Agora

AgoraGateway

Ruggedized Edge Computing Device

By harnessing the power of edge computing and data analytics, Agora is the gateway to edge intelligence. With an open, secure and scalable platform, Agora℠ edge IoT solutions enable operators to reduce nonproductive time, minimize HSE risk, enhance production and lower total operating costs.

At the center of the platform is the AgoraGateway™ ruggedized edge computing device, which collects, analyzes and transmits data from field devices to the enterprise in real time. Edge Apps—domain-specific workflows and algorithms—are deployed to the gateway to enable insights to be derived on location. Working in tandem with the platform's middleware and software solutions, the AgoraGateway also enables real-time connectivity to data ecosystems, thus revealing the actionable insights needed to transform oilfield operations.

Design and Operation

The AgoraGateway is designed to operate in the most challenging and remote environments. Built on industry standards, the ruggedized gateway meets all environmental requirements for temperature and shock and vibration. The enclosure of the AgoraGateway is NEMA 4X IP 66 certified for outdoor use.

The AgoraGateway connects to field devices from any vendor or manufacturer using standard industrial protocols. AgoraConnect℠ data transmission services provide multiple connectivity options to ensure data collected at the edge is connected to the enterprise. With cellular (4G LTE), satellite and Ethernet connection capabilities, the AgoraGateway delivers seamless, real-time communication across the edge ecosystem.

The AgoraGateway collects, manages and transmits data from field devices to the enterprise in real time.

Intrinsically Secure

The AgoraGateway is designed to minimize hardware vulnerability. The physically hardened gateway allows only necessary services to run and disables all other ports. Its robust security policy ensures that only approved applications can run on the device. For an extra layer of security, the gateway utilizes an advanced configuration that only permits outbound connections to known and trusted internet locations.

Each AgoraGateway is deployed in a unique and highly trusted manner. This approach safeguards the device and eliminates the risk associated with default configurations and credentials. The gateway's hardware-based root of trust utilizes the TPMv2.0 cryptographic chip to deliver secure communications with the cloud—minimizing the chances of attackers comprising the device and gaining access to critical data. Federation and secure hardware tokens ensure that only authorized entities can access data and perform actions.