Technical Bulletin,
Using the Audit Trail
(Event Logger) Feature
and Sealing of the
Flow Computer

NOTE: User Manual Reference - This Technical Bulletin complements the information contained in Volumes 2 & 3 of the User Manual, applicable to all firmware revisions.

Table of Contents

Figures

Scope

All firmware revisions of OMNI 6000/OMNI 3000 Flow Computers have an Audit Trail feature. This Technical Bulletin explains how to use the Audit Trail feature and other Security features designed to prevent unauthorized access. The information contained in this Technical Bulletin are for intermediate users.

Abstract

All OMNI Flow Computer firmware revisions include an "Audit Trail" feature. In current revisions, this security feature consists of an archive file that stores 150 records of the most recent changes made to the flow computer database. The flow computer always logs changes made to the database via the OMNI front panel keypad. It can also log changes made remotely via a Modbus port, using OMNICOM® PC Configuration Software for instance, if passwords have been activated on the serial port. Each record consists of a unique event number, time and date tag, the database index number of the affected variable, and the new and old value of that variable. The value of gross and net totals at the moment of the event are also stored in the record. Furthermore, the firmware can log events that involve a group of consecutive database addresses. In this case, only the starting index number and the number of consecutive index points appear in the audit trail. The records comprise the Audit Trail Report which, when printed, lists the latest 150 records in time sequence starting with the most recent. You can view this report in OMNICOM and print it either with OMNICOM or the front panel keypad. The Audit Trail Report has a fixed format and is not customizable by the user.

Activating the Audit Trail Feature

The OMNI Flow Computer will automatically log all changes made to the configuration settings via the front panel keypad. However, to avoid flushing the audit trail, the firmware does not log configuration changes made via serial ports other than complete download events, unless rigorous auditing is enabled. In order for the flow computer to log configuration changes made through a serial port, whether remotely (via modem) or via direct connection, the corresponding serial port must be password protected or enabled for rigorous auditing. With passwords activated, the firmware will fully log the target database address' old and new value only when single point writes occur. When blocks of data are written, only the starting database index and total number of consecutive points written to will be recorded in the audit trail log. Enabling rigorous auditing does not require serial port passwords to be used. The flow computer will archive all serial port transactions that represent configuration changes.

Password Protecting Serial Port Access

The flow computer will automatically log any single point writes to a specific database address made via a password protected serial port. Assigning serial port passwords for the first time can only be done via the front panel keypad of the flow computer.

To assign passwords and restrict access to serial ports via the OMNI front panel keypad, proceed as follows:

NOTE: Entering a Serial Port Password – Initially, you can only assign serial port passwords via the OMNI front panel keypad. Choose up to eight (8) alphanumeric characters for the password. Enter the selected password at the corresponding serial port enter under the 'Password Maintenance' submenu:

- **'Ser1 Passwrd'** for Serial Port #1
- 'Ser2 Passwrd' for Serial Port #2
- 'Ser3 Passwrd' for Serial Port #3
- 'Ser4 Passwrd' for Serial Port #4
- 'Ser5 Passwrd' for Serial Port #5
- 'Ser6 Passwrd' for Serial Port #6

If Serial Port #1 has a printer connected to it, you need not assign a password to this port. Ports #3, #4, #5, and #6 are available only if your flow computer has three (3) serial I/O modules installed. Firmware .73 and higher in all revisions allow for a third serial card.

- Using the flow computer's front panel keypad and in the normal display mode, press **[Prog] [Setup] [Enter] [Enter] [Enter]**. This will display the '**Password Maintenance**' submenu of the '**Miscellaneous Configuration**' menu.

```
PASSWORD
MAINTENANCE
Priveledged
_
Level 1
Level 1A
```

- Scroll down to place the cursor at the desired '**Ser*n* Passwd**' prompt and enter a password of your choice. The "***n***" in '**Ser*n***' represents the serial port number (e.g., the display shows **Ser2** for Serial Port #2 (see Note for additional information).

```
PASSWORD
MAINTENANCE
Ser1 Passwd
Lockout SW Active?
N
Ser2 Passwd _
```

- Press **[Enter]** once you have keyed-in your password for the selected serial port. The flow computer will prompt you to enter the privileged password for the flow computer to validate the new serial port password. If you have not yet assigned a privileged password, either use "**OMNI**" as the default or scroll up and assign a password now. If you do the latter, repeat the procedure for assigning the serial port password.

Once assigned, you have the option of changing the serial port passwords via the OMNICOM PC configuration software. To do this, while on any field edit screen, press **[Ctrl] [Alt] [P]** on your PC keyboard and follow the online instructions. You will need to enter the current valid password before you can change it.

Enabling Rigorous Auditing of Serial Ports

Rigorous auditing is normally used only as a diagnostic tool to track down unexpected changes made to the flow computer database. It allows you to log all transactions of one (1) or more non-password protected serial ports. Actually, the only way to log all changes to the OMNI database done through serial ports is by enabling rigorous auditing. To enable rigorous auditing you must define a user-programmable variable statement. This statement places the decimal value of the serial port's hexadecimal code into the database address the correspondence to the special diagnostic function (Index # **3800**). To enable rigorous auditing to one or more serial ports, perform the following:

- From Table 1, select the hexadecimal codes of the serial ports to which you want to apply rigorous auditing. Then determine the decimal equivalent of the selected hexadecimal codes (indicated in the table).

- Formulate a variable statement that writes the desired decimal value to Database Point # **3800** (Special Diagnostic Function) using the following logic:

   o Address 3800 is **EQUAL** (=)to the **CONSTANT** (#) decimal value

Or simply select the respective variable statement from among those provided in the Table 1.

Table 1. Variable Statements for Enabling Rigorous Auditing to Serial Ports

VARIABLE STATEMENTS FOR ENABLING RIGOROUS AUDITING TO SERIAL PORTS								
Serial Port(s) #						Hexadecimal Code	Decimal Equivalent	Variable Statement
1	2	3	4	5	6			
1						000A	10	3800=#10
	2					00A0	160	3800=#160
		3				0A00	2560	3800=#2560
			4			A000	40960	3800=#40960
				5		0005	5	3800=#5
					6	0050	80	3800=#80
1	2					00AA	170	380=#170
1		3				0A0A	2570	3800=2570
1			4			A00A	40970	3800=340970
1	2		4			A0AA	41130	380=#41130
1		3	4			AA0A	43530	3800=#43530
1	2	3				AAA0	2730	3800=#2730
1	2	3	4			AAAA	43690	3800=#43690
1		3	4		6	AA5A	43610	3800=#43610
	2	3				0AA0	2720	3800=#2720
	2		4			A0A0	41120	3800=#41120
	2			5		00A5	165	3800=#165
	2	3	4	5		AAA5	43685	3800=#43685
		3	4			AA00	43520	3800=#43520
	2	3	4			AAA0	43680	3800=#43680
	2	3				0AA0	2720	3800=#2720
		3	4	5	6	AA55	43605	3800=#43605
		3	4			AA00	43520	3800=#43520
		3	4		6	AA50	43600	3800=#43600
		3	4	5		AA05	43525	3800=#43525

- Either via OMNICOM or the front panel keypad, open the '**Program Variable**' submenu under the '**Miscellaneous Configuration**' menu, select an available (empty) variable point, and key-in the variable statement. Press **[Enter]** when done to enable the rigorous auditing feature. In OMNICOM, remember to download the variable statement to the flow computer when done if working offline.

Printing and Viewing the Audit Trail Report

You can print the Audit Trail Report from either the flow computer's front panel keypad or from OMNICOM. However, you can view this report only from OMNICOM.

NOTE: Verifying the Audit Trail Feature – To verify that the audit trail feature are rigorous auditing are active, make any necessary flow computer configuration changes and view or print the Audit Trail Report (as indicated in this Technical Bulletin). If the changes you made appear on the report, the audit trail feature is active.

Printing the Audit Trail Report via Front Panel Keypad

To print the Audit Trail Report from the flow computer's keypad, perform the following:

- In the display mode, press **[Prog] [Print] [Enter]** to display the '**Print Report Menu**'.
- Scroll down to place the cursor at the '**Audit Trail ? (Y)**' prompt and type the number '**150**', indicating the total number of records to print. It is not necessary to print all 150 records, unless you want to.
- Press **[Enter]** and the report will print.

Viewing and Printing the Audit Trail Report via OMNICOM

To print the Audit Trail Report from OMNICOM, perform the following:

- With OMNICOM running, select '**Audit Trail Report**' under the '**Report**' menu and press **[Enter]**.
- Select '**Load from OMNI**' in the popup box and press **[Enter]**. OMNICOM will prompt you for a password to continue. It will allow you to change the password if you want (for loading the Audit Trail report via OMNICOM only). In any case you will need to enter the password you assigned for rigorous auditing.
- Type the password and press **[Enter]**. OMNICOM will proceed to load the audit trail data and display the Audit Trail Report.
- If you want to print the report, press **[Alt] [P]** and follow the online instructions.
- Exit OMNICOM when completed.

Sealing the Flow Computer

In addition to the audit trail, OMNI Flow Computers provide sealing features for added security. These security features prevent access to the circuitry and tampering of configuration settings, protecting data and system integrity.

The key sealing features are:

- Download Disabling (OmniCom Lockout)
- Serial Port Lockout Switches
- Program Inhibit (Keypad Lockout) Switch
- Housing Sealing

Download Disabling (OmniCom Lockout)

NOTE: You can set the download disabling and serial port lockout switches in one session while in the 'Password Maintenance' setup. You can set these features either via the front panel keypad or by using the OMNI Panel Emulator provided in OMNICOM. The recommended order for applying the sealing features is as follows:

- Disable download to the flow computer
- Select the serial port lockout switch option
- Activate the program inhibit switch
- Physically seal the flow computer housing enclosure

OMNI Flow Computer firmware allows you to block all complete downloads from OMNICOM to the flow computer. This feature protects against accidental downloads that could occur due to incorrect logon. Once a flow computer is configured, the correct way to log on is to 'Receive' the configuration in OMNICOM.

You can set this feature only via the front panel keypad. To set the download disabling feature, proceed as follows:

- In the normal display mode, press **[Prog] [Setup] [Enter] [Enter] [Enter]** to access '**Password Maintenance**' setup.

- At the '**Privileged**' Password prompt, type-in the corresponding password and press **[Enter]**. The download disabling setting will not appear if you do not enter the privileged password.

- Scroll down to the '**Disable Download?**' prompt. The LCD screen displays as follows:

```
PASSWORD
MAINTENANCE
Lockout SW Active?
N
Model #? 0=3K, 1=6k
1
Disable Download?
N
```

- Press **[Y] [Enter]** to disable or **[N] [Enter]** to enable OMNICOM downloading of the configuration data to the OMNI Flow Computer.

If desired, you can proceed to set the serial port lockout switches while in the '**Password Maintenance**' setup. The following section describes this feature.

Serial Port Lockout Switch Enable Option

The flow computer's configuration provides a lockout switch option for each serial port. You can activate or deactivate the serial port lockout switch option only via the front panel keypad, as follows:

- In the normal display mode, press **[Prog] [Setup] [Enter] [Enter] [Enter]** to access '**Password Maintenance**' settings.

- Scroll down to the '**Lockout SW Active?**' setting that corresponds to the selected serial port. Press **[Y] [Enter]** to activate or **[N] [Enter]** to deactivate the lockout switch for each serial port to which you want to set this feature.

- Press the **[Prog]** several times to exit the Program Mode and return to the Display Mode.

Program Inhibit (Keypad Lockout) Switch

NOTE: Preventing Access to the Program Inhibit Switch – To prevent unauthorized activating or deactivating of the program inhibit switch, seal the flow computer housing as indicated in this Technical Bulletin. Activating the program inhibit switch with firmware revisions prior to .72 blocked all configuration changes. This was subsequently modified to allow configuration changes to password level 2 operational parameters such as PID setpoints, batch end commands, and prove commands.

The Program Inhibit Switch allows you to lock access to the Program and Diagnostic/Calibration Modes via the front panel keypad. This prevents configuration settings from being changed. Attempting to enter a configuration submenu will have no effect when the switch is in the inhibit position, and "PROGRAM LOCKOUT" will display on the bottom line of the LCD screen. Nonetheless, you can still enter key presses to only view data in the normal Display Mode.

Figure 1 shows the location of the program inhibit switch; which is behind the front panel. To access and activate or deactivate, do the following:

- Hold the front panel from the bottom, gently lift it upwards to disengage the latching bezel, and withdraw the flow computer a couple of inches from its housing case.

- Locate the red Program Inhibit Switch. It will be on the bottom right (when facing the front panel) behind the front panel (Figure 1**)**.

- Using your right hand (recommended), place the switch to the downward position to lock the keypad or place it to the upward position to unlock the keypad.

- Reinsert the flow computer into its housing, making sure that the bezel latches in place.

You can test the program inhibit switch by pressing the **[Prog] [Setup] [Enter]** keys on the front panel keypad. This will take you to the Setup Menu in the Program Mode. Place the cursor on any of the submenus listed and press **[Enter]**. If the "Program Lockout" message flashes on the bottom line of the LCD screen, the program inhibit switch is active

CAUTION: These units have an integral latching mechanism which you must first disengage by lifting the bezel upwards before withdrawing the unit from the case.
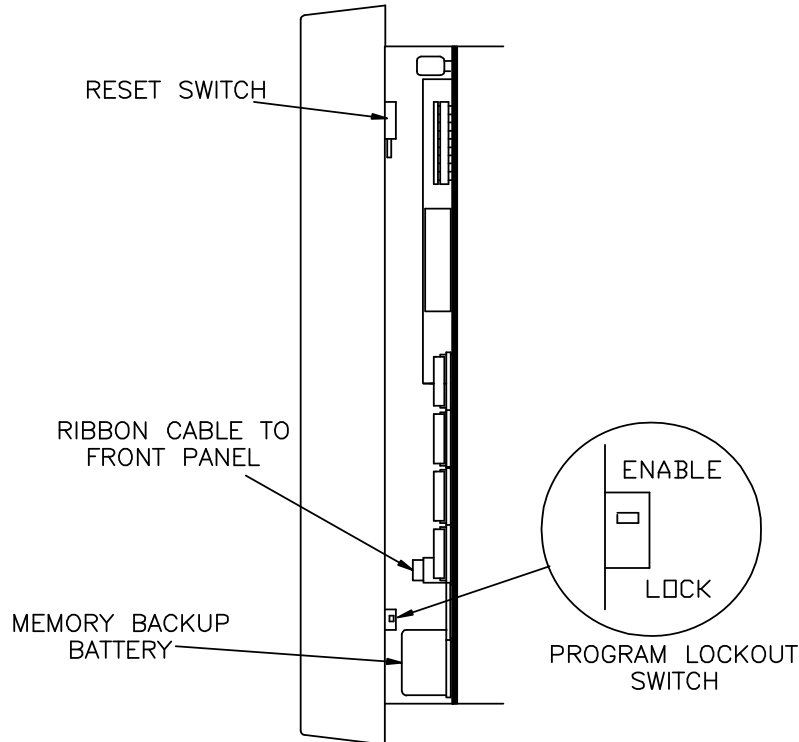

Figure 1. The Program Inhibit Switch

Housing Sealing

You can lock or seal the inner enclosure of the flow computer within the outer enclosure, blocking access to the 'Program Inhibit Switch' and to the circuitry. To seal the flow computer, insert an instrument sealing wire through the holes provided on the top-right and towards the back of the enclosures. Before placing the sealing wire, make sure that the integral latching mechanism is in place aligning the holes of both enclosures (inner and outer).

DOCUMENT REVISION HISTORY

DOCUMENT INITIAL RELEASE DATE..29-May-2003

REVISION	DATE	PURPOSE / CHANGE REQUEST
A	29-May-2003	Maintained on the Web - Initial release
B	06-March-2009	DCR 090050