
Data Communications Reference

EnviroRanger ERS 500 Modbus Port Security

Objective: To prevent unauthorized Modbus port communication with an EnviroRanger ERS 500.

Equipment:

- EnviroRanger ERS 500 Level Controller (software revision 5.01 or greater)
- EnviroRanger ERS 500 Infra-red hand programmer
- IBM PC compatible computer equipped with Dolphin Plus or Modbus communication software

While every effort was made to verify the following information, no warranty of accuracy or usability is expressed or implied.

Overview

The EnviroRanger ERS 500 enables parameter access via the RS-485 serial communications port. This may be accomplished using an IBM compatible PC with communications software and a dial-up modem. This type of data communications system facilitates remote process monitoring and optimization capabilities via the EnviroRanger ERS 500.

However, these capabilities may enable unauthorized ERS 500 access and configuration modification, which could result in a process problem. This guide details security measures that may be implemented to help avoid unauthorized ERS 500 access or alteration by these methods. (Implementing these measures does not guarantee unauthorized access prevention.)

Note: This guide does not apply to SmartLinx bus protocol modules, as access security is governed by the general communications network security implemented. Note that the SmartLinx modem is not compatible with the ERS 500.

Modbus Port Security Parameters:

These parameters are only available in EnviroRanger ERS 500 software revision 5.01 and greater. Consult your Siemens Milltronics equipment supplier if you have a previous software revision installed.

- P766 Port Lock
Enables communication port security for the selected port index number.
Values: 0 = disabled (factory setting), 1 = enabled
- P767 Port Access Code
User defined 4-digit access code. The access code may be modified by keypad or by remote access upon successful log-in.
Values: 0000 to 9999
- P768 Code Error Count
Reports the number of unsuccessful access attempts using the wrong access code.
Values: 0000 to 9999

MILLTRONICS

P769 Port Lock Status

Reports the current state of access security for the communications port. When the port is unlocked, full access is permitted. When “access code required” is active, parameter access is only granted after the Port Access Code (P767) value is written to Modbus register 400061. If the incorrect code is written to this register three times, the communications session is terminated. Upon three successive terminations the total lock function is activated, and port access is not possible until the Port Access Code is manually re-entered or changed via the hand programmer.

0 = unlocked

1 = access code required

2 = total lock

Application Example:

Implementing Modbus Port Security

For this example, an EnviroRanger ERS 500 is used to monitor a remote lift station in a wastewater collection system. The ERS 500 is connected to a local phone line via a dial-up modem, so that station operating data can be monitored from the sewage treatment plant. Note that this is only one example of where Modbus Port Security may be desired.

To minimize the risk of unauthorized EnviroRanger ERS 500 access, implement the following security measures.

Modbus Port Security Measures

1. Enable the Port Lock function (P766 = 1).
2. Enter a Port Access Code of up to four numeric digits (e.g. P767 = 1234).
3. Restrict Port Access Code distribution to authorized personnel only.
4. Occasionally check for unauthorized port access attempts (P767). (If repeated access attempts occur, or if the Total Lock Port Lock Status (P769 = 2) is ever set, consider changing the dial-up modem access number.)
5. Always reset Code Error Count (P767) to “0” if you accidentally enter the wrong code.
6. If unauthorized ERS 500 access is ever detected, change the Port Access Code (P767).

General Location Security Measures

1. Restrict physical access by mounting the ERS 500 in a secure enclosure or building.
2. Install an intruder detection and alarm system on the enclosure or at the facility.
3. Store all Milltronics brand hand programmers in a locked cabinet.
4. Use password security measures for any PC with Dolphin Plus configuration software installed.
5. Use general network security measures for any data bus connected to the ERS 500 via a SmartLinX card.