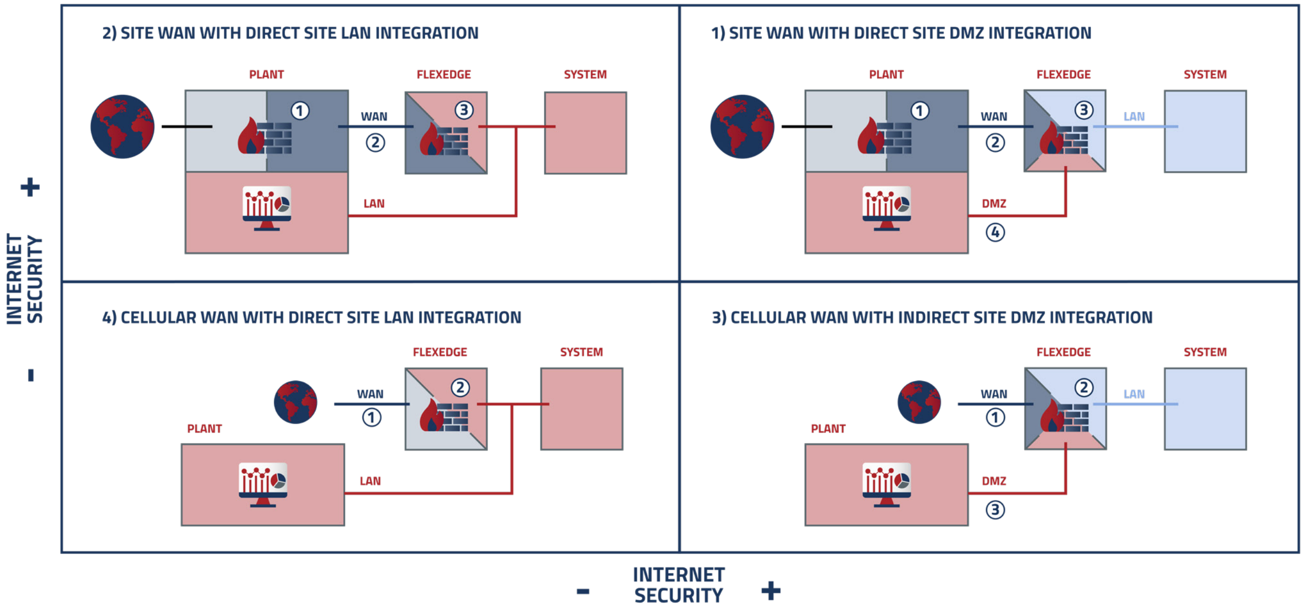
Whitepaper

IMPLEMENTING IIOT SOLUTIONS WITH FLEXEDGE®

IIoT connections must provide security features while handling multiple nodes of connectivity. As such, there are four unique topologies which can be implemented.

Scope:

When using a FlexEdge IoT device to implement IoT solutions, you can choose from four distinct network topologies, as illustrated below.


2) SITE WAN WITH DIRECT SITE LAN INTEGRATION
PLANT
FLEXEDGE
SYSTEM
1
WAN
2
3
LAN
1) SITE WAN WITH DIRECT SITE DMZ INTEGRATION
PLANT
FLEXEDGE
SYSTEM
1
WAN
2
3
LAN
DMZ
4
4) CELLULAR WAN WITH DIRECT SITE LAN INTEGRATION
FLEXEDGE
SYSTEM
WAN
1
2
PLANT
LAN
3) CELLULAR WAN WITH INDIRECT SITE DMZ INTEGRATION
FLEXEDGE
SYSTEM
WAN
1
2
LAN
PLANT
DMZ
3
+
INTERNET SECURITY
-
-
INTERNET SECURITY
+

In order from most secure to less secure, these topologies may be ranked as follows:

1. Plant internet connectivity to FlexEdge device with DMZ segregated connection to plant SCADA
2. Plant internet connectivity to FlexEdge device with direct LAN connection to plant SCADA
3. Cellular internet connectivity to FlexEdge device with DMZ segregated connection to plant SCADA
4. Cellular internet connectivity to FlexEdge device with direct LAN connection to plant SCADA

In the above arrangements, the primary areas of variance are:

- Source of internet connectivity to FlexEdge device
- Mode of system connectivity to plant SCADA

Security considerations specifically relating to these variances shall be explored within this whitepaper.

Section 1: Source of internet connectivity to FlexEdge

Internet connectivity to the FlexEdge device may be sourced from either:

A. A plant's Wide Area Network [WAN], or

B. A cellular signal from a regional Internet Service Provider [ISP]

For the two scenarios above, it is advised to choose option "A" since it allows for implementing extra security measures before connecting the FlexEdge device to the internet.

Plant WAN

In situations where a plant's WAN supplies internet connectivity to FlexEdge devices, the connection should be completely firewalled, except for the following minimum network requirements:

- Public internet access via a Class A, B, or C private network
- VPN traffic allowed via TCP/IP Port 1194
- MQTT-over-TLS/SSL traffic allowed via TCP/IP Port 8883
- DNS resolution and free traffic towards VPN & data acquisition servers
- Encrypted traffic allowed

If the plant's internet connectivity for the FlexEdge device does not meet these minimum network requirements, some or all features of your IoT application may be compromised or unattainable.

Cellular WAN

When FlexEdge devices receive internet connectivity through a cellular signal from a regional ISP, it is recommended that the plant owner or operator manages the cellular service contract. This allows for better administrative control over cellular internet connectivity within the plant's domain. Consider implementing the following security measures:

- Disabling/Blocking of voice services
- Disabling/Blocking of P2P SMS services
- Utilize data caps to regulate/monitor how much data is transferred
- Use cellular ISPs which incorporate real-time monitoring and anomaly detection

Typically, IoT-focused cellular connectivity providers offer network firewalls that restrict data services accessible by a device (or SIM card) - for example, allowing traffic only to specific IP addresses or ranges. This effectively limits the SIM card's data service to its intended application.

Section 2: Mode of System Connectivity to Plant SCADA

System connectivity to a plant's SCADA may be implemented via either:

A. 'Demilitarized Zone' [DMZ] segregated connection to plant SCADA, or
B. A direct Local Area Network [LAN] connection to plant SCADA

For the two scenarios above, it is recommended to choose Option 'A', as it provides the ability to implement extra security measures and flexibility between the system and the plant's SCADA network.

DMZ segregated connection to Plant SCADA

In cases where the system connects to a plant's SCADA network through a separate 'Demilitarized Zone' (DMZ), the following additional security measures and flexibility can be applied:

- Stateful firewalled routing
- Network Address Translation [NAT]
- Completely disabled routing between WAN and DMZ

Direct Local Area Network [LAN] connection to Plant SCADA

In situations where the system connects to a plant's SCADA network directly from the Local Area Network (LAN) to the plant SCADA, it is advised that the plant owner/operator implements stateful routing rules for traffic between the system and SCADA application. This provides better administrative control over data traffic monitoring within the plant's domain. Consider incorporating the following security measures:

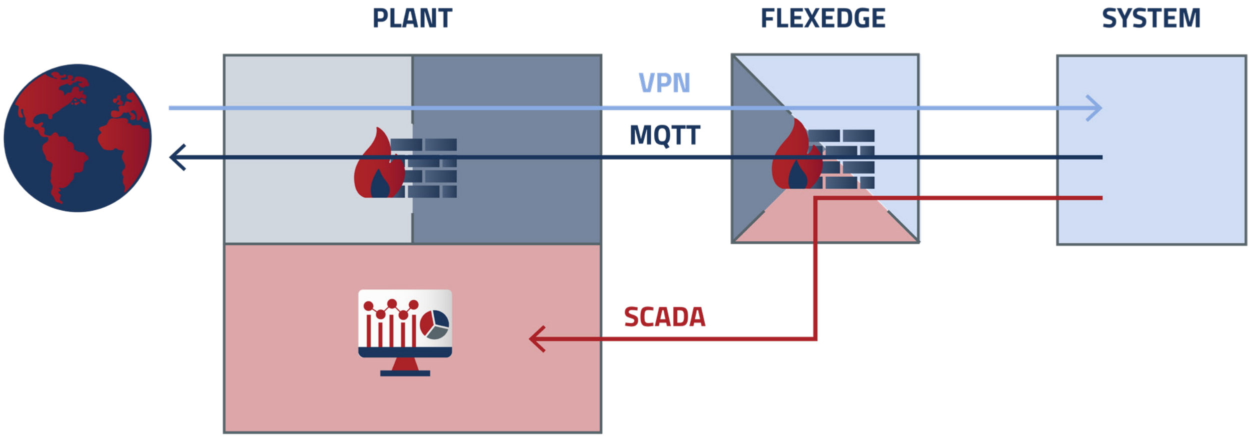
- Packet filtering - IP address, packet type, port number, etc.
- Circuit-level filtering - TCP handshake and protocol monitoring, etc.
- Stateful firewall routing – Entire session monitoring of IP addresses and payloads, etc.

Section 3: Description of Data Transmission Functional Applications

In the case of topology #1, data transmission involving the FlexEdge device, the internet, the plant, and the system can be categorized into three distinct functional applications:

A. VPN data Transmission between internet and system
B. MQTT data transmission between system and internet
C. SCADA integration protocol between system and plant

These three functional applications can be visualized as shown below:



VPN data transmission between internet and system

FlexEdge offers powerful ways to enable VPN connectivity by using the on-board I/O. For applications that would like the end user to have complete control over when remote access is available, one could use a physical swich to enable/disable VPN access to the industrial application.

MQTT data transmission between system and internet

This connection enables data transmission for the IIoT application. Selected system data tags related to performance metrics and process variables (such as flow, pressure, temperature, component status, alarm history, etc.) are extracted and sent to the MQTT broker of your choice for data analytics, reporting, and dashboard visualization. FlexEdge provides the capability to create multiple tag groups, allowing for different data transmission intervals and conditions based on your requirements.

SCADA integration protocol between system and plant

This connection facilitates data transmission for integrating the system with the plant's SCADA using IP-based communication protocols, such as OPC-UA, ModbusTCP, and ProfiNet, among others.

About Red Lion

Red Lion is focused on being THE Industrial Data Company™. We empower industrial organizations around the world to unlock the value of data by developing and manufacturing innovative products and solutions to access, connect and visualize their information. Red Lion's global manufacturing and support facilities serve customers in factory automation, alternative energy, oil and gas, power and utilities, transportation, water and wastewater industry segments. We provide scalable solutions for cloud connectivity, edge intelligence and asset management, industrial Ethernet switches and industry leading panel meters and operator panels, to make it easy for companies to gain real-time data visibility that drives productivity.

www.redlion.net

RED LION®