

Valtoris Engineering Cheat Sheet

Air-Gapped PLC Remote Routing & VPN Setup

Document Version: 1.2

Prepared for: System Integrators & OEM Machine Builders

Supported Hardware: Valtoris VT-LTE400 Industrial 4G Gateway

1. Architecture Overview (The Air-Gapped Strategy)

To bypass factory IT firewalls securely, the VT-LTE400 acts as an independent cellular gateway. It connects out to an OpenVPN/IPsec server, creating a secure tunnel back to your engineering PC. The customer's internal IT network remains completely untouched.

2. Router VPN Client Configuration (VT-LTE400)

1. Insert the 4G SIM card and power on the VT-LTE400.
2. Log into the Web GUI (Default IP: **192.168.1.1**).
3. Navigate to **VPN -> OpenVPN Client**.
4. Upload your **.ovpn** configuration profile provided by your VPN server.
5. Ensure **"NAT"** is enabled on the VPN tunnel interface so traffic can route back from the PLC.

3. Critical: PLC Default Gateway Configuration

The most common mistake engineers make is forgetting to point the PLC's gateway to the router.

For the PLC to reply to your remote TIA Portal / Studio 5000 requests, its Default Gateway **MUST** match the VT-LTE400's LAN IP address.

- **VT-LTE400 LAN IP:** **192.168.1.1**
- **PLC IP Address:** **192.168.1.10**
- **PLC Subnet Mask:** **255.255.255.0**
- **PLC Default Gateway:** **192.168.1.1** (CRITICAL)

4. Port Forwarding Cheat Sheet

If you are using Port Forwarding (DNAT) over a static IP cellular network instead of a full VPN tunnel, you must map the external WAN ports to the internal PLC IP address. Go to **Network -> Firewall -> Port Forwards** and apply the following rules based on your PLC brand:

PLC / Device Brand	Protocol	External Port	Internal IP (Example)	Internal Port
Siemens S7 (TIA Portal)	TCP	102	192.168.1.10	102
Allen-Bradley (Studio 5000)	TCP/UDP	44818	192.168.1.11	44818
Allen-Bradley (Implicit)	UDP	2222	192.168.1.11	2222
Modbus TCP (Universal)	TCP	502	192.168.1.12	502
HMI VNC Viewer	TCP	5900	192.168.1.15	5900

5. Best Practices to Prevent "Bricking"

- **Ping Test First:** Always run a continuous ping command (`ping 192.168.1.10 -t`) to the PLC for at least 5 minutes before attempting a logic download. Ensure packet loss is 0%.
- **Use Hardware Key Switch:** For maximum safety, wire a physical key switch on the cabinet door to a Digital Input (DI) on the Valtoris 4CH-IO-ETH module. Configure the router to only enable the VPN connection when the DI is triggered by the on-site operator.

LEGAL DISCLAIMER & LIABILITY LIMITATION

USE AT YOUR OWN RISK. This document is provided for informational and educational purposes only. Valtoris provides this routing cheat sheet "as is" without warranty of any kind, either expressed or implied.

By utilizing the configurations outlined in this guide, you acknowledge and agree that:

1. **Network Security:** Establishing remote access to industrial control systems (ICS) inherently carries cybersecurity risks. It is the sole responsibility of the user/system integrator to ensure that proper security measures, including but not limited to strong passwords, encryption, and strict access controls, are implemented.
2. **Machine Safety:** Remote modification of PLC logic or HMI parameters can cause unexpected machine movements. Always ensure the physical area around the machine is clear and that on-site personnel are notified before initiating any remote downloads or control commands.
3. **Liability:** Under no circumstances shall Valtoris, its affiliates, or its employees be held liable for any direct, indirect, incidental, consequential, or special damages—including but not limited to loss of production, equipment damage, data breaches, or injury—arising out of or in connection with the use or inability to use the configurations described herein.

Copyright © 2026 Valtoris. All rights reserved. Do not distribute without permission.

VALTORIS
CONFIDENTIAL