

NETWORK SEGMENTATION WITH AN INDUSTRIAL ETHERNET ROUTER

HIGHLIGHTS

- ✓ Industrial production is unimaginable without the digitalisation of manufacturing, which enhances the efficiency of production devices.
- ✓ Network segmentation is crucial for advanced control, enhanced security, and improved performance and reliability. It ensures that only specific recipients have access to confidential data.
- ✓ The RUT140 Ethernet router is excellent for network segmentation while also providing network security, seamless connectivity, network traffic optimisation, and control of data flow.

THE CHALLENGE – A PRIVATE NETWORK FOR CONFIDENTIAL DATA

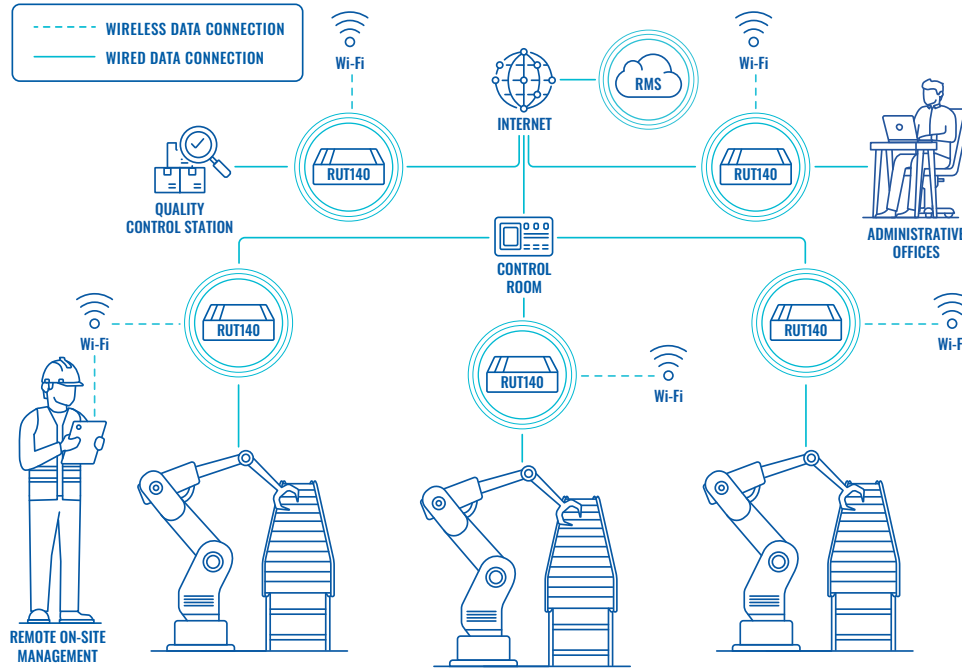
The global manufacturing sector has reached a value of almost \$20 trillion in 2023. Naturally, this makes it important for manufacturers to work without disruptions that would result in loss of goods, time, and huge profits.

Industrial manufacturing companies improve their efficiency with the help of automation and modernising their operations. Besides many production lines that contain separate sets of control systems and machinery, manufacturing facilities also have quality control areas and administrative offices. All of these fields contain sensitive data and different security and access requirements.

Additionally, external vendors or contractors might also need access to certain internal systems or equipment. That is because vendors might need specific data to assess the manufacturing process in real time and base decisions on this data.

These diverse operational requirements and different levels of sensitive data access needed network segmentation that would enhance network security levels, optimise data flow, and isolate critical systems. That is where the Teltonika Networks RUT140 Ethernet router steps in.

TOPOLOGY



THE SOLUTION – NETWORK WITHIN NETWORK

The RUT140 is a compact industrial Ethernet router designed to ensure the security of sensitive data by creating a new network within an existing one. Network segmentation means dividing the network into smaller segments by adding a router with an integrated Network Address Translation (NAT) feature. That way, a router is able to create a new network within an existing one, giving access to the data only for specific recipients.

Separate networks enable manufacturers to provide controlled and limited access to external entities without exposing the entire network. This way, an industrial manufacturing facility can reduce the amount of security breaches and maintain data integrity while enabling communication between production lines and data control systems.

Although the feature of creating a network within an existing network is quite common in routers, our industrial router stands out as one of the best-suited network devices for this particular task. With a compact size of 113.10 x 25 x 68.6 mm, this Ethernet router fits right into an industrial environment, such as automation cabinets.

The integrated DIN rail bracket allows for easy installation in any control box, while the industry-focused 3-pin power connector prevents power surges by grounding leads in industrial applications. In addition to this, our RUT140 is a front-facing connectivity device, which allows easy access to its antenna and two Ethernet ports for LAN and WAN.

Moreover, our industrial router comes with RutOS and supports industrial protocols like Modbus, DLMS, DNP3, and OPC UA, allowing it to work perfectly in an industrial setting. These protocols ensure compatibility with many different industrial systems and devices. This Ethernet router also has many built-in VPNs that allow for easy integration of secure communication with external entities and networks.

This Ethernet router is equipped with Wi-Fi 4 for efficient on-site management. By connecting to the device via Wi-Fi, engineers can effortlessly access and manage the device, without accessing the control box on-site.

Finally, the RUT140 is supported by our Remote Management System (RMS), allowing for remote management and monitoring. Using this system, engineers can remotely fix connection issues and hiccups, such as disrupted connectivity.

