Forté Series X760 System

RAID Maintenance & Recovery Procedure for
SiS Controller in Industrial PC #61-1252
January 23, 2009
P/N 85-1065

REV A

RAID Maintenance and Recovery Procedure – SiS Controller

REVISION HISTORY:

Rev. A   January 23, 2009   MCD   Initial Release

TABLE OF CONTENTS

REV A

1.0 RAID 1 ARRAY IN FORTÉ INDUSTRIAL PC #61-1252

This procedure describes how to maintain and recover a RAID 1 array as setup on a FORTÉ Industrial PC with Part #61-1252 using the SiS Controller installed on the motherboard.

The RAID Setup Utility program is accessed during the boot process of the PC by pressing the <Ctrl> and <S> keys when prompted by the display screen.

If the system detects that the RAID is broken during the boot sequence, it will stop and ask if the user wishes to repair the RAID. The repair procedure is described in the following sections below.

NOTES ON THE OPERATION OF THE RAID 1 SYSTEM:

1. The FORTÉ Industrial PC motherboard does not support hot-swapping of the hard disks. The industrial PC must be turned off to remove the hard disks. The removable hard disk enclosures should remain locked in place while the PC is turned on. Once the RAID 1 System is configured both of the hard disks must remain operating, or the RAID System will detect a broken RAID.

2. The RAID 1 array is a mirroring system and supports (2) hard disks as supplied. The hard disks should be the same make, model, and size.

3. The RAID Setting Utility recognizes two NEW hard disks as SINGLE disks and requires that a RAID1 array be created. See Note 6.

4. If only one hard disk is detected as a RAID1 disk, it is possible to re-configure the system to operate with only the one detected disk. The RAID Setup Utility program changes the detected hard disk from RAID1 to SINGLE operation. The procedure to change to SINGLE hard disk operation by using the RAID Setup Utility takes only five minutes.

5. If both hard disks are detected, but the RAID is broken, it is possible to rebuild the RAID1 array by using the RAID Setup Utility program to select a SOURCE disk to duplicate. Rebuilding the RAID1 array from the source disk can take over an hour to complete in some cases.

6. If both hard disks are detected, but the RAID is broken, it is possible to CREATE a RAID1 array by using the RAID Setup Utility program. Creating the RAID1 array requires that Windows XP and all other programs and drivers be re-installed, including the VGA and Ethernet drivers for the motherboard, Microsoft .Net 2.0, Microsoft SQL Server 2005, and the FORTÉ X760 System software and drivers. The latest Microsoft updates and Service Packs should be installed for each application, if possible. Because of the time required to install the Microsoft Service Packs and updates, three hours or more of installation time may be required. FORTÉ Technology highly recommends keeping a fully configured spare PC on hand so that it can be immediately put into service following the installation of current FORTÉ backup files.

REV A

2.0 INDICATION OF NORMAL OPERATION OF THE RAID 1 ARRAY

Indications of a properly functioning RAID1 array:

1) The FORTÉ System PC boots properly. The startup text messages during the boot process report that both hard disks are recognized as being part of a RAID1 array.
2) Windows XP opens.
3) The keyboard and mouse operate correctly.
4) FORTÉ Systems use three different types of RAID hard disks. The first type is an array of two fixed hard disks inside the PC enclosure. The second and third types are two different styles of removable hard disks, which are accessible at the front of the Industrial PC and can be removed by the use of a key switch.
5) During normal operation, the blue LCD screen on the "ICY DOCK" type of removable hard disk enclosure is active and contains disk status information.
6) During normal operation, the green (power) LED and the yellow (disk access) LED on the MILITARY type of removable hard disk enclosure is on and active.
7) The On/Off switch on the front panel of the PC operates properly..
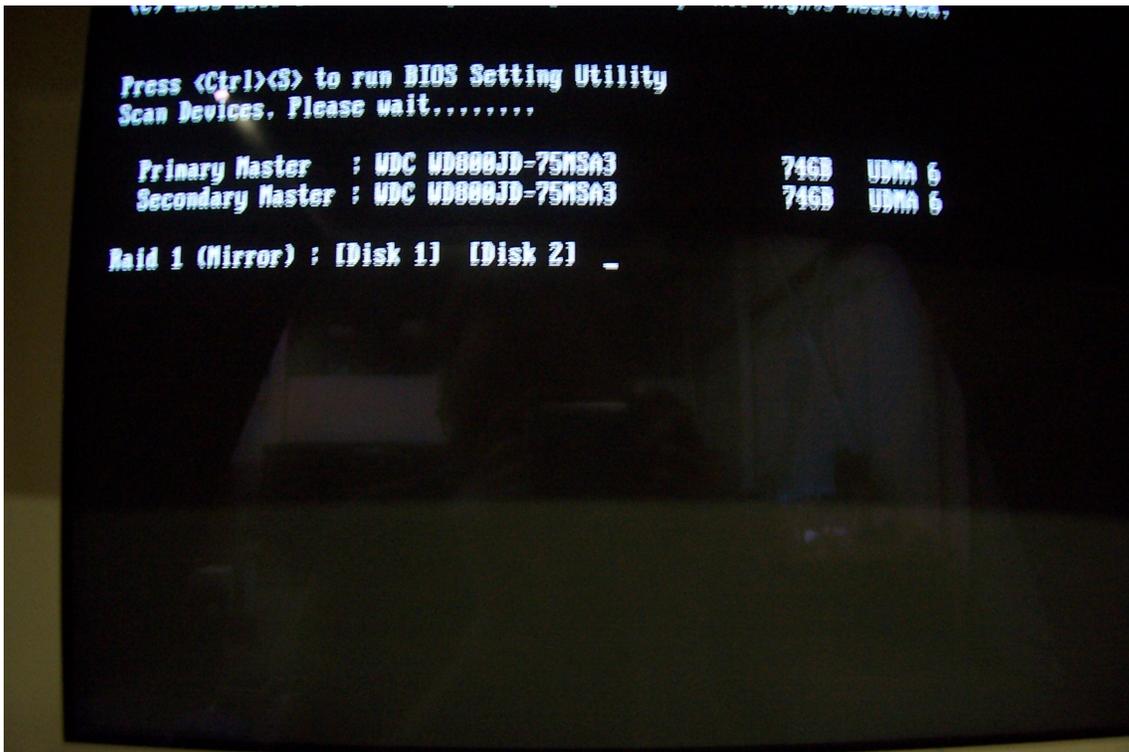
Figure 1. Screen Message for Normal Boot of RAID1 Array

REV A

3.0 INDICATIONS OF A BROKEN RAID CONDITION IN WINDOWS

If one of the two RAID1 SATA hard disks has been corrupted, or if power or data connections to one or both of the disks have been interrupted, Windows XP and the FORTÉ System software might stop functioning.

Indications of a broken RAID **during startup of the FORTÉ PC:**

1) The FORTÉ System PC stops during the boot process and reports a broken RAID or missing hard disk. Either the Primary Master (Disk 1) or the Secondary Master (Disk 2) is reported as missing.
2) The operator is prompted to press the <Y> key to enter the SiS BIOS Setting Utility.

Indications of a broken RAID **once the system is started and operating in WINDOWS XP:**

3) The keyboard and/or mouse do not function.
4) The Windows "hourglass" is shown on the screen in place of the normal pointer cursor.
5) A Windows "popup" error message box is shown on the screen, but cannot be closed by the keyboard or mouse.
6) Windows Task Manager cannot be invoked by using the <Ctrl> + <Alt> + <Delete> keys.
7) The blue LCD screen on the "ICY DOCK" type of hard disk enclosure is blank or off.
8) On the MILITARY type of hard disk enclosure there is a green (power) LED and a yellow (disk access) LED. If the chassis is unlocked or if connections to the hard disk are lost, both LEDs will be off. In some cases where the RAID is not functional the green and yellow LEDs on both disks might be on or blinking steadily.
9) The On/Off switch on the front panel of the PC does not work.
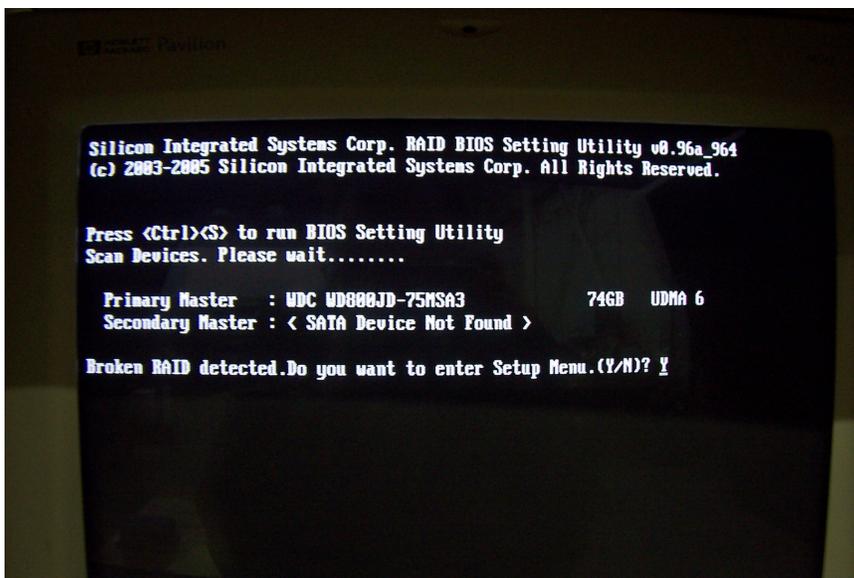
Figure 2. Broken RAID Detected During Boot Sequence

REV A

4.0 THE RAID1 ARRAY RECOVERY PROCESS

At this point, a technician should check that the two RAID1 hard disks are firmly seated in the mounting rack enclosure and that both key switches are in the LOCKED position.

#1 Style RAID hard drive carriers, "ICY DOCK"
This style RAID array will run without carriers being locked in place, but easier to break RAID and hang FORTE System operation.

FORTE Industrial PC RAID HDDs

#2, RAID hard disk carriers, "Military Style"
Shown with key switch in "LOCK" position.
Drive is active only in "LOCK" position.
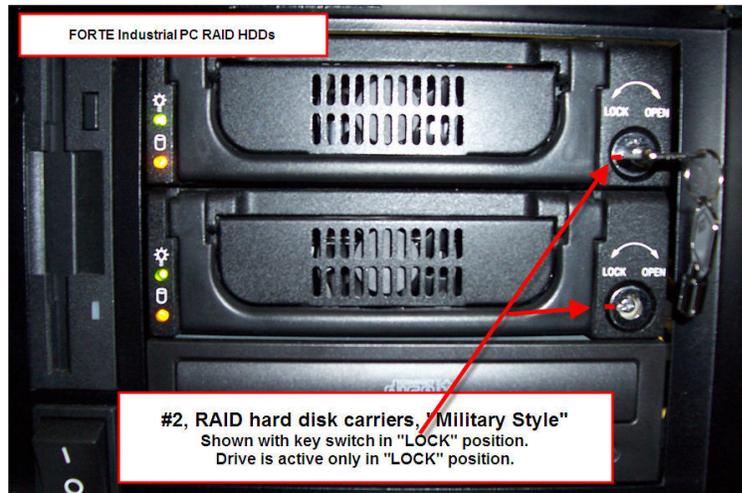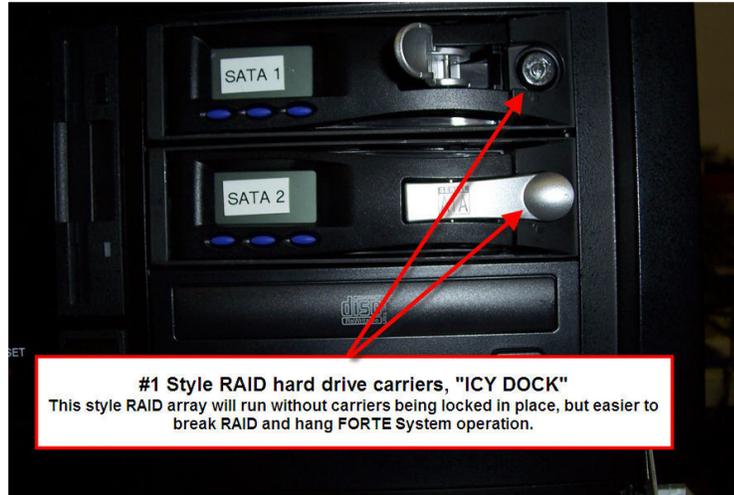
The technician should also remove the top cover of the PC and check that the power cables and red SATA data cables are securely connected to the back panels of the hard disk enclosures.

The technician should then re-boot the and check system operation.

If the system again stops at the SiS BIOS Setting Utility, perform the following steps to recover from the broken RAID1 array by operating the system on a single hard disk.

REV A

4.1 REBOOTING THE FORTÉ COMPUTER

If the FORTÉ Windows System has crashed during normal operation, re-boot the computer to begin the RAID recovery process.

If the front panel On/Off switch on the Industrial PC will not function, turn off the main On/Off switches on the two redundant power supply modules located on the back panel of the Industrial PC. Both power cables can also be removed. All three (3) green LEDs will turn off.

Turn on the two redundant power supply modules, and then press the front panel On/Off switch to re-boot the PC.
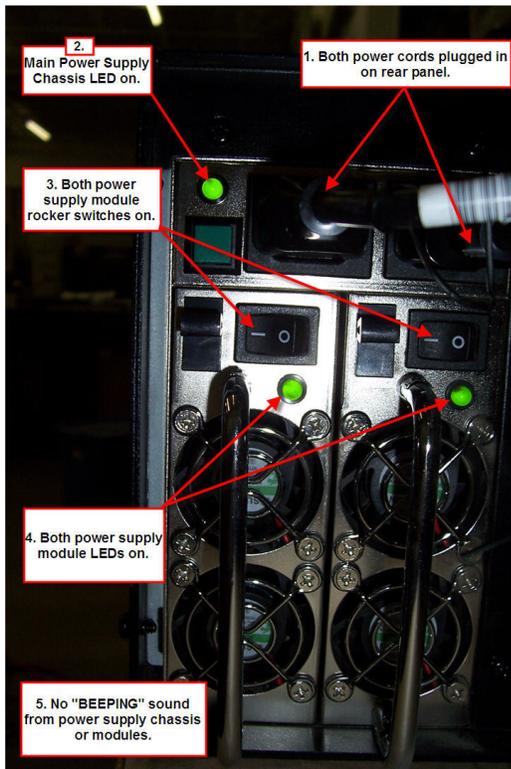
Figure 3. Rocker Switches on Power Modules

4.2 ENTER THE SiS RAID BIOS SETTING UTILITY

Press the <ENTER> key when prompted to enter the BIOS Setting Utility to recover from the broken RAID1 (Mirror) Array. In this case, the Secondary Master Hard Disk was not detected, likely due to a poor SATA data cable or power cable connection.

Figure 4. Enter the BIOS Setting Utility

4.3 RAID BIOS SETTING UTILITY – NORMAL DISPLAY

No maintenance is required from the SiS BIOS Setting Utility screen for a **normal** RAID1 array. Press the <Q> key to exit.
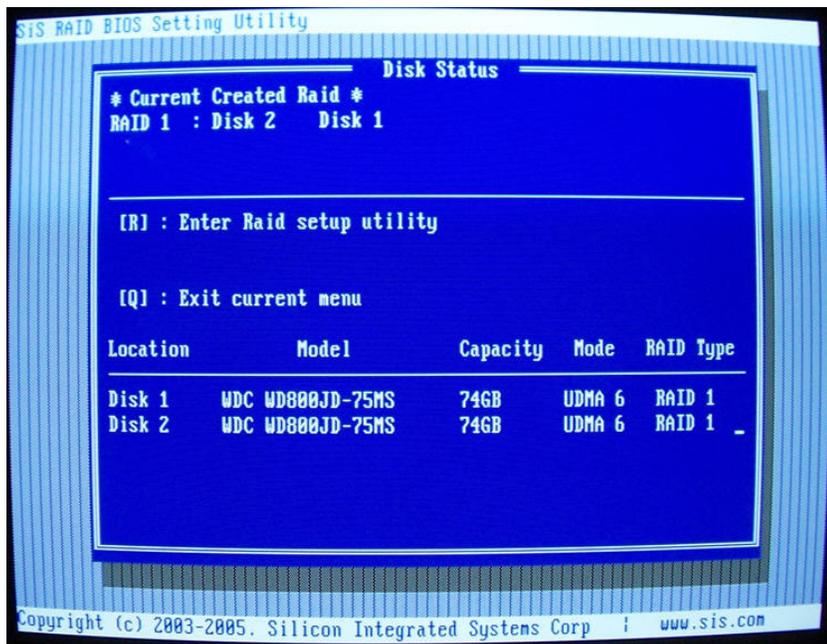
Figure 5. Normal Utility Display

4.4 RAID BIOS SETTING UTILITY – ONE DISK DETECTED

If a problem is detected during the boot sequence similar to FIGURE 2, the display for the SiS BIOS Setting Utility will look similar to the following screen:
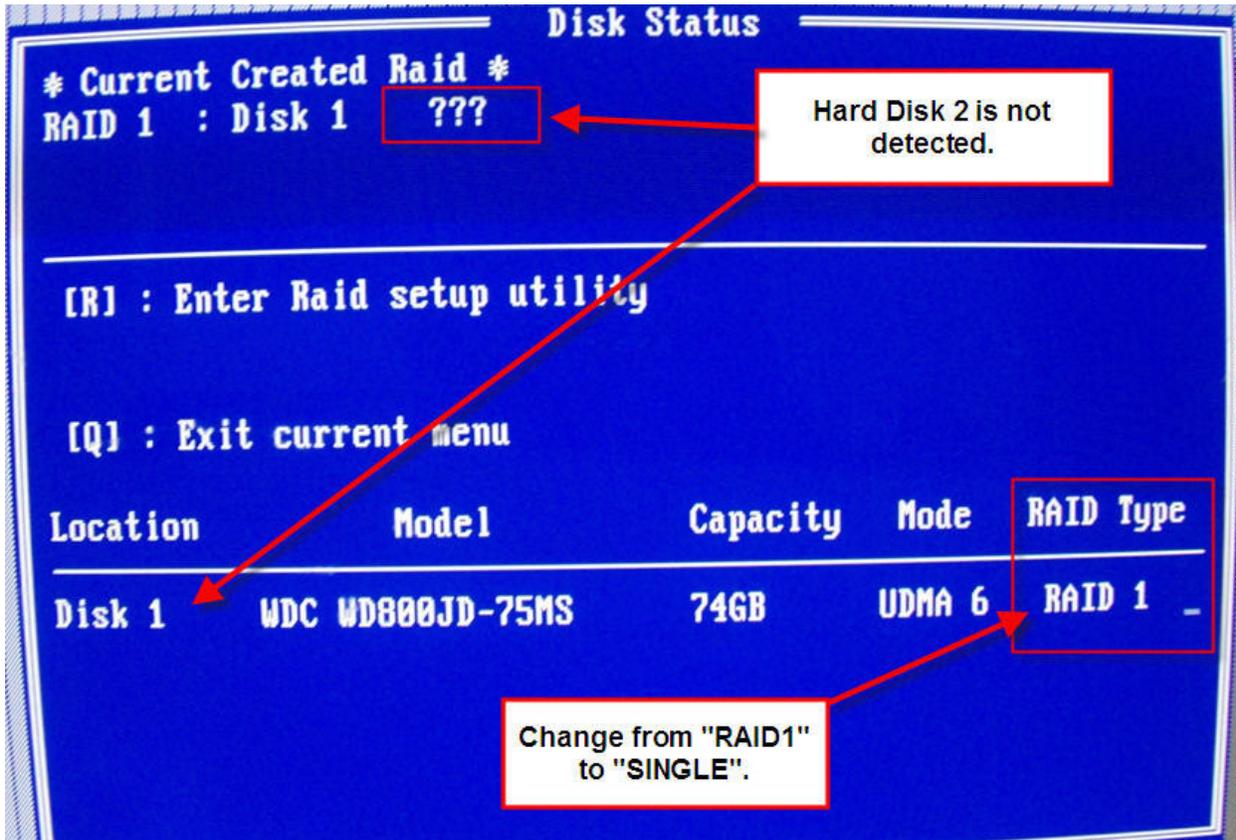
Figure 6. Disk 2 of RAID1 is not Detected

The FORTÉ System PC will not run if only one hard disk is recognized in the RAID1 array. In order to run the FORTÉ System the RAID TYPE for the recognized hard disk (Disk 1) must be changed from "RAID1" to "SINGLE".

Press the <R> key to enter the RAID Setup Utility.

4.5 DELETE THE RAID1 ARRAY – CHANGE TO SINGLE DISK OPERATION

The <R> key opens the following display screen:
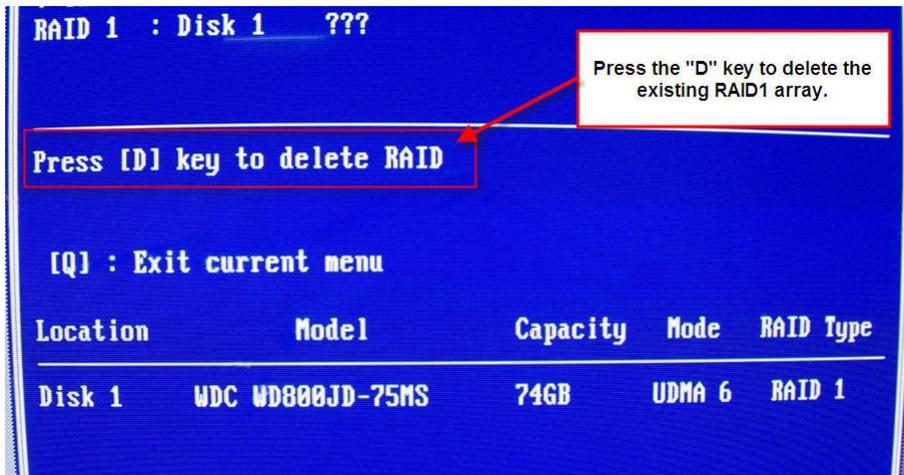
Press the <D> key to delete the existing RAID1 array and set the recognized hard disk to SINGLE operation. This will allow the PC to complete the boot sequence and open Windows XP.

NOTE : In this example, deleting the RAID1 array does not delete the contents of the hard disk. Deleting RAID only sets the disk to SINGLE operation.

Press the <ENTER> key to delete the RAID1 array.
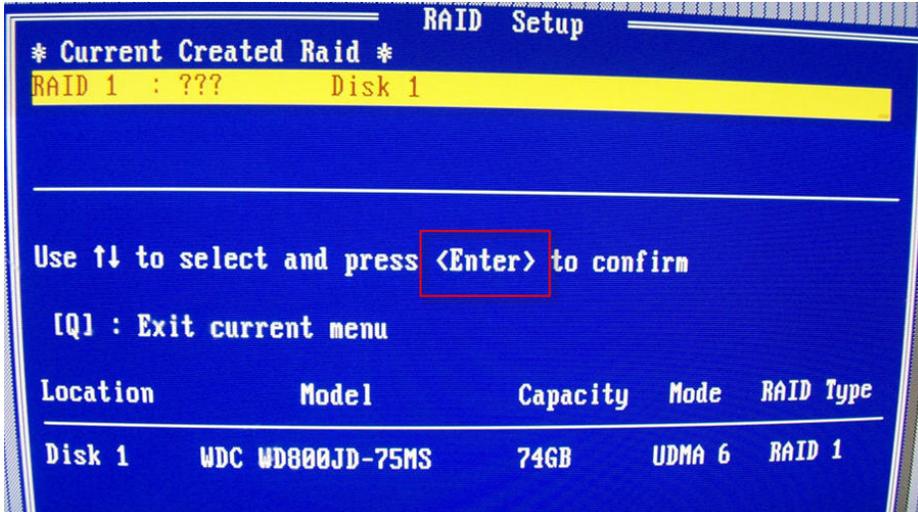
There are not enough disks recognized to recover the RAID1 array.

The RAID Type is set to SINGLE.
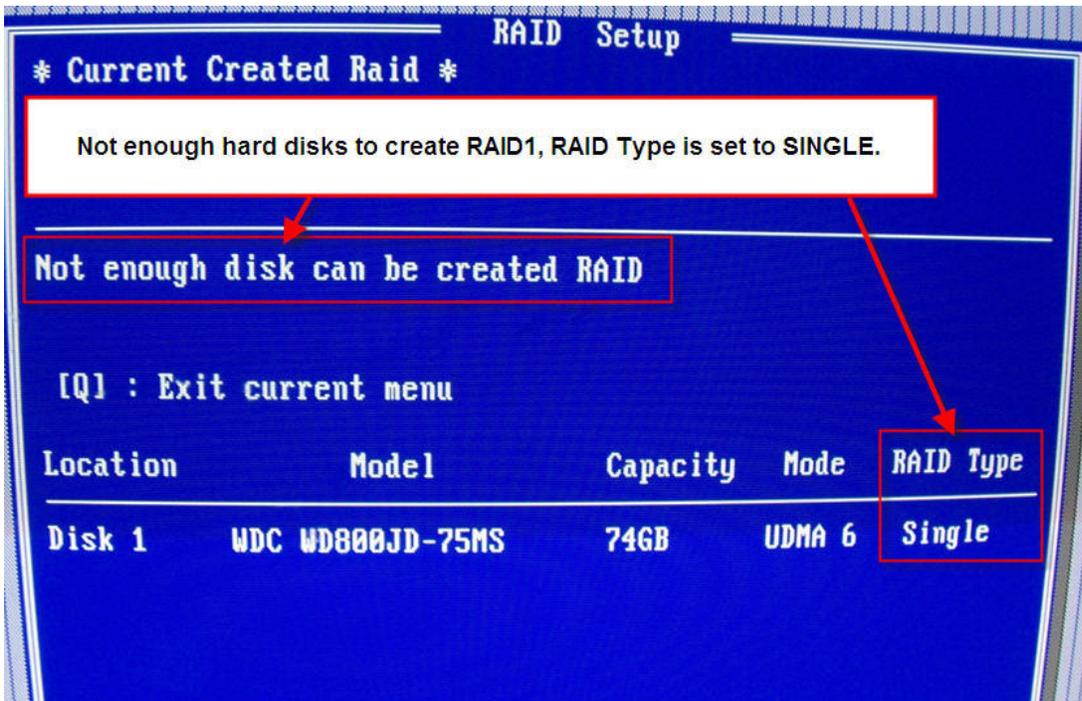
Press the <Q> key.
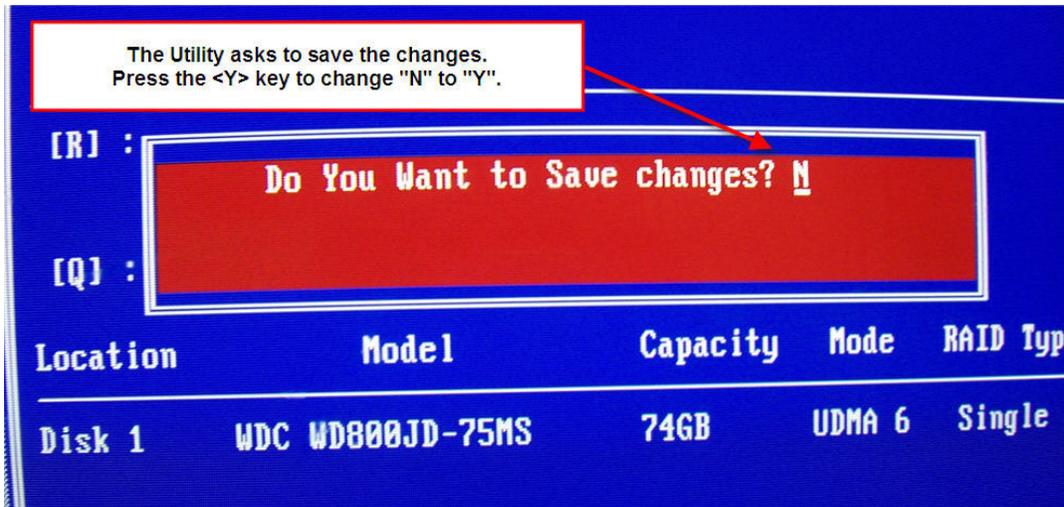
Press the <Y> key to change the "N" (No) to "Y" (Yes).
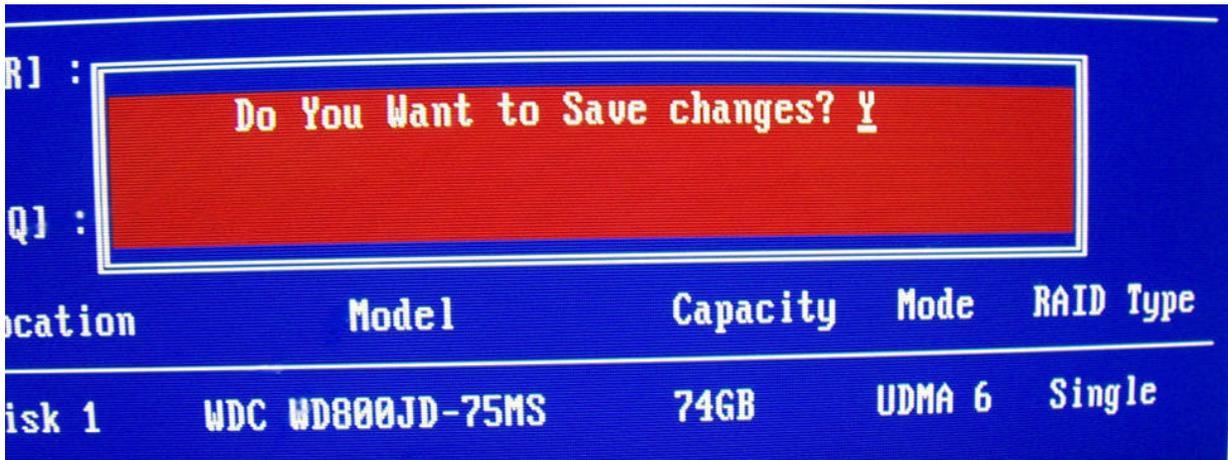
Press the <ENTER> key on the keyboard to confirm the change to SINGLE disk operation.

When the <ENTER> key is pressed the system will exit from the SiS BIOS Utility and boot into Windows XP.

The Industrial PC is now running on one hard disk.

The assignment process is a three-step procedure:

- Each user is assigned a unique name.

- Each user is assigned a unique password. This is an optional step. A password is not required.

- Users are then assigned to an appropriate access group matching their level of responsibility for setup, maintenance and operation of the Forté moisture measurement system.

Once a user name is created by the Security Subsystem, that operator may log on to any other Forté subsystem installed on that computer, subject to the restrictions imposed by the assigned access group.

To log on to a subsystem, the user selects a desktop icon to start the subsystem. A validation box for the subsystem is displayed. The user enters the appropriate user name and password, if required, into the Name and Password text boxes on the validation box and then presses the Submit button to activate the selected subsystem.

Once users log on to the Security System through the Measuring System menu bar command, they are not required to log on to the other subsystems (Calibration, Product Definition, Archives) if they open them from the Applications menu bar commands.

5.0 FEATURES OF THE SECURITY SUBSYSTEM

The Forté Security Window contains a menu bar that contains a User command menu and a Maintenance command menu.

5.1 THE USER COMMAND MENU

The User command menu allows the system administrator to perform the following user-related procedures:

- Add a new user,
- Remove a user,
- Authenticate a user,
- Change a user's password,
- Change a user's group access level.

To access the User commands, place the mouse cursor over User on the menu bar. A popup box with the available commands appears. Highlight the desired command with the mouse cursor. Click-on the command with the mouse button or press the "Enter" key on the keyboard to activate the command routine.
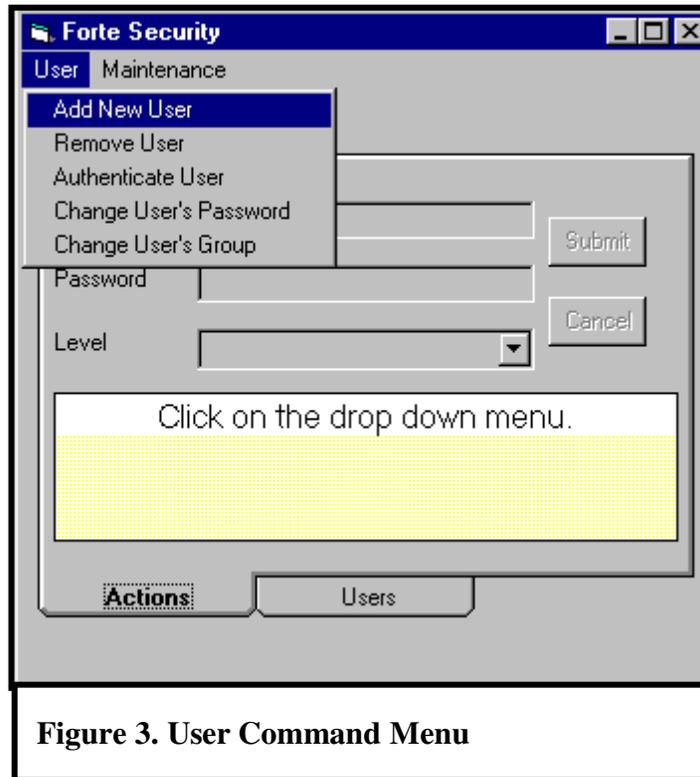
Figure 3. User Command Menu

5.2 THE MAINTENANCE COMMAND MENU

The Maintenance command menu allows the System Administrator to perform the following maintenance-related procedures:

- Delete all users,
- Clear all passwords,
- File Backup of security related information,
- File Restore of security related information.
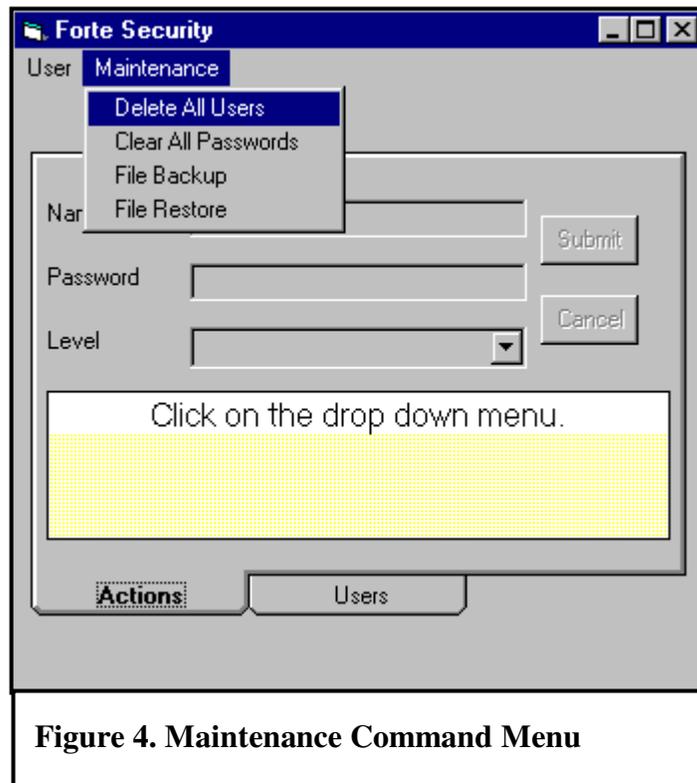
Figure 4. Maintenance Command Menu

To access the Maintenance commands, place the mouse cursor over Maintenance on the Menu bar. A popup box with the available commands appears. Highlight the desired command name with the mouse cursor. Click on the command with the mouse button or press the 'Enter' key on the keyboard to activate the command routine.

6.0 HOW TO USE THE SECURITY SUBSYSTEM

The following procedures are step-by-step descriptions of using the Security Subsystem menu commands. The System Administrator must start the Security Subsystem by running the UPG.exe file from the Security folder in the installation directory for the Forté program. After completing the Security-Login box, the main Security window will be displayed.

NOTE: Passwords are not required except for the default "Forté" user entry. System Administrators should use passwords to protect and limit access to system configuration settings. Password assignment is optional for lower level users.

6.1 HOW DO I ADD A NEW USER?

1. Highlight "User" on the menu bar.
2. Select "Add New User" from the popup box.
3. Enter a new user name in the "Name" text box. Up to 16 alphanumeric characters may be entered. Press the "Enter" key on the keyboard.
4. Enter a new password in the "Password" text box and press the "Enter" key. Up to 16 alphanumeric characters may be entered. If a password is not required, just press the "Enter" key on the keyboard.
5. Select a user access level from the "Level" combo box.
6. Press the "Submit" button to complete the creation of the new user identity.
7. The new user information will be displayed on the "User" tab screen.
.

5.1
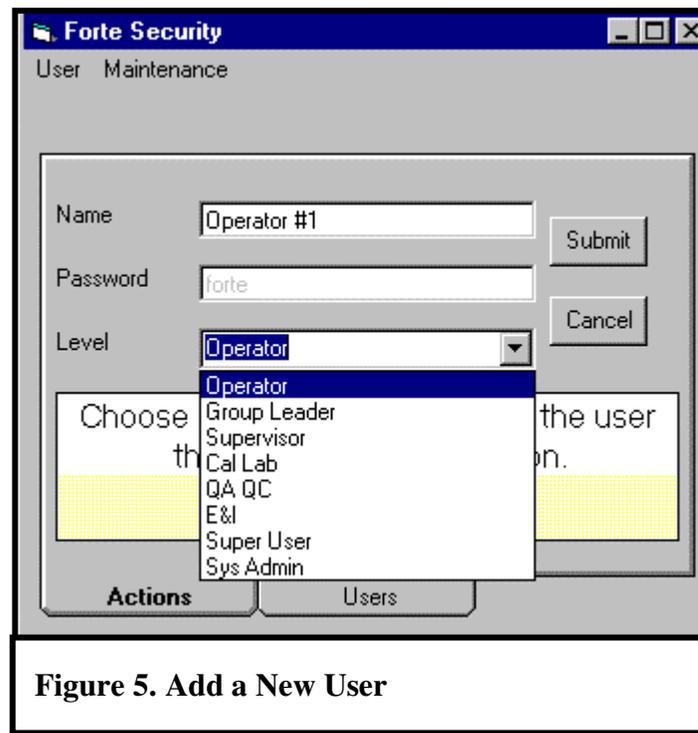
Figure 5. Add a New User

6.2 HOW DO I REMOVE A USER?

1. Select the "Users" window tab. A list of users is displayed.
2. Highlight the user to be removed on the list of users.
3. Highlight "User" on the menu bar.
4. Select and click-on "Remove User" from the popup box.
5. Confirm or deny the removal by selecting "OK" or "Cancel" in the "FSecurity" message box.
6. Asterisks replace the user name and related information. The asterisks will be removed the next time the Security Subsystem is started.
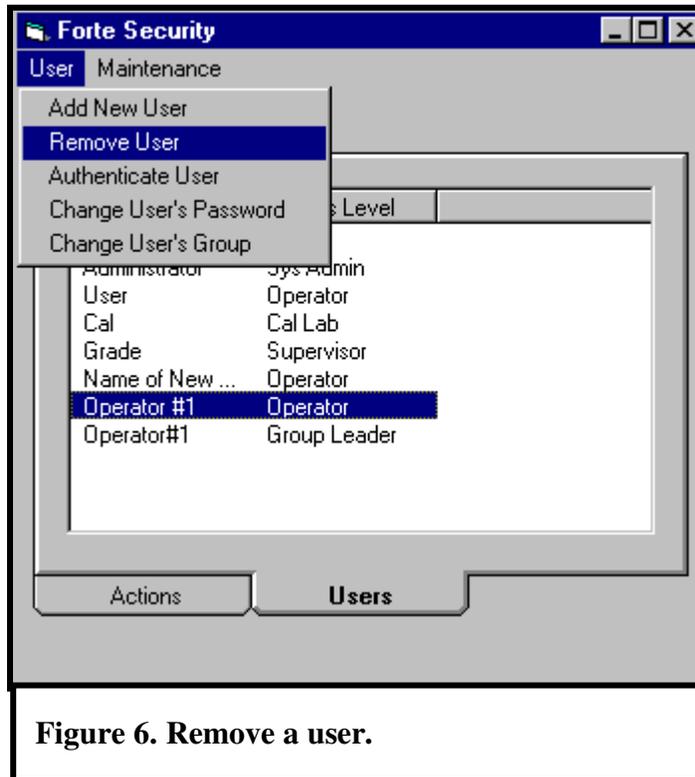
Figure 6. Remove a user.

6.3 HOW DO I AUTHENTICATE A USER?

NOTE: The purpose of authentication is to verify that a user name and password is valid. Authentication can also be achieved by viewing the listview display on the Users tab.

1. Highlight "User" on the menu bar.
2. Select "Authenticate User" from the popup box.
3. Enter the user name to be authenticated into the "Name" text box and press the "Enter" key.
4. Enter the user's password into the "Password" text box and press the "Enter" key.
5. Press the "Submit" button to authenticate the selected user name.
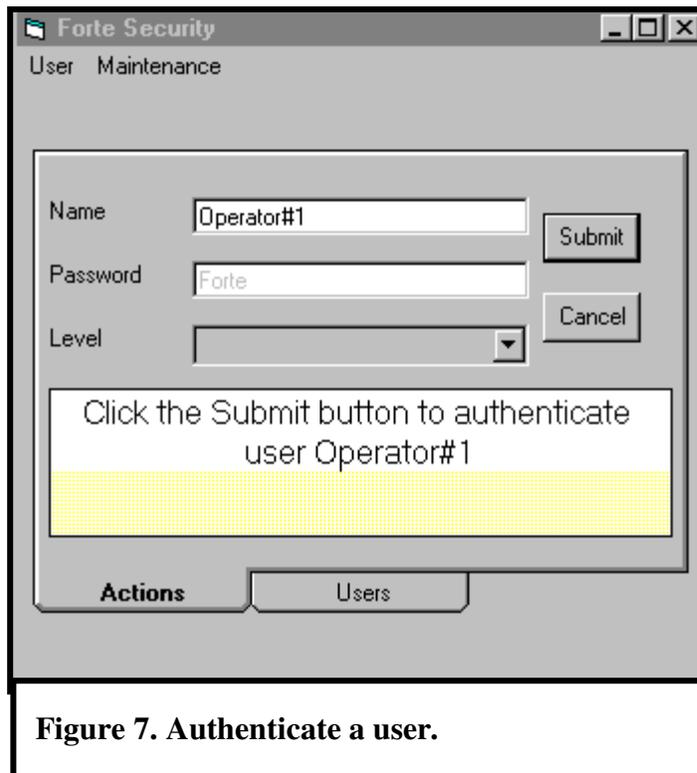
Figure 7. Authenticate a user.

6.4 HOW DO I CHANGE A USER'S PASSWORD?

1. Highlight "User" on the menu bar.
2. Select "Change User's Password" from the popup box.
3. Enter the user name into the "Name" text box and press the "Enter" key.
4. Enter the user's current password into the "Password" text box and press the "Enter" key.
5. Press the "Submit" button to authenticate the selected user name.
6. Type in the new password and press the "Enter" key.
7. Press the "Submit" button to confirm the new password.
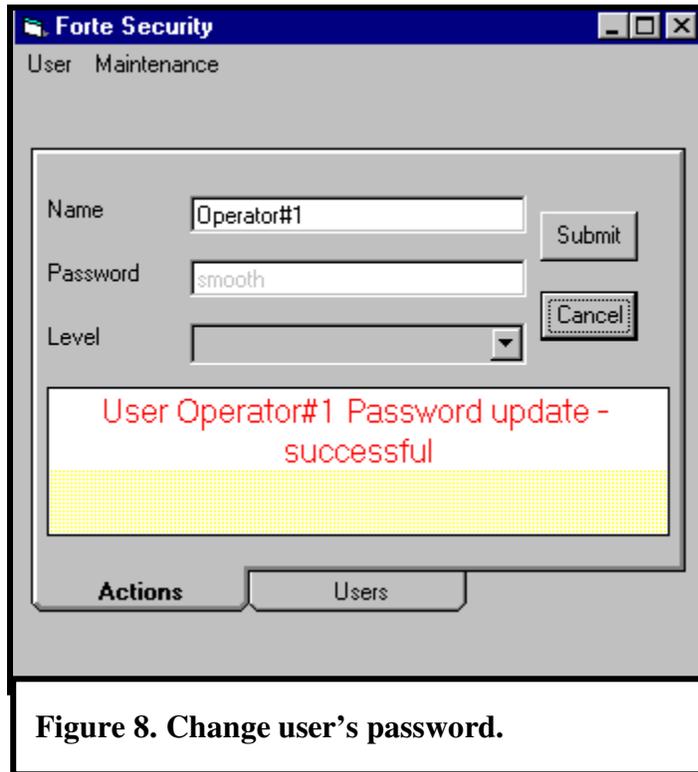
Figure 8. Change user's password.

6.5 HOW DO I CHANGE A USER'S GROUP ACCESS LEVEL?

1. Highlight "User" on the menu bar.
2. Select "Change User's Group" from the popup box.
3. Enter the user name into the "Name" text box and press the "Enter" key.
4. Enter the user's current password into the "Password" text box and press the "Enter" key.
5. Press the "Submit" button to authenticate the selected user.
6. Select the new group access level from the "Level" combo box.
7. Press the "Submit" button to confirm the new group level.
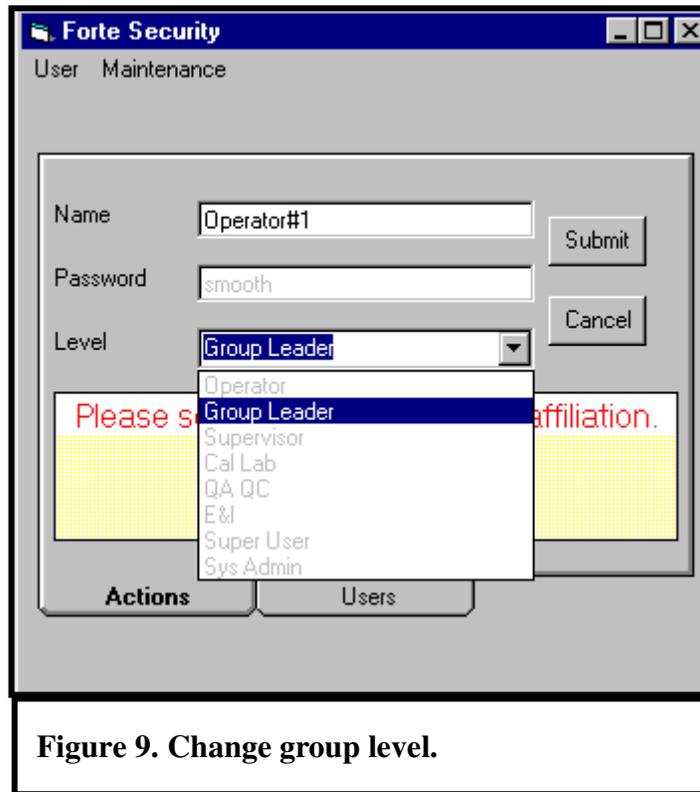
Figure 9. Change group level.

REV A

6.6 HOW DO I DELETE ALL CURRENT USER IDENTITIES?

1. Highlight "Maintenance" on the menu bar.
2. Select "Delete All Users" from the popup box.
3. A Maintenance message box appears. Select "OK" to delete all users or "Cancel" to return to the main Security screen without deleting any information.
4. If "OK" is selected, another Maintenance message box appears listing the total number of users to be deleted. Select "OK" to delete all users or "Cancel" to return to the main Security screen without deleting any information.
5. All names and related information, except for the default Forté user, are removed from the user list by the "Delete All Users" command.
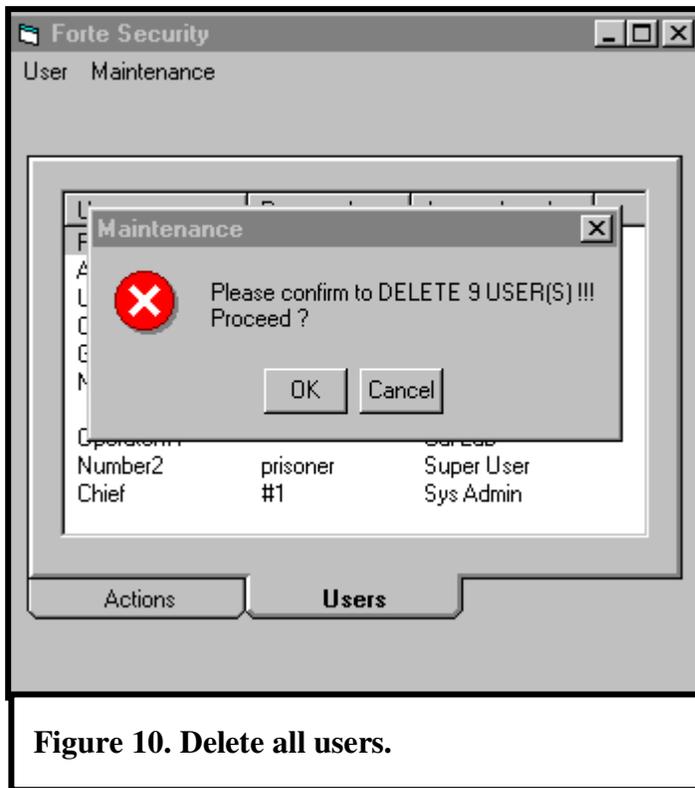
Figure 10. Delete all users.

REV A

6.7 HOW DO I CLEAR ALL EXISTING PASSWORDS?

NOTE: You cannot recover deleted passwords.
1. Highlight "Maintenance" on the menu bar.
2. Select and click-on "Clear All Passwords" from the popup box.
3. Passwords are immediately removed from the user list. No warning message is given.
4. All passwords are removed from the system, except for the password associated with the default Forté user.
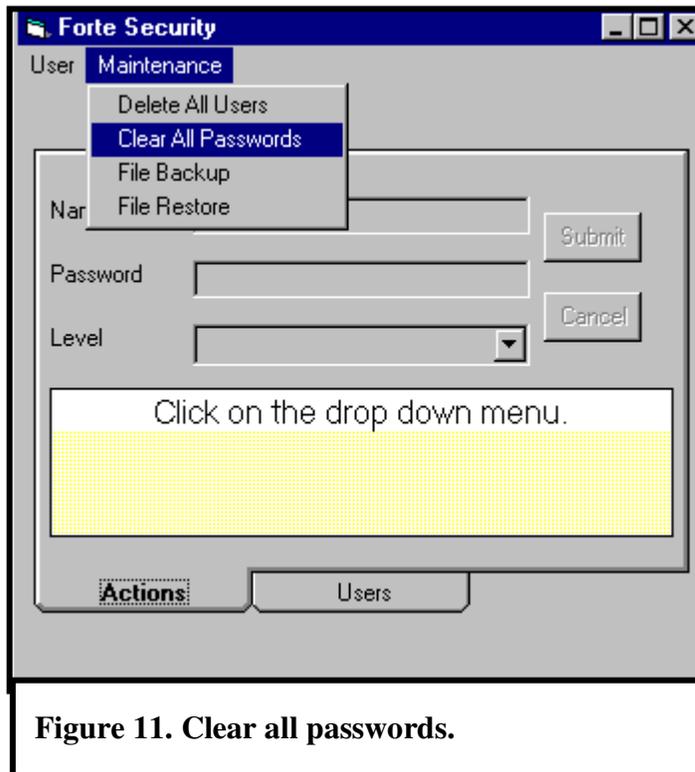
Figure 11. Clear all passwords.

6.8 HOW DO I MAKE A BACKUP FILE OF ALL SECURITY SUBSYSTEM INFORMATION?

1. Highlight "Maintenance" on the menu bar.
2. Select and click-on "File Backup" from the popup box. The File Maintenance window opens.
3. Select the Security check box at the top of the File Maintenance window.
4. Select the Backup Destination Directory from the listview box, or right click within the listview box to create a new backup directory.
5. Press the Backup button.
6. If there is a backup UPG.DAT file already in the target backup directory, the user will be prompted to replace the file with the new security data file or cancel the operation. Select "YES" to overwrite the file, or "NO" to quit the backup.
7. A confirmation box appears when the backup is complete.
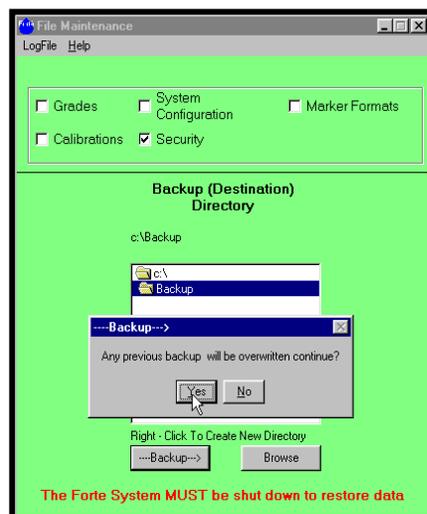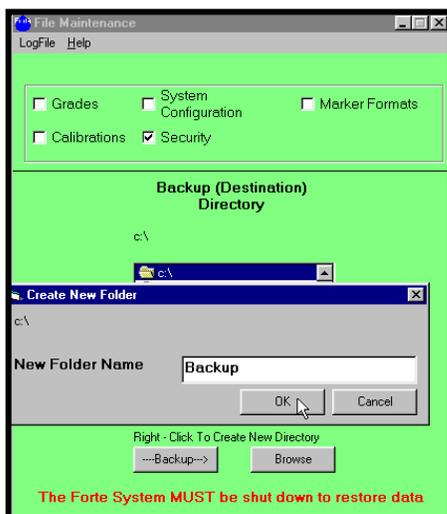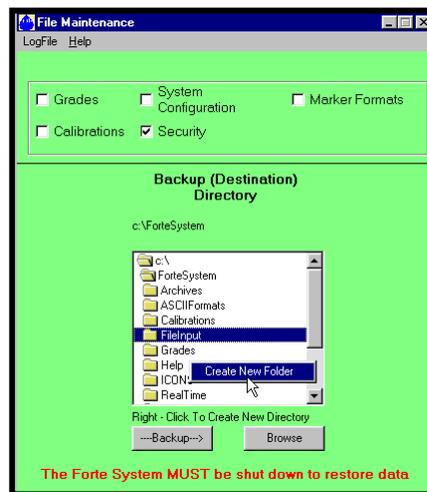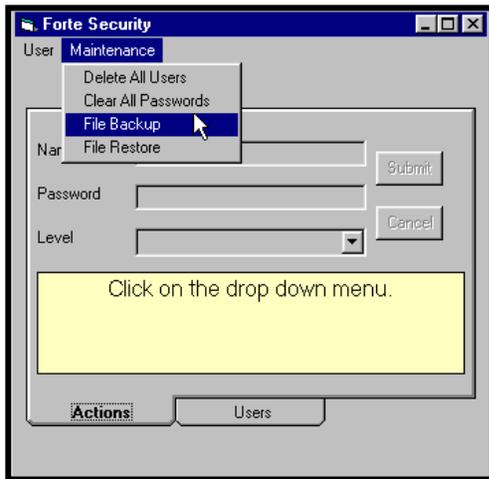
6.9 HOW DO I RESTORE SECURITY BACKUP FILES?

1. The Forté System, including the Measuring System, Summary and Archives, must be shutdown during the restoration of the Security data.
2. Highlight "Maintenance" on the menu bar of the Forté Security window.
3. Select and click-on "File Restore" from the popup box. The File Maintenance window opens.
4. Select the Security check box at the top of the File Maintenance window.
5. Select the directory that contains the backup security file from the listview box.
6. Press the Restore button.
7. A message box will appear asking the user to confirm the restore. Select "YES" to overwrite the existing UPG.DAT file in the Security folder, or "NO" to quit the restore.
8. A confirmation box appears when the restore is complete.
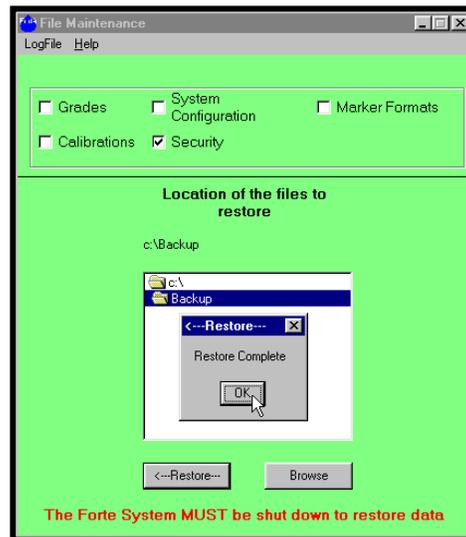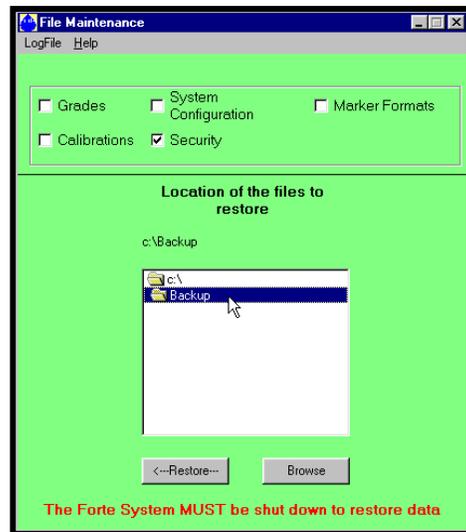
6.10 HOW DO I EXIT FROM THE SECURITY SUBSYSTEM?

1. To exit from the Security Subsystem, click-on the windows close box in the upper right-hand corner of the Forté Security window.
2. Any change to the security information data is saved upon the entry of the new data. A "Save" command is not required before exiting from the subsystem.
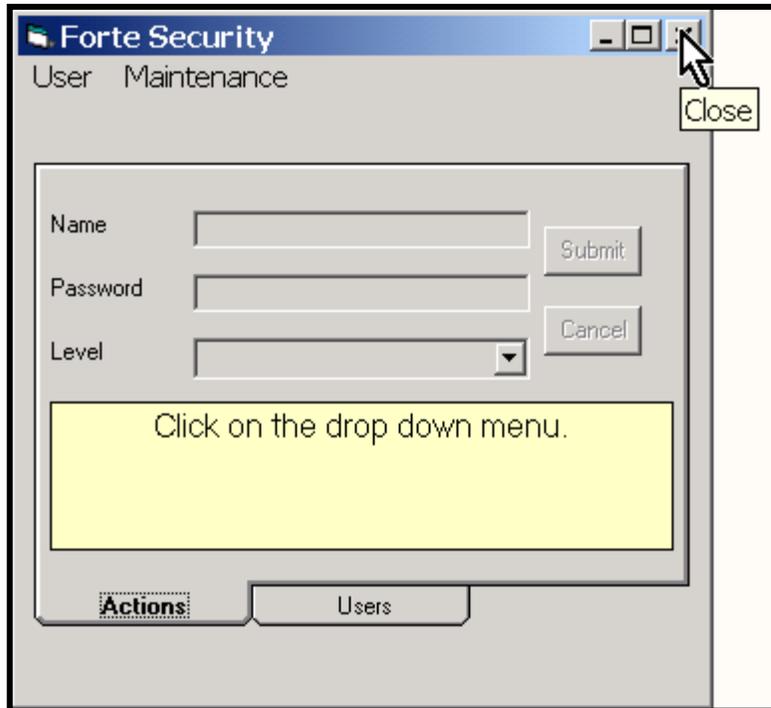
7.0   GROUP ACCESS LEVEL DEFINITIONS

The group access level definitions are assigned to users in the Security Subsystem.
They define user access to ALL of the Forté Subsystems.

All users, except Super Users, are logged off the Forté Subsystems after fifteen minutes.

The following chart lists the group access levels in order of importance:

#	LEVEL NAME	PERMISSIONS:
1	Sys Admin	Security Subsystem: Full Access
		All other subsystems: Partial Access

#	LEVEL NAME	PERMISSIONS: Partial Access.
2	Super User	Full Access to all Subsystems & menus, except Security Subsystem.

#	LEVEL NAME	PERMISSIONS: Partial Access.
3	E & I	MMS Schematic: Setup Menu - Devices & Digital I/O. Lots Menu – Full Access. Applications Menu – Partial Access To Grade & Cal. Maintenance – No Access. Measurement – Full Access. Stations – Full Access. System Log – Full Access. Product Info – Full Access. Security – Log On/Log Off.
		Summary Window: Configuration - Formats only. Summaries - Flush active.
		Calibration Subsystem: Print, System Log, and User only. Modify Status of data points.
		Grades Subsystem: Print, System Log, and User only. Modify Parameters Tab.
		Security Subsystem: No Access.

#	LEVEL NAME	PERMISSIONS: Partial Access.
4	QA/QC	MMS Schematic: Setup Menu – No Access. Lots Menu – Full Access. Applications Menu – Partial Access To Grade & Cal. Maintenance – Full Access. Measurement – Full Access. Stations – No Access. System Log – Full Access. Product Info – Full Access. Security – Log On/Log Off.
		Summary Window: Configuration - Formats only. Summaries - Flush active.
		Calibration Subsystem: Print, System Log, and User only. Modify Status of data points.
		Grades Subsystem: Print, System Log, and User only. Modify Parameters Tab.
		Security Subsystem: No Access.

#	LEVEL NAME	PERMISSIONS: Partial Access.
5	Cal Lab	Calibration Subsystem Only: Full Access.
		MMS Schematic: Setup Menu – No Access. Lots Menu – Full Access. Applications Menu: Calibration Menu – Full Access. Grade Menu – Partial Access. Maintenance – No Access. Measurement – Full Access. Stations – No Access. System Log – Full Access. Product Info – Full Access. Security – Log On/Log Off.
		Summary Window: Configuration - Formats only. Summaries - Flush active.
		Grades Subsystem: Print, System Log, and User only. Modify Parameters Tab.
		Security Subsystem: No Access.

#	LEVEL NAME	PERMISSIONS: Partial Access.
6	Supervisor	MMS Schematic: Setup Menu – Item Grouping. Item Numbering. Lots Menu – Full Access. Applications Menu – Partial Access. Print, System Log, User menus. Maintenance – Full Access. Measurement – Full Access. Stations – No Access. System Log – Full Access. Product Info – Full Access. Security – Log On/Log Off.
		Summary Window: Configuration – Full Access. Summaries - Flush active.
		Calibration Subsystem – Partial Access. Print, System Log, User only.
		Grades Subsystem: Print, System Log, and User only. Modify Parameters Tab.
		Security Subsystem: No Access.

#	LEVEL NAME	PERMISSIONS: Partial Access.
7	Group Leader	MMS Schematic: Setup Menu – No Access. Lots Menu – Full Access. Applications Menu – Partial Access. Print, System Log, User menus. Modify the Parameters Tab. Maintenance – No Access. Measurement – Full Access. Stations – No Access. System Log – Full Access. Product Info – Full Access. Security – Log On/Log Off.
		Summary Window: Configuration – Formats only. Summaries - Flush active.
		Calibration Subsystem – Partial Access. Print, System Log, User only.
		Grades Subsystem: Print, System Log, and User only. Modify Parameters Tab.
		Security Subsystem: No Access.

#	LEVEL NAME	PERMISSIONS: Partial Access.
8	Operator	MMS Schematic & Summaries, Limited Menus

		MMS Schematic: Setup Menu – No Access.
		                     Lots Menu – Full Access.
		                     Applications Menu – Partial Access.
		                        Print, System Log, User menus.
		                        Modify the Parameters Tab.
		                     Maintenance – No Access.
		                     Measurement – Full Access.
		                     Stations – No Access.
		                     System Log – Full Access.
		                     Product Info – Full Access.
		                     Security – Log On/Log Off.

		Summary Window: Configuration – Formats only. Summaries - Flush active.
		Calibration Subsystem – Partial Access. Print, System Log, User only.
		Grades Subsystem: Print, System Log, and User only. Modify Parameters Tab.
		Security Subsystem: No Access.

#	LEVEL NAME	PERMISSIONS: Forté Use Only.
9	Forte	Full Access to all subsystems.

8.0   NOTES:

REV A

9.0   SERVICE AND SUPPORT INFORMATION:

Forté Technology Inc. provides telephone and e-mail support for up to ten (10) hours, computed in 15-minute increments, for a period of one (1) year after installation of a system. Thereafter support is charged at our standard hourly service rate, computed in 15-minute increments.

For information on current service rates, please contact Forté Technology Inc.

Our scheduled business hours are Monday through Friday, 08:00 to 17:00 Eastern Standard Time (EST).

Mailing/Shipping Address:

FORTÉ Technology, Inc.
125 John Hancock Road, Suite 9
Taunton, MA 02780
U.S.A.

Forté Technology can be contacted by any of the following methods.

Telephone: 1-508-802-9634

Fax: 1-508-824-2085

E-mail: service@forte-tec.com

Internet: www.forte-tec.com