White Paper

MICRO MOTION 5700 TRANSMITTER SECURITY FEATURES AND BEST PRACTICES

BY JASON LEAPLEY, MICRO MOTION, INC.

EMERSON
Process Management

Introduction

The model 5700 transmitter from Micro Motion contains a host of powerful features to deliver simple installation, commissioning, and ease of use. Advanced diagnostics and tools deliver measurement confidence, and robust logging capabilities enable greater process insight.

As process instrumentation grows more powerful and connectivity options grow in sophistication, security is a topic that is worth examining to understand the options and features available and how they impact well designed processes.

This white paper will outline the various methods of security and access control in the 5700 transmitter; such as write protect options and password protection, as well as address the new technology introduced such as data logging and file transfer using USB methodology to highlight the secure nature and best practices.

Protection and Access Control - Security Switch

One of the methods of securing the transmitter and your process is in the form of the write protect switch. This switch is located on the front display of the 5700 transmitter, underneath the display cover.

Figure 1. Security Switch Location

When enabled by moving the bottom switch to the right, towards the Lock icon, this puts the transmitter in secure, or “read only” mode. While this mode is active, operators and personnel can access all the outgoing information from the transmitter (E.G.: process variables, diagnostics, alerts, Smart Meter Verification functions, and resetting totals). However, no configuration changes or other activity can be performed that would change how the transmitter operates.

This method protects changes from the local display as well as any hosts or connection through the I/O.

For additional protection and to prevent unauthorized access to the switch, the terminal covers can be secured using a wire tie and applicable sealing mechanism. This also provides the level of security and confidence needed in accordance with Custody Transfer standards.

Figure 2. Sealing and Lockout Mechanism

Password Protection

A different method of security and access control for the 5700 is the password protection feature. This methodology is similar to the security switch, but allows authorized personnel to perform changes to configuration or other needed tasks by entering a password rather than needing to physically unseal the transmitter and/or open the display compartment to reach the switch, which could be problematic in hazardous area installations.

The password protect feature can be initialized through the local display of the 5700, and puts the transmitter into a “read only” mode similar to the physical switch, in which operators and users can view information and perform diagnostics but not change the way the meter operates. This method protects from changes made to the LOI, but does not authenticate for remote Modbus or HART access.

Additionally, it also puts the 5700 transmitter into a mode where files and data cannot be loaded or saved to or

from a USB drive via the Universal Service Port unless the password is entered (more details on the USP below).

Universal Service Port Functionality

One of the advantages of the 5700 is the design of the new Universal Service Port. This service port is based on USB technology, rather than RS-485 connections as in previous transmitters.

Figure 3. Universal Service Port

This allows for a lot of advantages and new functionality. Access to the service port is now accomplished through commonly available, low cost hardware such as a Type A to Type A USB cable for connection via the ProLink service tool. Rather than costly and difficult to find RS-485 converter modems

Additionally, this allows for files and data to be transferred onto and off of the 5700 transmitter using a USB "Thumb" drive. There are some exceptions to the type of drive able to be used which are outlined the next section.

USB Drive Compatibility

The 5700 transmitter is designed to operate with a wide variety of commercially available USB drives. The maximum capacity of information stored in the 5700 is 4 GB. However, most data files used for troubleshooting or normal operation are around 5 MB or less, so a particularly large drive is not needed.

The 5700 does not have a traditional "operating system". Interaction with USB drives is limited to basic file transferring. While this methodology provides a robust security and anti-virus approach, it is worth noting that USB drives that require specific auto run functionality, or specific drivers will not work with the 5700. This includes USB "backup" type hard drives as well as advanced USB thumb drives with built in encryption software that requires decoding from the device.

Figure 4. Variety of USB drives tested with 5700

Virus and Malware Concerns

Virus concerns and Malware are an important topic when discussing USB technology. At a fundamental level these are programs or scripts containing malicious code that, when initialized, perform unwanted routines or actions in a device. This can become problematic in three ways with many PCs and devices:

1. Most PCs and devices contain some type of "autorun" feature which automatically performs certain actions and programs when a USB drive is detected.
2. If an executable file is transferred from the USB drive (like a software installation program) and run on the host device, the executable file could have been tampered with and malicious code inserted which is run when the original program is executed (These are commonly called "Trojan" viruses).
3. There is also a special kind of USB virus that doesn't inhabit the file system of a USB stick – instead the virus is embedded in the USB-stick controller (a small computer on every USB stick that communicates with the host and handles the files). This unique virus spreads because many hosts support an automatic USB-stick controller SW upgrade mechanism which essentially causes the host to execute the virus hidden in the USB-stick controller.

It is important to note that, in every case, this program or script must be executed by the host device to perform its functionality.

This leads to the unique attribute of the 5700 transmitter that allows it to be invulnerable to these security concerns. The 5700 uses the USB for data file storage and transfer only, not programs or scripts. It can export historian data, diagnostic data, configuration files etc.; or, it can import configuration files or hex files for upgrade purposes.

The 5700 software is highly specialized. Unlike most commercial hosts (PCs, phones, tablets), the 5700 has no capability to execute a program, or run a script file, from the USB stick. Any virus on a USB stick will be completely ignored. The 5700 also does not support the mechanism that the special USB "embedded-in-the-stick-controller" virus uses.

While this approach to file transfer and use within the 5700 transmitter renders it invulnerable to virus attacks, it is worth noting that any viruses present on the USB drive could still affect other devices the USB drive is used with, such as PCs. Micro Motion recommends that these devices have up to date anti-virus software.

If USB access as a whole is not permitted throughout your facility, the USB functionality of the 5700 can be disabled through a lock out protection feature, or third party USB port hardware locks can be used.

Conclusion and Best Practices

With advances in technology and process automation, security and the ability to control unwanted changes are an important topic.

The Micro Motion model 5700 transmitter contains several different features and attributes to address any concerns. The hardware lockout and password protection feature can be used to prevent unauthorized configuration changes, while the unique nature of how the 5700 utilizes the USB-based Universal Service Port prevents infiltration and use of viruses.

Micro Motion recommends the following best practices to provide confidence in your measurement and the device integrity:

- Institute or follow your existing facility guidelines regarding access to, and performing changes to, your instrumentation configuration and operation.
- The password protection feature of the 5700 can be a valuable asset to maintaining these controls.
- In situations where more stringent access control is desirable, or regulatory or custody transfer standards require it, the physical security switch and lockout capability provide a thorough restriction mechanism.
- While the 5700 is not vulnerable to USB drive based viruses and malware, other devices or computers could be. It is recommended to utilize anti-virus software or other means of protection on these devices.

About Micro Motion

For over 35 years, Emerson's Micro Motion has been a technology leader delivering the most precise flow, density and concentration measurement devices for fiscal applications, process control and process monitoring. Our passion for solving flow and density measurement challenges is proven through the highly accurate and unbeatable performance of our devices.

Emerson Process Management
Micro Motion
7070 Winchester Circle
Boulder, Colorado USA 80301
T: +1 800 522 6277
T: +1 (303) 527 5200
F: +1 (303) 530 8459
www.MicroMotion.com

WP-001988 Rev A

EMERSON™
Process Management