No remote access in this extra-secured Edge gateway, instead, the onboard key controls separation, at physical layer, of a dedicated data acquisition port.

This allows the unit to securely acquire field data, process it and push it to a cloud application, without leaving any possibility for a cloud-to-field transfer. mbXLINK offers all mbEDGE.advanced functionalities on a dedicated platform, combined with the advantages brought by the hardware secure element.

SPECIFICATIONS

- ✓ Pre-Installed Docker Engine
- ✓ Pre-Installed Containers:
  - Portainer.io to manage Docker Containers
  - Node-RED for easy programming
  - Optional: 3 containers for running user application
- ✓ Node-RED provides:
  - Web-based programming user-Interface with Drag&Drop
  - Industrial protocols: MQTT, OPC-UA, Modbus, S7 and more
  - Cloud connectivity: Azure, IBM, Amazon and more
  - TCP/IP, HTTPs, Email, Twitter and more
  - User defined function-blocks
  - mbCONNECT24 node to connect with dashboards & widgets
- ✓ Data stored on the SD card is encrypted
- ✓ 8GB industrial grade SD card (MLC NAND, UHS-I Interface)
- ✓ Temperature (usage): -40 to 85°C
- ✓ Dimensions: 24mm x 32mm x 2,1mm

Order Details

Name	Type	Item No.	Node-RED	Node-RED User-Nodes	Docker Container	Portainer.IO
mbEDGE.start	EDG100	1.901.000.01.00	√	-	-	-
mbEDGE.advanced	EDG200	1.902.000.01.00	√	√	√	√

www.mbconnectline.com

MB connect line GmbH
Winnettener Str. 6
91550 Dinkelsbuehl

Tel.: + 49 (0) 9851 / 58 25 29 0
Fax: + 49 (0) 9851 / 58 25 29 99

info@mbconnectline.com
www.mbconnectline.com

mbEDGE_EN_4S_15Bnov18

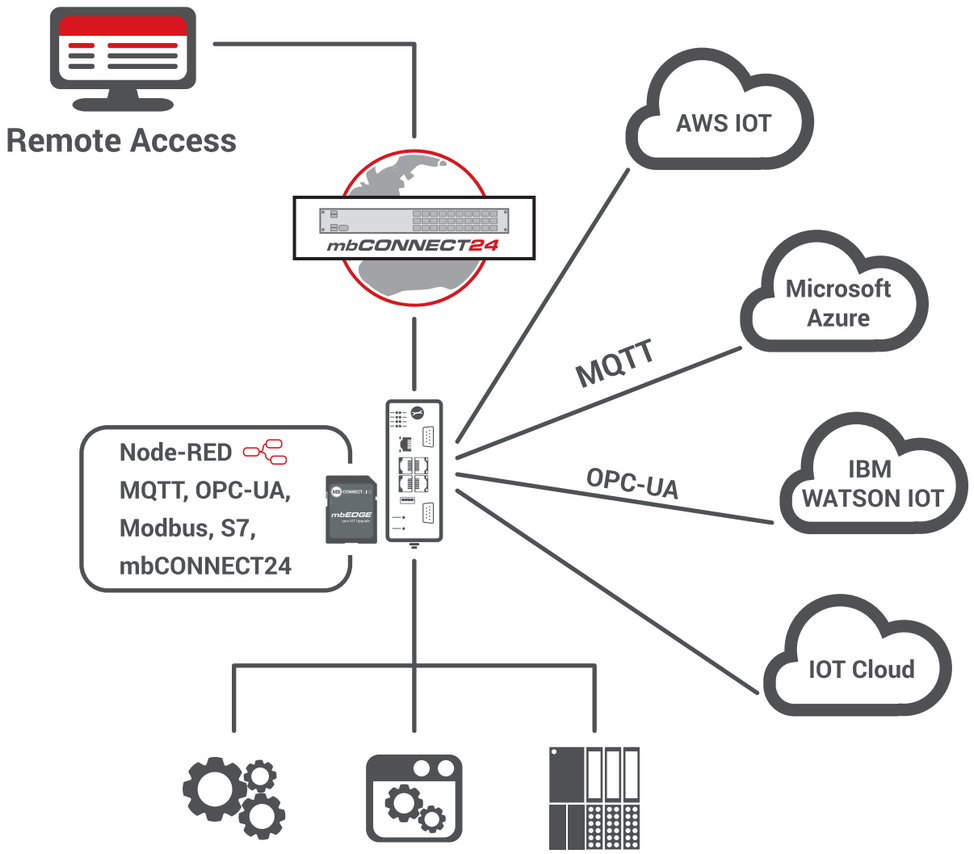
MB CONNECTLINE

mbEDGE

IOT-UPGRADE FOR YOUR REMOTE ACCESS ROUTERS

mbEDGE

UPGRADE YOUR REMOTE ACCESS TO AN IOT GATEWAY

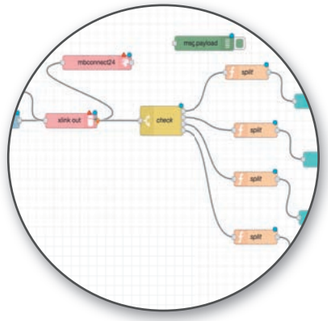


Why Edge Computing?

Data is the new gold. If remote access noticeably improved the support experience and allowed qualified engineers to perform maintenance more efficiently, data takes remote operations & services to another level. Supporting a variety of cloud platforms as well as modern communication protocols, mbEDGE option transforms your mbNET into a powerful IOT-gateway. With mbEDGE, your mbNET unit will acquire data locally, process it and push it to your cloud application.

Doubling remote access with data collection allows you to develop new services and have a closer control on remote installations. The Docker/Container technology of mbEDGE lets you to run your own applications, either within the graphical programming environment of NodeRed or, completely independently, in the virtual space of your own container.

Simplify IOT-Edge applications development with Node-RED



Node-RED simplifies the creation of your IoT-Edge application. It is web-based and consists of a graphical user interface and a library of pre-built functions & blocks of code, called nodes. Each node, standard or user defined, manages a single functionality: send an email, perform a Modbus read, communicate with mbCONNECT24, MQTT publish/subscribe, OPC-UA,...

To create your application, simply drag & drop the nodes on the design sheet, connect them following the logical flow of actions and configure them according to your application context.

With Node-RED, you will acquire data, process it and post it to your preferred cloud application. The Node-RED container has access to all mbNET resources.

Docker & Containers: running your embedded IoT-Edge app in a secure way

Docker creates virtual workspaces (containers) for user applications and manages their access to the operating system and the system resources. The containers and their applications are isolated and can only communicate through Docker controlled mechanisms.

Node-RED environment runs in such a container. With mbEDGE.advanced, you get access to a second container, running Portainer.io: a GUI for Docker, to configure and manage containers. You also get access to three more Containers, to run your own personalized applications.

Docker secures deployment & distribution of these applications and only allows signed and trusted images to run in the Containers.

Security by design, from mbNET to mbEDGE

Cybersecurity is a core competence of MB connect line and our products are created according to the principles of security by design and the standards set forward in IEC62443. To do so, MB connect line R&D engineers are certified for secure software development (TeleTrusT's T.I.S.P & T.P.S.S.E.).

mbNET platforms are equipped with a hardware secure element (crypto chip) and a Secure Boot concept that allows only signed and trusted firmware to be installed and boot.

All data stored in memory or on the mbEDGE card is encrypted, making it impossible to read without the key stored safely in the crypto chip.