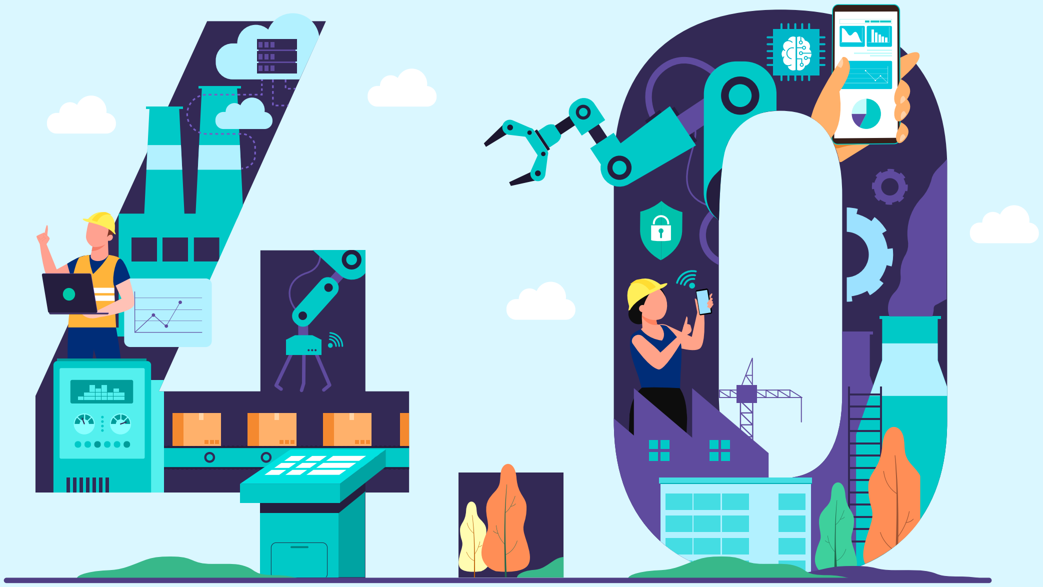
Network and Cloud Technologies for Industry 4.0

February 2022, Turnium.com and Comms365.com


ERP
INDUSTRY 1.0
Mechanization, steam power, weaving loom
INDUSTRY 2.0
Mass production, assembly line, electrical energy
INDUSTRY 3.0
Automation, computers and electronics
INDUSTRY 4.0
Cyber Physical Systems, internet of things, networks
1784
1870
1969
TODAY

The industrial world has experienced three periods of radical transformation and is now in the fourth great transformation driven by the Internet of Things. This transformation is based on interconnecting devices, people, processes, and tools and is driving an ever-increasing quantity of transactional data that requires secure transfer to the cloud computing services and storage that are required to deliver IoT solutions globally. At the same time, machine learning (ML) and artificial intelligence (AI) are required to process data at the network edge efficiently.

Turnium SD-WAN delivers a secure, disaggregated, networking foundation that supports and substantially enhances Industrial Internet of Things (IIoT) deployments. Turnium enables service providers and enterprises to network IIoT devices easily and securely at geographically dispersed sites with private or public clouds and in a cost-effective manner. Channel partners can deploy Turnium to build fixed-mobile and mobile-mobile converged networks using any combination of available wired and wireless connection at each site or IoT node. Turnium aggregates the multiple circuits, treating them as a single connection at each site, and enables multi-path failover, making any IIoT deployment highly resilient and redundant.



Industry 4.0 and the Industrial Edge

Industry 4.0 creates a substantial impact on business and business networking requirements. It creates an environment in which IIoT devices and smart devices are ubiquitous and need constant connection to the Internet.

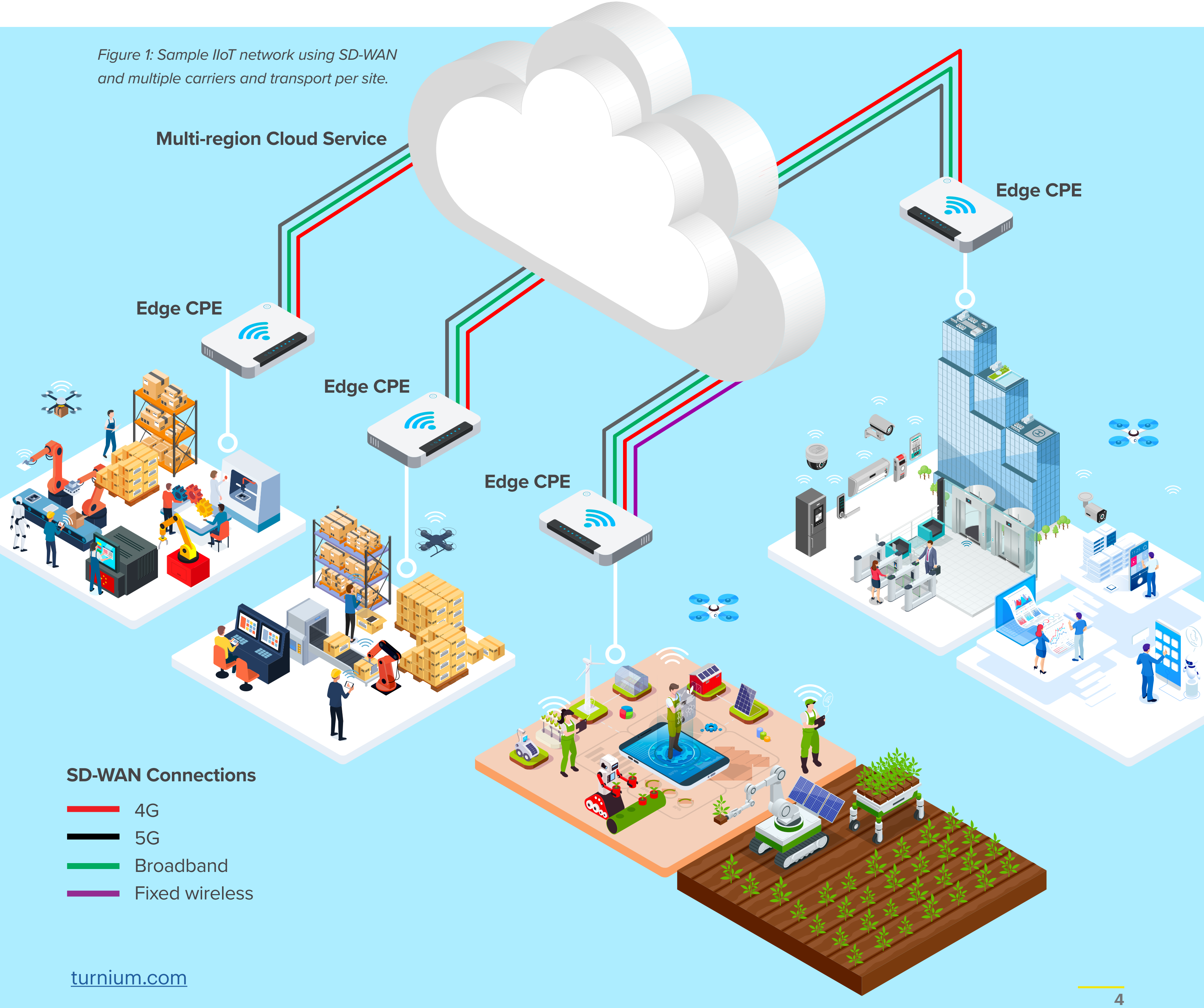
To meet the "constantly connected" requirement, IIoT deployments must leverage multiple technologies. Iot and IIoT devices themselves may communicate on-site with long range transmission technologies such as LoRaWAN, Narrowband IoT (NB-IoT) and LTE-M, or short-range variants such as Bluetooth Low Energy (BLE), Zigbee and others. In turn, each site must communicate IIoT telemetry and commands to-and-from the public or private cloud repositories in which the various command, control, and database applications are hosted. This creates a virtual 'river' of data (fed by diverse systems and assets) requiring orchestration of security, routing priority and resilience. This is where Turnium's SD-WAN and Industrial Edge solutions create a significant impact.

Network Tools for the Edge in Industrial 4.0

The simplest solution for site-to-cloud connectivity is to use a combination of whatever is available; to use circuits from any available carrier and transport technology at each site and then connect all these circuits and technologies together in software.

Turnium enables services providers and enterprises to build multiple national, regional, or global SD-WAN overlay networks using multiple underlying carriers, multiple transport technologies, and non-proprietary white-box x86 CPE and servers. Individual site connectivity can be built using multiple 3G, LTE, 4G, 5G or MPLS, VPLS, cable, xDSL, wired ethernet or fixed wireless circuits. Turnium's highly flexible connectivity-focused SD-WAN is uniquely suited to delivering the Industry 4.0 networking tools required.

Figure 1: Sample IIoT network using SD-WAN and multiple carriers and transport per site.



Moving data from industrial edge IIoT devices to the cloud creates distinct challenges for security and performance. As Gartner says, “as IoT deployments grow, the production and consumption of data will also grow. Gartner forecasts IoT units to grow with an 11% CAGR through 2030. However, data-heavy verticals will grow even faster (e.g., IoT unit growth in manufacturing and natural resources will grow with a CAGR of 18% through 2030)[1]. And the risk of data compromise will increase along with the risk of the physical accessibility of IIoT devices.

At the same time, IIoT devices have round-trip latency requirements that must be met to keep the device performing correctly and to meet end-user expectations of the data’s currency and accuracy.

[1] “Predicts 2022: The Distributed Enterprise Drives Computing to the Edge.” 20 October 2021. Thomas Bittman, Bob Gill, Tim Zimmerman, Ted Friedman, Neil MacDonald, Karen Brown.

Latency and IoT Networks for Industrial vs Critical/Real-time Use Cases

IoT deployments can be divided into two rough categories:

- *Massive IoT* involving large-scale industrial deployments with many IoT devices sending data through multiple nodes to the application layer, and,

- *Critical IoT* in which data and responses to the IoT device are time-sensitive and must have a guarantee associated with data delivery. A critical IoT application has tighter latencies as well as associated reliability.

In a Massive or Industrial deployment, the entire network including the IoT device, local nodes, WAN circuits, and application controller, must have a round-trip latency of less than 2 seconds to transmit messages and respond with appropriate IIoT device commands.[2] In LoRaWAN networks for example, the distance that an IoT sensor measuring gas concentrations is from a receiving IoT base station/gateway impacts the transmission time on air, which in turn has a demonstrable impact on latency and the real-time nature of the data received.

By contrast in Critical deployments, data must be delivered in 50ms or less, with a 99.9% reliability, for example. This would apply to use cases involving robotic control, mobility automation, remote control, vital signs monitoring, and real-time media. Deploying Edge Computing as part of the Industry 4.0 networking tool-set can improve performance in critical IoT scenarios to reduce latency to the 5ms range.
In any IoT network, the overall design has a large impact on performance. The number of local nodes and the volume of tenant devices per node, as well as the frequency of data transmission and the distance from the local node (power consumption of the transmission) will influence overall performance.

The below figures from UK's O2 (now part of Virgin Media in a JV between Liberty Global and Telefonica) provide useful summaries of IoT cellular technologies, use-cases and the associated latency and data rate requirements.

[2] https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/critical-iot-connectivity and https://arxiv.org/pdf/1708.02562.pdf

HIGH ← LATENCY → LOW

NB-IoT	LTE-M
• Focused on low data rates • Higher latency-suited to batch communication • Ideal for simpler static sensor applications	• Highest throughput speed and highest bandwidth of any LPWA technology • Lowest latency of any LPWA technology - suited to real time communication • Ideal for fixed and mobility applications

LOW ← SPEED → HIGH

Figure 2: Narrowband-IoT (NB-IoT) vs Long Term Evolution for Machines (LTE-M) Comparison by O2/Telefonica UK

Applications	NB-IoT	LTE-M
Smart Metering	✓	✓
Waste Management	✓	✓
Smart Building	✓	✓
Agriculture	✓	✓
Smart City	✓	✓
Intelligent Street Furniture	✓	✓
Asset Tracking & Monitoring	✓	✓
Smart Grid	✓	✓
Transport & Logistics	✗	✓
Home Security	✗	✓
Assisted Living	✗	✓
Industrial IoT	✓	✓
Retail	✗	✓
Consumer Devices & Wearables	✗	✓

Figure 3: Application Use Cases and Suitability for Higher Latency (NB-IoT) vs Low Latency (LTE-M) from O2/Telefonica UK[3]

In all use-cases, attention must be paid to security, suggesting that IIoT commands and telemetry must be encrypted in-transit.

[3] https://www.o2.co.uk/business/solutions/iot/lte-m

uCPE Hubs at IIoT Sites

Universal CPE (uCPE), which are often IoT hub devices, help to facilitate the deployment and management of networks that support IIoT devices (e.g., robotics, sensors). A secure connection to data warehouse facilities or a “secure on-ramp” to the public cloud is imperative for secure operations. Building such as secure on-ramp is simpler when deploying multi-path bonding technologies such as Turnium SD-WAN.

uCPE that are part of a Turnium SD-WAN transmit packets from their downstream sensors to upstream cloud computing and storage resources across the multiple circuits that are used to create the WAN. Splitting the packets across multiple circuits, and encrypting the packets in the process, is one way that Turnium secures IoT data in-transit and obfuscates data to mitigate the possibility of man-in-the-middle intercepts. This is possible as data (1) is encrypted and (2) is transmitted over multiple circuits and transmission technologies from multiple carrier connections, breaking up a single flow into non-consecutive packets that are transmitted over the multiple circuits.

Organizations that are in the process of modernizing their operations are looking to IoT and IIoT as part of their Industry 4.0 tools and transformation. Realizing the promise of IoT or IIoT while maintaining security requires the organization or its services providers to deploy secure, high-performance connectivity and to automate management functions such as network deployment and the process of bringing uCPE online.

Containers or VMs at the Edge?

When deploying SD-WAN networks, service providers and enterprises must also determine the specific technologies to deploy at the edge. In addition to selecting a uCPE hardware vendor, decisions must be made around how to deploy the SD-WAN software and any other required applications on the uCPE. In the past, the choice was limited to bare metal or virtual machines.

However, with the development of container technologies such as Kubernetes, Docker, and others, there is a clear benefit to using containers on bare metal over virtual machines.

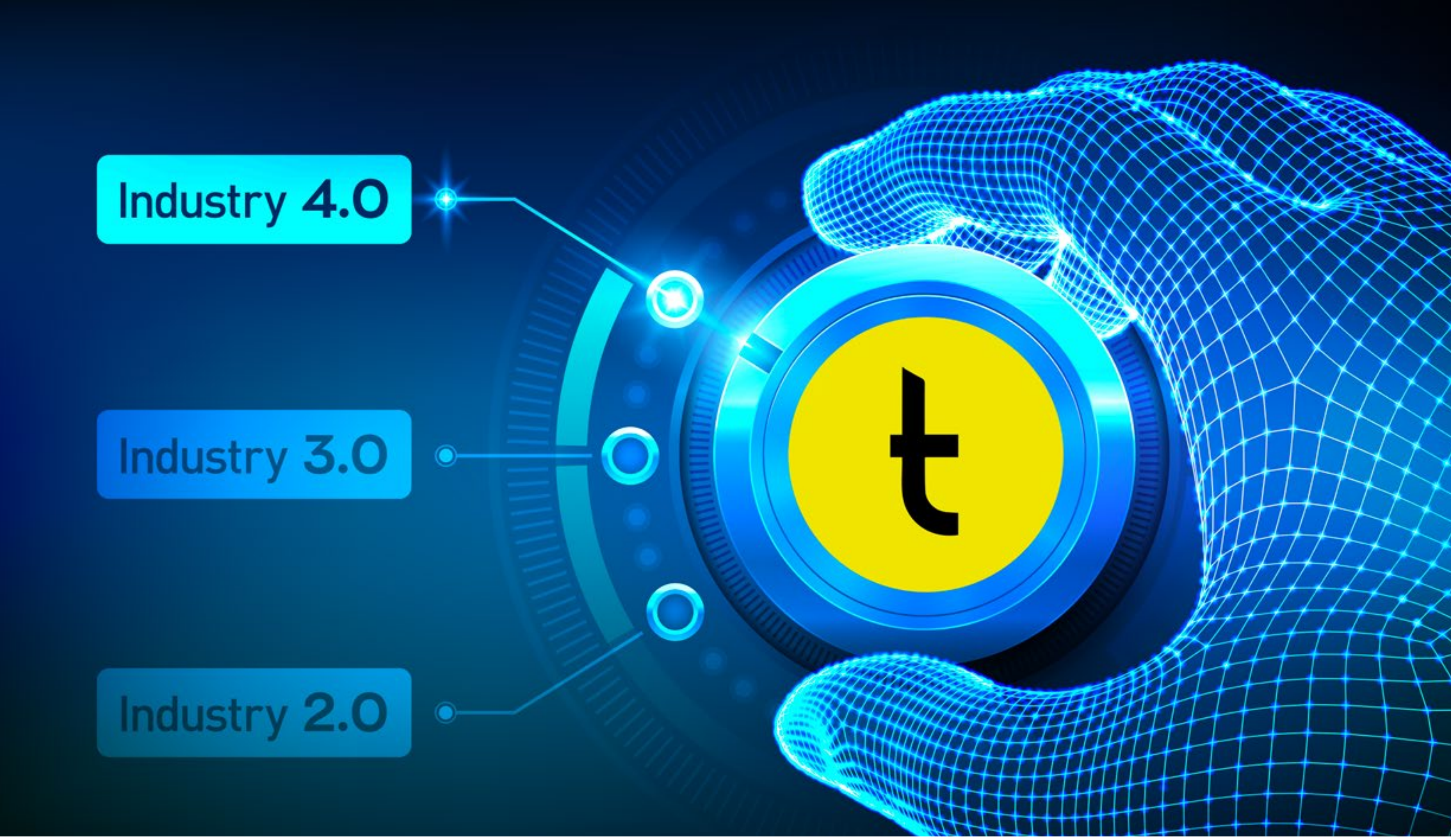
Containers on bare metal	Virtual machines
Management node/console No hypervisor overhead = no resource penalty	Management node/console Hypervisor overhead reduces VM performance
Simple workload deployment and mobility	VMs have to be restarted or workloads uninstalled/installed to deploy new code
Enables DevOps and continuous deployment (CI/CD) for cloud-native applications	VMs are better suited for static workloads that do not change much over time
Containers are easily moveable from one machine to another regardless of geography; the only prerequisite is that the correct packages are installed in the destination machine	VMs must be backed up, shutdown, copied to a location that is local to the destination server and then booted locally from memory
Smaller footprint, easier to manage	Larger footprint requires special skill sets to manage
Simple deployments of multiple workloads on a small form factor purpose-driven device, that can become remote or mobile	Complex deployments on large form factor devices, which often need to remain in one place

Cloud-native, disaggregated Network Architecture: Industry 4.0 Technology for Success

Cloud-native solutions have become more popular as service providers and enterprises need to connect multiple devices to multiple clouds across multiple geographies. As a result, organizations need to evaluate the workloads they want to push to the edge, why, and ensure that the implications for the edge applications are acceptable.

Dynamically pushing workloads to the edge and using cost-effective hardware requires a smaller software footprint. This means that edge hardware needs to run efficient platforms as offered by container technologies; containers offer the ability to deploy, run, and then terminate applications dynamically on edge devices. As a result, Edge compute and IIoT networks need to use a disaggregated approach.
IIoT devices are, by definition, dispersed and require a security architecture that can match that dispersion. Therefore, customers also need an approach to SD-WAN or SASE networking that is disaggregated and allows each enterprise or its service providers to assemble network deployment, monitoring, management, and security building blocks over top of a robust SD-WAN foundation. This enables the SD-WAN to integrate with existing applications that the enterprise has deployed, integrated with each other, and that staff are already familiar with using.

A common single-vendor approach is to deploy an integrated stack of proprietary, monolithic, black-box security and networking that negates customer preference and locks them into long term contracts whose advantage of scope and scale goes to the service provider, not the customer. However, without involving certified security experts with domain knowledge of the customer's industry, any such deployment is simply a cookie cutter solution that may not address the customer's specific needs and risks.
In contrast, a disaggregated architecture can incorporate a customer's preferred security vendors and applications from solution providers who have knowledge of the customer's needs and who can apply domain expertise. A disaggregated approach enables the network to integrate with existing network management and monitoring solutions, as well as with existing security solutions and existing data networks.



Turnium Disaggregated SD-WAN: A Tool for Industry 4.0 Transformation

Turnium's disaggregated approach to SD-WAN delivers the secure, scalable networking layer in a disaggregated SASE solution. Turnium provides a secure and scalable foundation on top of which existing or new applications can be deployed to meet a customer's unique requirements.
Turnium's SD-WAN is designed to be simple and flexible enough for organizations to easily manage and scale their enterprise WAN across the Internet and over multiple connection types (e.g., ethernet, LTE/5G, MPLS, etc.). It also delivers bi-directional, elastic QoS and secure data transfer over multiple aggregated circuits at each site and integrates easily with a customer's preferred security vendor(s), business applications, and operational systems.

Use cases for traffic light management, drones, tire pressure monitoring for construction, agriculture, and healthcare are real and in the wild right now. The ability to build the network stack in a flexible manner is the only way to truly get to the industrial edge, and Turnium's SD-WAN allows customers to build and design their own secure solutions by including Turnium's flexible layer-3 software solution.

Why Turnium?

Service Providers choose Turnium for its disaggregated, software-only, containerized Layer 3 managed network-as-a-service platform. Turnium delivers the foundation that enables service providers and enterprises to build their own unique bundled offerings, including IIoT and SASE, for specific verticals, markets, and customer segments.

- Deployable in Debian, OpenSUSE Leap, Red Hat Enterprise Linux, and virtualization environments.
- Non-proprietary hardware for optimized cost, sparing, and procurement.
- Seamless multi-path network convergence over multiple wired or wireless circuits for multi-carrier site and device survivability.
- Packet-based link load balancing and IP extension for session survivability.
- Automatic network node configuration and built-in encryption simplifies deployment, management, and increases security.
- Managed service reseller licensing option for IT consultants and VAR.
- White-label, partner-hosted licensing telecommunication service providers, managed service, and internet service provider profitability.
- Use your existing service provider IP addressing.
- CNF Certified with Red Hat OpenShift for container deployments with enterprise-grade scale and support.
- IBM ROKS certification (Red Hat OpenShift Kubernetes Service) for deployment in IBM Cloud using OpenShift-as-a-Service.
- IBM Cloud PAK for Network Automation certification.

Learn More

To learn more about how Turnium and Comms365 can provide complete IoT solutions for your enterprise, utility, or service provider business, please contact us at sales@ttgi.io or follow us on Twitter @turnium.

Turnium Technology Group, Inc.
1127 West 15th Street
North Vancouver, BC, Canada
V7P 1M7
Tel: +1-604 398 4314
Email: sales@ttgi.io

COMMS365 Limited
South House 3, Bond Avenue
Milton Keynes, UK
MK1 1SW
Tel: 01234 865880
Email: sales@comms365.com

turnium

comms365