Connected World.
Connected Experiences.

Tech Mahindra

WIRELESS SECURE FACTORY

Post COVID, Robotics & Automation will be on rise which will lead to rise in Remote worker, Remote asset management use cases All these will require a secure – high bandwidth –low latency network.

The old, distributed, low bandwidth-latency network is a bottleneck for a new way of working.

There is a need to upgrade Enterprise & Industrial network and plan for the edge devices, support network for remote working. & underline Security. Remote working R&D, Field technician will need strong wireless network and end point cybersecurity.

Industry Challenges

- Key use cases like Robotics, IoT, Remote worker, AR-VR need low latency and high bandwidth.
- Network systems are vulnerable to cyber attacks
- Higher cost associated with Maintaining the legacy systems
- Need a way to connect all the key vendors/protocols
- Industry 4.0 will require massive number of devices from different vendors/protocols to be connected plus massive amount of data to be collected and analyzed.

Tech Mahindra Solution

1. Inside the 4 walls of factory, warehouses: ETHERNET, WIFI6, Private Network, LTE/5G

2. Outside 4 walls: Global enterprise connectivity with SD-WAN
3. OT Cybersecurity

4. Multi access EDGE Compute 3 tier architecture

Business Benefits & TechM Capabilities

- Monitor and Identify network issues before it causes the downtime or any external cyber attacks.
- Manage the new data flow from different systems effectively
- High level of IT networking and IT security enterprise.
- Bring all the un connected networks under the one umbrella

Case Studies

Industry Security Assessment for a leading American OEM

It included IT and OT Integration security Gaps, Industrial / OT Network performance Gaps

Wireless Mines to facilitate digitalization for a large mine company in South Africa

Value delivered: Better Performance in terms of higher bandwidth. Lower Cost compared to traditional LANs

Contact Us : MFG@TechMahindra.com