Providing Read-Only Modbus Protection

System and plant engineers are facing greater challenges every day. Two of the greatest challenges are providing increased access to device level data and the ever increasing need for security. These two challenges are compounded because as access to data increases, so do the security risks.

So, how does one solve these two conflicting challenges? Secure networks are a good solution for tightly controlled installations. But what if your installation can no longer be tightly controlled? What if your IT department now requires data for their new SCADA system? What if a government agency wants to monitor the installation? And what if you have no direct control over those monitoring systems and cannot prevent those systems from attempting to change device level configurations or set-points? Then what?

In order to provide the required data and prevent unauthorized changes, Comtrol has added the ability to enforce Read-Only serial ports on its Modbus Router firmware. This Disable Writes (Read Only) option affectively creates Read-Only devices by rejecting all standard Modbus write messages. This allows monitoring systems to retrieve the required data and prevents changes by blocking all write messages from being transmitted to the serial devices. Write violations are also logged to help locate the source of the write messages.

With an extensive set of connectivity options and the Read-Only Modbus message option, the Modbus Router firmware application provides the connectivity and security options required for today's challenging installations.

MADE IN USA

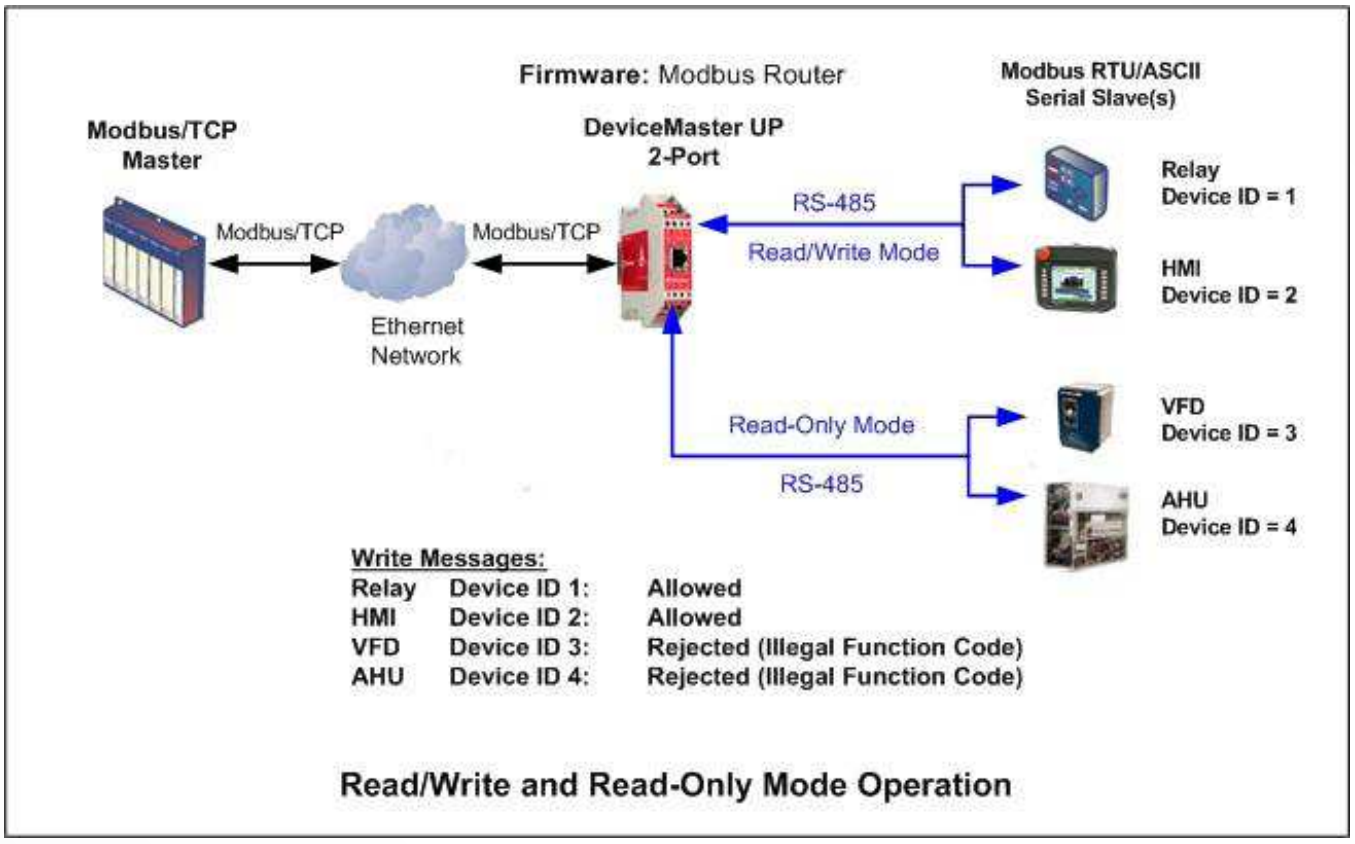
COMTROL®

Call or email for more information: 1.800.926.6876 | 763.957.6000 | IADSales@comtrol.com

1. Implementing the Disable Writes (Read Only) Option

The Disable Writes (Read Only) option has been developed to block all standard Modbus write messages from being transmitted out a serial port. An entire gateway can be configured to be Read-Only by selecting this option on all of its serial ports.

The Read-Only mode as compared to standard Read/Write mode is demonstrated in the following diagram:



Read/Write and Read-Only Mode Operation

A. Web Page Configuration

The Disable Writes (Read Only) option is enabled using the serial port configuration page:

B. Write Violation Log Web Page

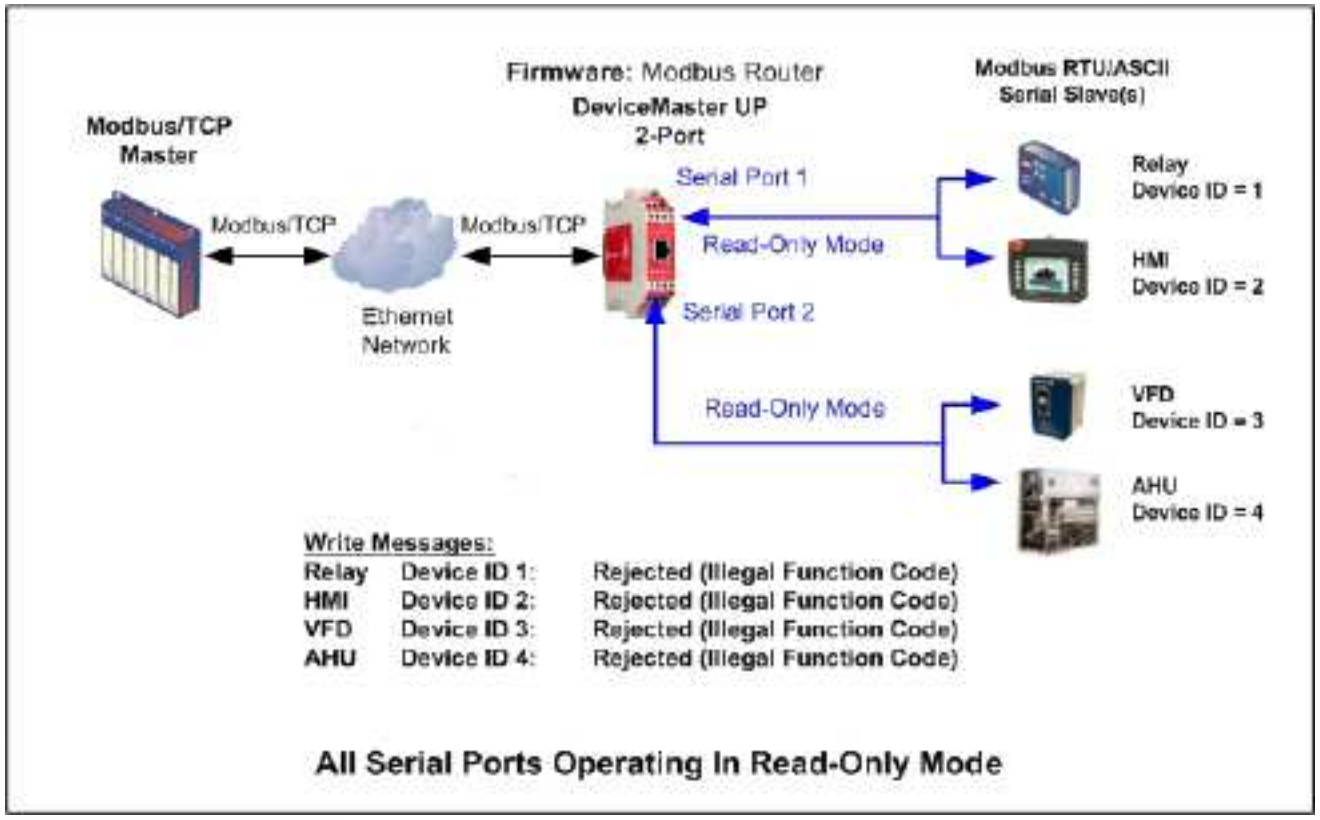
A write violation log is provided to help locate the source of rejected write messages:

2. Solutions for Read-Only Modbus Devices

A. Providing Access to Read-Only Modbus Devices

Problem: A Modbus master needs to communicate to read-only devices and it is desired to block all write messages.

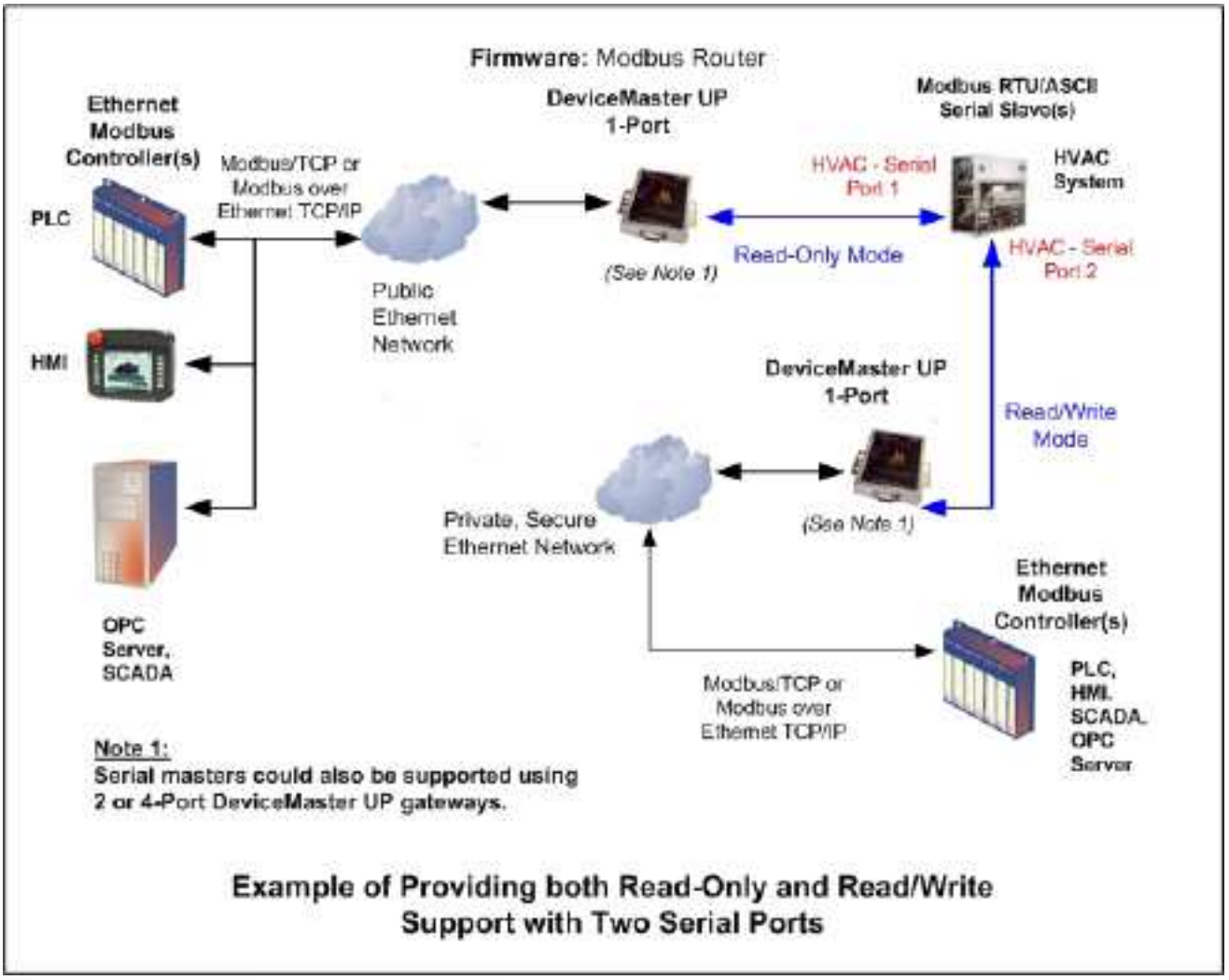
Solution: Enable *the Disable Write (Read Only)* option for all serial ports on the DeviceMaster UP.



B. Accessing Read-Only and Read/Write Devices that have Two Serial Ports

Problem: Read-Only access is required for a public network and Read/Write is required for a private, secured network.

Solution: Use two DeviceMaster UP gateways, one connected to each device serial port, to provide the desired connectivity. The Read-Only gateway is connected to the public network and the read/write gateway is connected to the private, secure network.

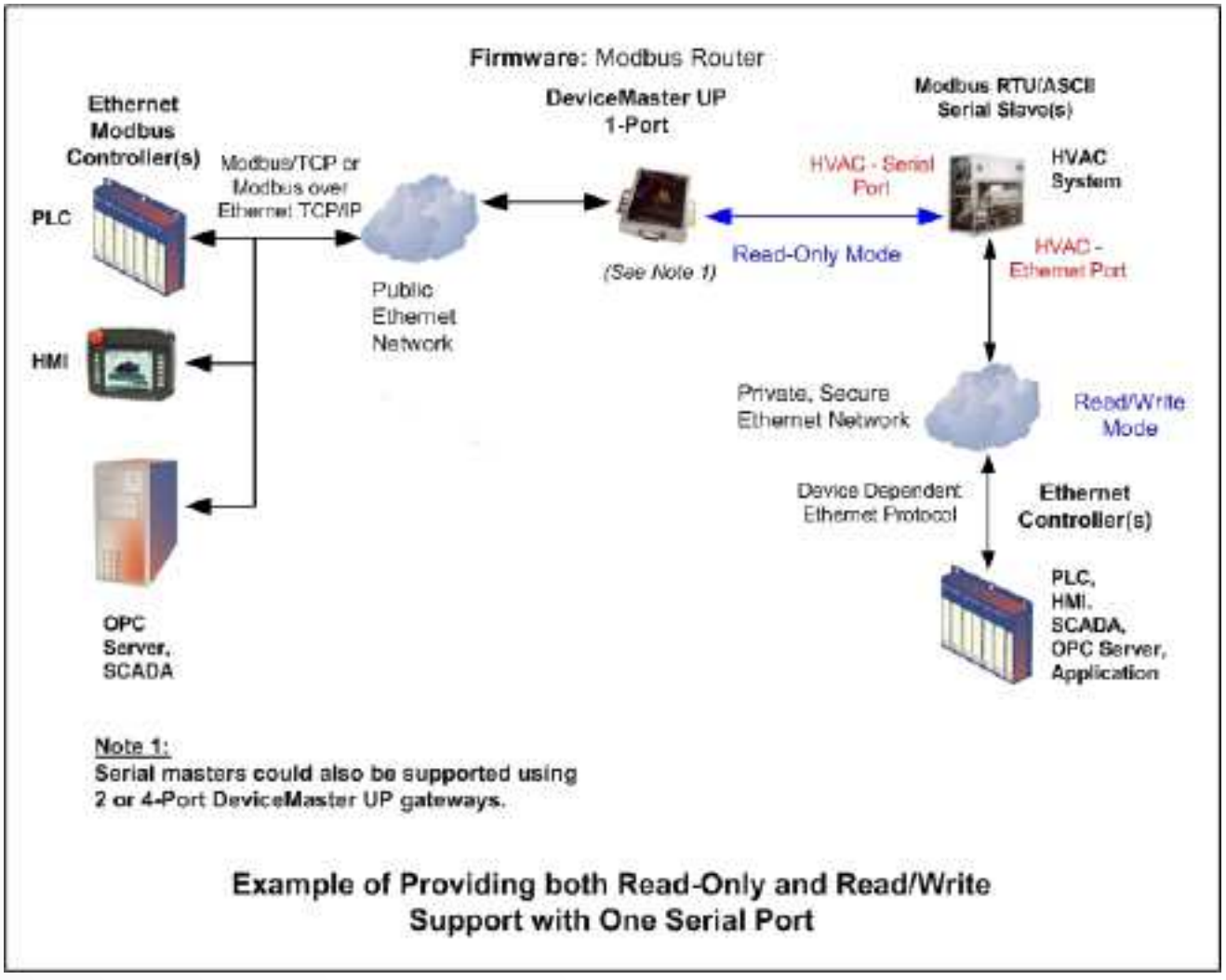


Example of Providing both Read-Only and Read/Write Support with Two Serial Ports

C. Accessing Read-Only and Read/Write Devices that have One Serial Port and One Ethernet Port

Problem: Read-Only access is required for a public network and Read/Write is required for a private, secured network.

Solution: Connect the Ethernet port to the private, secured network. Connect a DeviceMaster UP gateway to the device's serial Modbus port. The gateway is then connected to the public Ethernet network.



Example of Providing both Read-Only and Read/Write Support with One Serial Port