Replacing a Digitech System Controller with a Falcon XT

To allow existing Digitech sites to obtain modern access control features available from PTI (such as our mobile phone applications), while retaining Digitech keypads and other peripheral devices, this document explains how to replace the Digitech System Controller (or Syscon) with a Falcon XT. Note that DigiGuard wireless alarms are not supported by the Falcon XT and the associated StorLogix software.

Table of Contents

Computer Requirements

1. Before installation, confirm that the PC that is to have StorLogix installed meets the requirements needed to run the software. These computer requirements are the minimum for running the software by itself. **NOTE:** If you are using any other software along with StorLogix, it is imperative that you ensure that your computer specifications more than exceed the combined total requirements for all of the software installed on the computer. These software specifications only cover a computer dedicated to PTI Security Systems software.

   - 1.8GHz+ processor.
   - 2+ GB RAM, 4+ GB RAM for StorLogix.
   - 10+ GB available hard drive space.
   - DVD-ROM. (with high storage capacity, such as a DVD-RW, available for backups)
   - 800 x 600 minimum resolution monitor.
   - Sound card and speakers recommended.
   - One or more available working ports [Ethernet TCP/IP port(s), USB port(s), or RS232 port(s)].[1]
   - Broadband/high-speed business internet connection (cable, T1, or DSL), always-on connection.
   - Keyboard and Mouse.
   - A high quality printer (for printing Reports)
   - Remote access software for technical assistance. To receive technical support, you MUST have a remote access software installed on your PC. (Join.me, LogMeIn, ShowMyPC, TeamViewer, etc.)
   - Anti-virus software. (Windows Security Essentials, Trend Micro, McAfee, Norton, etc.)
   - Windows Firewall or other firewall protection is strongly recommended (ensure settings do not interfere with other applications running the system). This should be set up by a knowledgeable computer tech as some configuration may be required.
   - UPS (Uninterruptible Power Supply) power backup and surge protection recommended. (Part # PPWRUPSAPCBP350).

   Supported Operating Systems

   - 32-bit (x86) or 64-bit (x64)* Windows® Vista SP2, 7 SP1, 8, 8.1, or higher.
   - 32-bit (x86) or 64-bit (x64)* Windows® Server 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, or higher.
   - Windows® XP is no longer supported; StorLogix 5.0 and higher will not run on this OS.
   - All necessary updates and service packs for Windows should be loaded onto the computer before beginning installation.

[1] Connection through a Network port is recommended. USB connection if network port is not available. RS-232 connection is not recommended.

Notes on Interfacing with Management Software

Many DigiGate systems interface with a third party management software that is used for the day-to-day operations of the facility (e.g. Domico, SiteLink, Syrasoft, etc.). These applications send information to the DigiGate system via a data file that is formatted to specifically work with DigiGate.
The settings for the management software will need to be changed to send the information to the new StorLogix program instead of DigiGate. Because of the large number of different management applications that are available, we cannot give any instructions on how this is done. The site doing the conversion will need to contact the help desk for their particular application to receive instructions on how to make these changes.

Retrieving DigiGate Setups

The DigiGate application installed on the PC that was running the access system will be used to print out reports to assist in the configuration of the new StorLogix software. (**I**f you do not have a printer, contact your PTI Salesperson for information on how to transfer your setups to our servers where they can be printed out.)

1. In the DigiGate program main menu, select the “Report” button.

2. In the Reports Menu, select the tab labeled “Misc. Reports”.

3. Select the button labeled “Setup Info”. This will print immediately to your default printer, and will not show a preview screen.

4. If your site does not have hard-wired door alarms, close the report view, exit out of DigiWin, and continue to the next page.

5. Select the button labeled “Mux/Slot”. This will display a preview screen for the report. Click on the Disk icon at the top of the screen.

6. Change the “Save as Type” to “Text file” (*.txt), provide a file name to save to, and then click “Save”. (If you are installing the Storlogix software on a different machine from the one that ran the Digigate program, you will need to transfer this saved file to that machine for use later on in this document.)

7. Close the report view and exit out of DigiWin.

Temporary XT Location

Note: You may wish to do this step concurrently with installing the StorLogix software (below) as some parts of the software installation can take 30 minutes or more to complete

Place the XT controller in a temporary location near where its final location will be. The purpose of this is to test communications to the XT and ensure that it works, before any DigiGate equipment is disconnected.

After locating it, connect it to power and to your selected communication cable. It is highly recommended that a network connection be used, even on sites where the controller and PC are in the same room. Depending on the site in question, this may require networking equipment (such as a router) to be installed. See appendix A of these instructions for examples of communication connections from the PC to the XT.

Installing the StorLogix software

After you have printed out the DigiGate system information, follow the instructions that came with your StorLogix software DVD and install it onto your PC. To function correctly, the version of the StorLogix software must be 5.0 or greater.

1. Following installation of the StorLogix software, the Configuration Wizard will prompt regarding which type of access system the software is to be used with. Make sure you select the ***DigiGate*** option.

2. The Configuration Wizard will request various site information. A name, password, and gate code will be required for the initial user of the system (usually the manager).

3. Under “Access Devices”, select the layout which best matches the current access configuration at the site. See Appendix B of these instructions for examples of gate layouts. If *any* of the keypads on your site have LCD screens for messages, select the radio button labeled “Display”.

4. Click “Next” after entering this information. The database will initialize and this may take a few minutes to complete before the next step is displayed.

5. The wizard will ask for information regarding the Business Hours for the site. This setting corresponds to the “Time Zone” setting in the DigiGate setups. Refer to the printout of the DigiGate setups you did and find the page for the time zones. Use the settings that are listed for Time Zone #1 “Normal Hours” and enter them into the setup wizard.

If hours are different on Saturdays, Sundays, and Holidays, be sure to specify those days individually. If the site is closed on any day of the week or holidays, place a checkmark in the corresponding "Closed" checkbox.

6. The next step is to choose the connection type. Select the method that you used to connect to the XT controller. Follow the on-screen instructions to connect to your XT.

7. After connection has been made, the Configuration Wizard will ask which type of management software is being used. Select the one in use on the site. If your management software is not in the list, select "Generic".

8. After the wizard has finished, StorLogix should be run for the first time. Log into it using the manager name and password that was selected previously in step 2. In addition to StorLogix opening, you will also see the "StorLogix Interface" window open. This is the interface to the management software and can be minimized at this time.

9. The first time that the StorLogix software runs it may ask if you want to display in "Classic" mode or "Standard". The DXT setups will only function in "Classic" mode so this option should be selected.

10. When first running the StorLogix program, it will automatically update the controller by doing a "Send All". You may notice a progress meter in the status bar while this update is taking place.

    Note: If you cannot establish connection to the XT controller (LogixServer shows as "Offline"), contact PTI Security support at https://support.ptisecurity.com/ to resolve this problem before continuing any further.

11. After the Send All has completed, shut down StorLogix.

12. Remove power and battery from the XT and disconnect the communications cable. Continue on to the next section to begin removing the old DigiGate System Controller and replacing it with the XT.

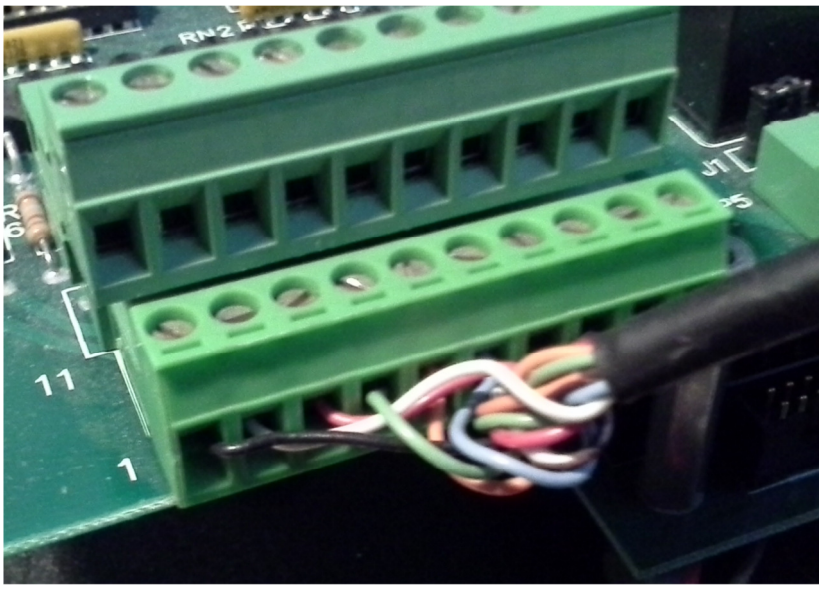
Hardware Replacement

Note: During this changeover, your access control system will be inoperable. You should take steps to ensure that your customers can enter and exit the facility by manually opening any gates or doors until the changeover has been completed.

The following steps are for replacing the hardware of the Syscon. Some steps are optional, depending on the existing Digitech equipment setup. Disconnect power from the Syscon before starting.

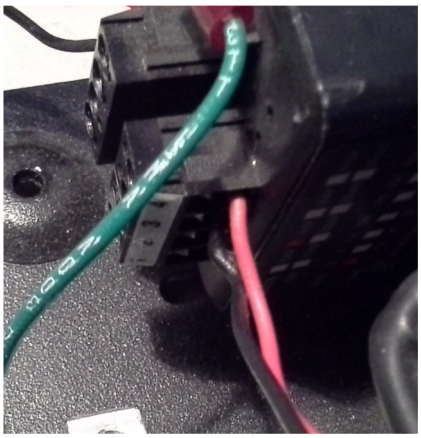
If the Syscon to be replaced does not have any keypads connected to the keypad I/O board (the upper board of two installed inside the Syscon), start at step #2. Note that some Syscons may not have a keypad interface board installed in which case you can start at step #3.

1. Unplug any standard keypads from the keypad interface board (the top board in the Syscon) and label each one as port #1 through port #4. (Port one is in the lower left of the keypad interface board inside the controller, shown in the picture below. Port two is the upper left port, three is the lower right, and four is the upper right).



2. Disconnect and label any relay outputs from the keypad interface board.

3. Disconnect and label the RS485 data line(s) from the surge suppressor located in the bottom right of the Syscon, if any are connected.



4. Disconnect and label any siren or alarm system trigger wires connected to port P3 on Syscon bottom board, if any are connected.

5. Disconnect the serial communications cable from the Syscon. Depending on the system this cable may be connected to a PC, a DigiPort network adapter, or a telephone modem. This cable is no longer used and can be disconnected. If the system used a DigiPort network adapter, it is no longer needed.

6. Remove the Syscon assembly and its power supply from its installed location.

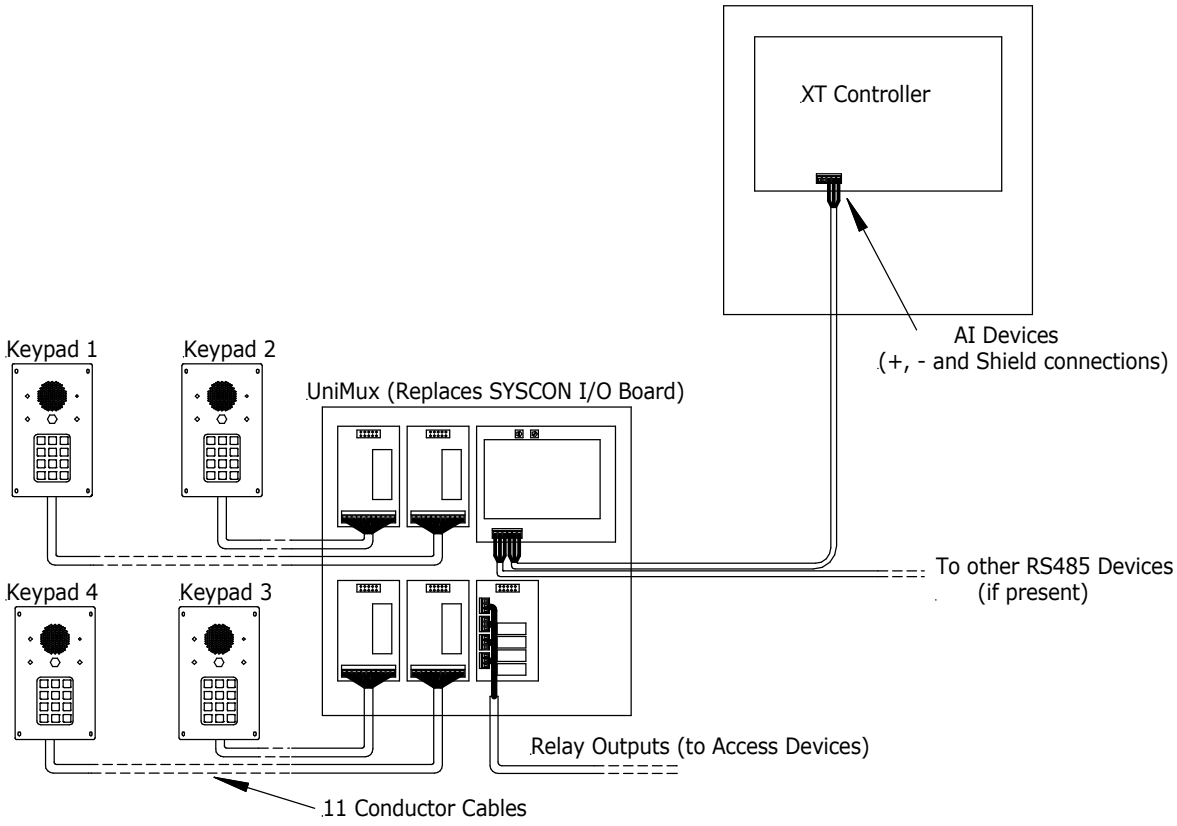
7. Install the Falcon XT in the location previously occupied by the Syscon. Leave enough room to install a new Digitech UniMux if one is needed. (See step 10). Refer to PTI Document 114A3866 "Falcon XT System Installation Manual" for instructions on mounting, providing power to, and proper grounding of the XT.

   Note: ***It is extremely important that the XT be connected to a good earth ground so that the onboard surge suppression circuitry can function correctly***. This should be a copper grounding post or grounded water pipe as per local code and as close to the XT location as possible.

8. Connect the communications cable (network or USB) that you used earlier to communicate with the XT.

9. Connect any siren output wires that were disconnected in step #4 to relay #1 N/O output in the XT. Connect any alarm trigger wires to relay #2, N/C output.

10. If you disconnected any standard keypads from the Syscon in step #1, then a Digitech UniMux will need to be installed to connect these keypads. (If no UniMux is used, skip to step #13[1]). The UniMux ordered for this will have 4 keypad daughterboards and one relay board installed. An example of this is in the drawing below.



Refer to Chapter Six in the document "1100-044 DigiGate 700 System Installation Manual with Uni-MUX" (http://www.ptisecurity.com/download/digigate-700-system-installation-manual-including-uni-mux/) for instructions on how to install this UniMux. Connect the keypads that were originally attached to the Syscon to the daughterboards inside the UniMux (Page 6-3 of document 1100-044). Keypad #1 connects to the terminals on Daughterboard A, Keypad #2 on daughterboard B, and so on.

[1] If you are not using a keypad UniMux to replace a Syscon I/O Board, the RS485 data wire disconnected from the Syscon (step 3, page 7) will connect to the "AI Devices" port of the XT. Red to +, Black to -, and bare drain to shield.

11. Connect any relay outputs that were previously connected to the Syscon keypad interface board to the new UniMux. (See page 5-33 of document 1100-044). Use the following chart for connections. Note if the device uses normally open contacts (for example, gate operators & door strikes) or normally closed contacts (mag locks).

Previous relay inside System Controller	New relay inside UniMux
#1 (Pins 21 & 22)	Daughterboard E, Relay 1
#2 (Pins 23 & 24)	Daughterboard E, Relay 2
#3 (Pins 51 & 52)	Daughterboard E, Relay 3
#4 (Pins 53 & 54)	Daughterboard E, Relay 4
#5 (Pins 25 & 26)	UniMux Motherboard, Relay 1
#6 (Pins 27 & 28)	UniMux Motherboard, Relay 2

12. Connect the "AI Devices" port of the XT to one set of terminals on the RS485 port of the new UniMux, and then connect the RS485 data line that was previously connected to the Syscon (if one was present) to the other set of terminals on the RS485 port of the UniMux. (Page 5-31 of document 1100-044). **Set this UniMux to RS485 address #1** (Page 5-32 of document 1100-044).

13. (Optional) If you have a DigiGraphics, connect the RS485 cable for it to the "AI Devices" port of the XT.

14. Disconnect and remove the DigiGuard wireless receiver, if one is present. Any other DigiGuard equipment (Repeaters or Transmitters) will not interfere with the operation of the rest of the system, and may be disconnected or left in place as the owner desires.

15. Reconnect the XT to its power and battery.

Finishing the StorLogix Setups

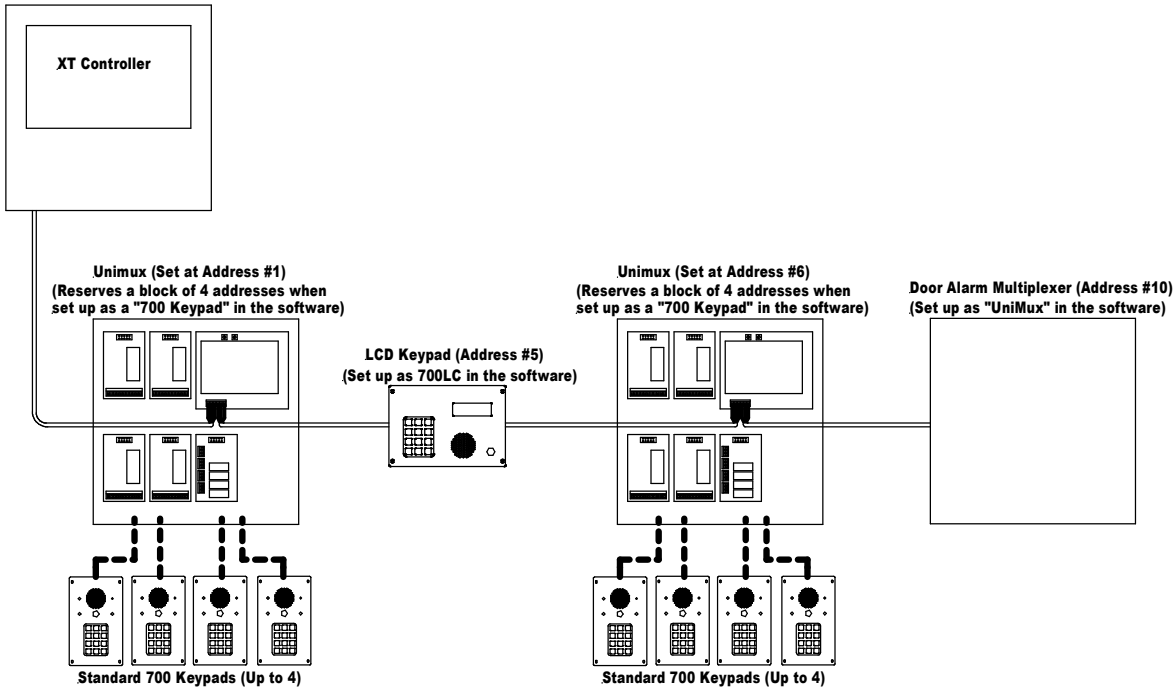
Note that these instructions cover situations dealing with basic access control and hardwired individual unit alarms. The steps here are meant to be a general guide and do not cover all possible programming situations that may arise while doing a conversion. Complex Digigate system setups, such as those involving elevators, lighting control, etc., may require assistance from a local dealer or installer.

Notes on RS485 Addressing

All of the access control and alarm devices communicate back to the XT controller over the two wire RS485 network. Each of these devices is assigned an “address” so that messages over the network can be delivered to a specific device.

With the Digigate system, standard keypads were plugged into either the Syscons I/O board (Address #1) or into a Keypad Expansion MUX (which could be assigned an address of 5 or higher). The keypads themselves did not have an address; instead, the board they were plugged into did.

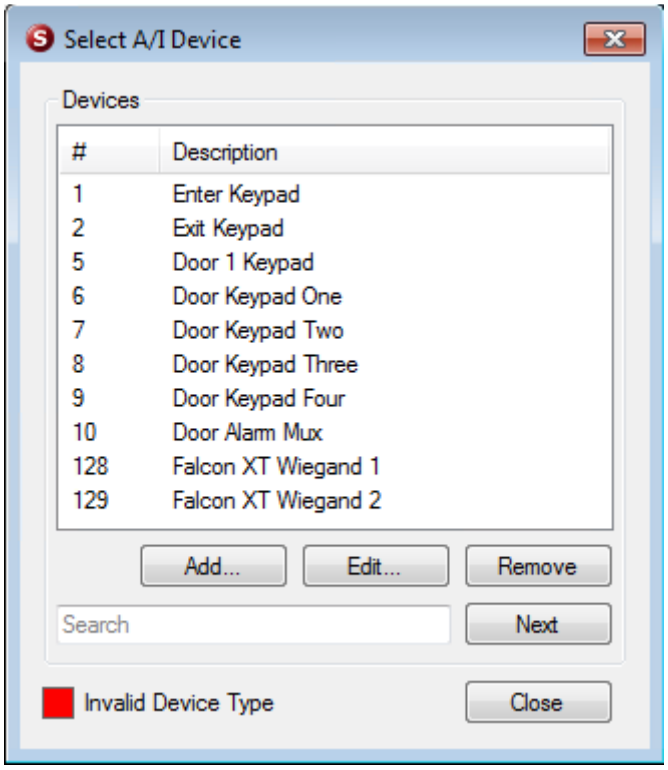
Because of the nature of the Storlogix database and setups, when programming Digitech standard keypads, the keypads are assigned an “address” in the software. Also, these addresses are reserved in blocks of 4, because up to 4 keypads can be connected to a UniMux.



The example on the previous page shows a Keypad UniMux that replaced the Syscon, and is set to address #1. The addresses from 1 through 4 are reserved in the programming setups for standard keypads (i.e. all 4 addresses are reserved even if less than 4 keypads are actually connected to the UniMux).

In the example, an LCD keypad is assigned to address 5 and a second keypad UniMux is set to address #6. This reserves 4 more slots (#6 through #9) for standard keypads. Finally, a door alarm multiplexer is assigned to address #10.

Below is a screen shot of what the AI device list would look like in StorLogix for the example layout. Note that in the example, devices #3 and #4 are skipped over, as the first Keypad UniMux only has two keypads plugged into it.



Note: Even though the list of Devices shows "Falcon XT Wiegand 1" and "Falcon XT Wiegand 2", the built-in Wiegand ports of the XT **do not function** when the system is in Digi mode.

Note: If a system that you are replacing has an existing Keypad Expansion MUX and also has other muxes using the RS485 addresses directly after it, the RS485 address of either the Keypad Expansion MUX or the muxes following it may need to be changed. In some situations where the existing MUX is of an older version that does not have a changeable address, the MUX may need to be replaced with a newer UniMux that does. Examples are shown in Appendix B.

Programming Standard 700 Keypads

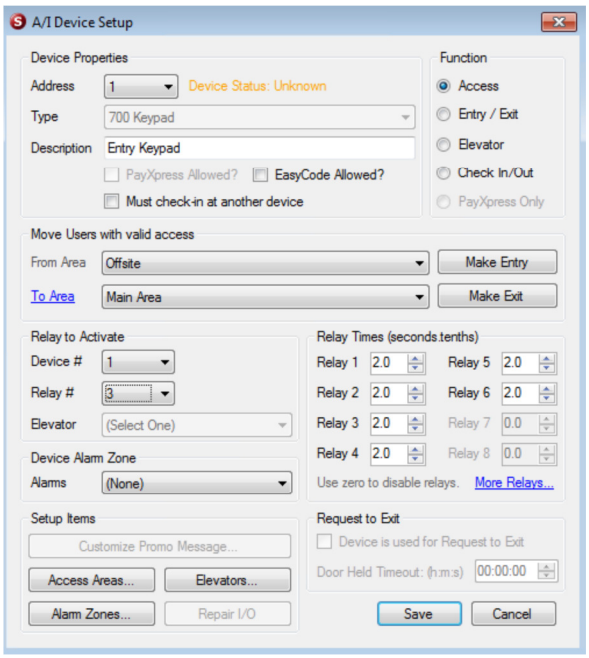
If your system has any Digitech standard keypads (the kind that connect using an 11 wire cable), a UniMux is used to connect them. Follow these steps to program the keypads into your system.

1. In StorLogix, Select the “Protected Site Setup” menu. The default password is 1234.

2. Click on “A/I Device Setup” option, and then click “Select”.

3. You will see a list of current A/I devices. Click on the “Add” button.

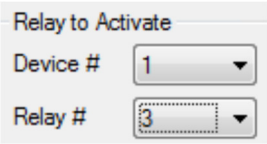
4. You will see the screen shown below. The UniMux that the keypads are plugged into is not added into the system. Instead, the keypads themselves are added in. The example below shows the first keypad on the UniMux addressed as device #1.



5. Referring to your printout of the previous DigiGate setups, determine if the Keypad being added is used to enter or exit the site. Set the “From Area” and “To Area” drop-downs as needed.

6. The first keypad on the Mux will also have the relay setups for the Mux. Set up all 6 relays, but use times relevant to the device being controlled (i.e. gates use 2 second times, while doors and mag locks should have a minimum of 10 seconds). Note that for UniMuxes, Keypad #1 will activate Relay #3. If using an older Keypad Expansion Mux, Keypad 1 will activate relay 1. See Appendix B for information on how to identify a Keypad Expansion Mux.

7. Set the relay to be activated on a good code entry. Refer to your previous DigiGate setups and use the following table for conversion.



Previous relay on Interface Board or MUX	New relay (If using UniMux)	New relay (If using Keypad Expansion MUX)
Relay #1	Relay 3	Relay 1
Relay #2	Relay 4	Relay 2
Relay #3	Relay 5	Relay 3
Relay #4	Relay 6	Relay 4

8. Click “Save” to add this device into the system.

9. Continue adding any other standard 700 style keypads that are connected to the Mux.

Programming 700LX and 700LC Keypads

Depending on the complexity of your system, your LX and LC keypads may have been set up by the Configuration Wizard when StorLogix was first run. If not, these keypads can be added using the following steps.

1. In StorLogix, Select the “Protected Site Setup” menu. The default password is 1234.

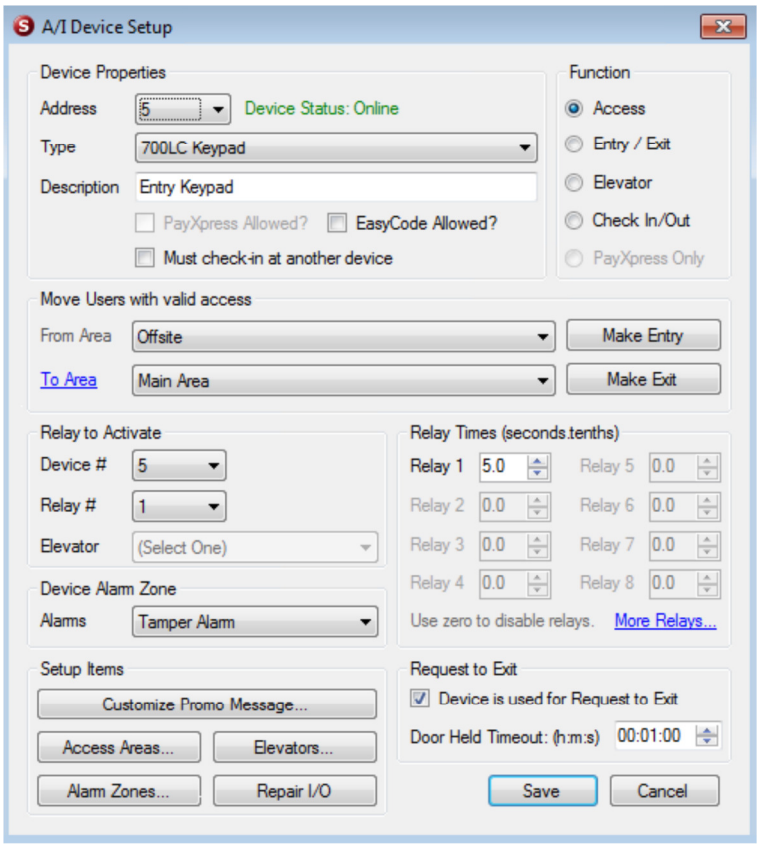
2. Click on “A/I Device Setup” option, and then click “Select”.

3. You will see a list of current A/I devices. Click on the “Add” button.

4. Refer to your DigiGate printouts for the device being added and set up the following items.

5. Set the A/I device to the same address that the device was set at in the DigiGate system.

6. Select “700LC” or “700LX” from the dropdown list, depending on which type you are adding.



7. Set the Description as needed.

8. Set the device To Area and From Area as needed.

9. Set the relay time for relay #1.

10. Set the Device and relay number to be activated on a good code. Generally this is the relay on the keypad, but sometimes it might be a relay on a different device.

11. If the keypad has a request to exit motion detector or pushbutton attached to it (typically only used at doors going into buildings), check the box "Device is used for Request to Exit". Set up the "Door Held Timeout" to the amount of time for the door to be shunted (Typically 1 to 2 minutes).

12. If the keypad has an alarm contact connected to it for door monitoring (typically only used at doors going into buildings), select an alarm zone in the "Device Alarm Zone" drop down menu. If you need to set up an alarm Zone for this, use the button for Alarm Zones in the "Setup Items" group in the lower left of the screen.

13. Keypads used for elevator control will need more detailed setup and this should be done by an experienced technician.

Click on "Save" to finish adding the device. The new device information will be sent to the XT automatically, as long as it is online. The XT will begin to poll the new device.

Programming the DigiGraphics

If your facility has the optional DigiGraphics display, enable it by:

1. In StorLogix, Select the "Protected Site Setup" menu. The default password is 1234.

2. Select "Falcon XT Setup".

3. Check the box labeled "Enable Site Graphics".

4. In the field labeled "Poll Timeout (ms)", set it to a value of 200.

5. Click on "Save".

Programming UniMuxes (Door Alarm and Relay)

If you have any Door Alarm or Relay Muxes on the system, configure them using the following steps.

1. In StorLogix, Select the “Protected Site Setup” menu. The default password is 1234.

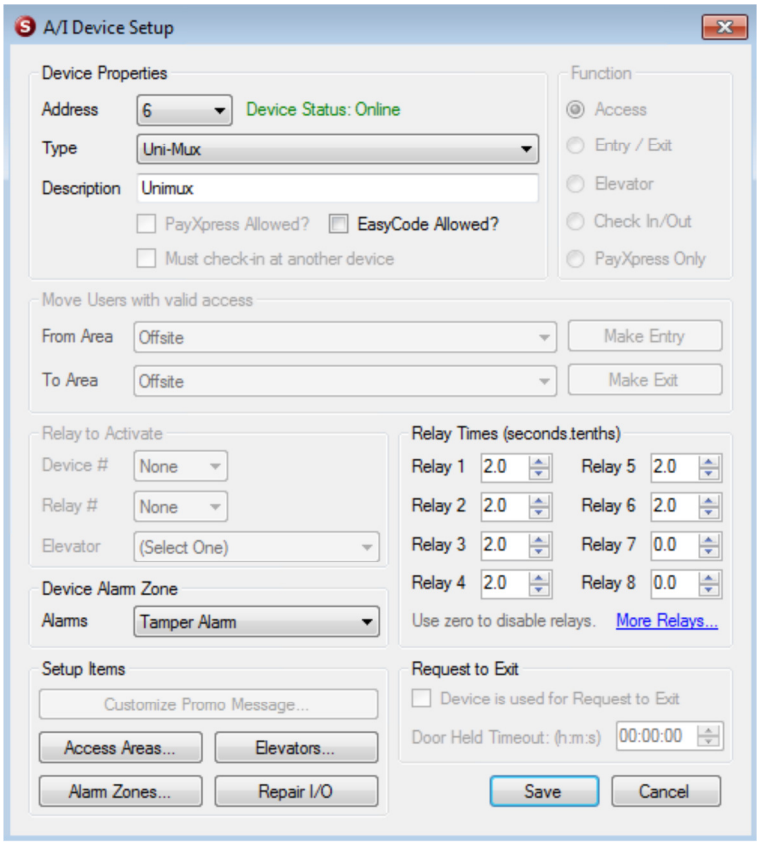
2. Click on “A/I Device Setup” option, and then click “Select”.

3. You will see a list of current A/I devices. Click on the “Add” button.

4. Refer to your DigiGate printouts for the device you are adding and set up the following items.

5. Set the A/I device to the same address that the device was set at in the DigiGate system.

6. Select “UniMux” from the drop down list of devices.



7. Set the Description as needed.

8. Set up the relay times for each relay in the UniMux. UniMuxes can have up to 22 relays installed, including the two relays on the motherboard, so this may require clicking on the “More Relays” option.

9. When clicking on “Save”, you will be prompted to add in the channels for this UniMux. “Starting Channel” value should be set to 1. Refer to your printed setups to the field labeled “Slots” for the DigiGate device. This is the number you should use for the “Ending Channel” value. In no case should this exceed 110.

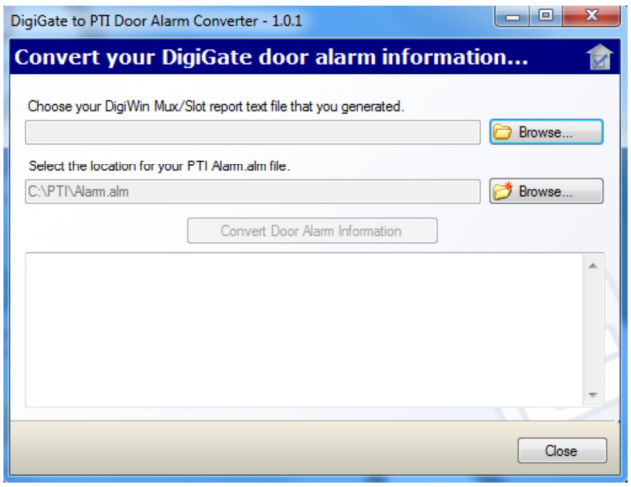
10. The new device information will be sent to the XT automatically, as long as it is online, and the XT will begin to poll the new device.

Transferring Mux /Slot Information for Door Alarms

If your system has door alarms setups, use the following steps to transfer the slot / channel data for the alarms.

1. On page 3, step 5 of this document you saved the DigiGate alarm information to a text file. If you are using a different PC to run StorLogix, transfer the file to that PC.

2. In the Program Files/PTI Security Systems/StorLogix folder (on 64 bit systems this will be Program Files(x86)/ PTI Security Systems/StorLogix), locate the program "DigiDoorConvert.exe" and run it. The screen below will be displayed:



3. Click on the "Browse" button to locate the text file that contains the DigiGate alarm information.

4. Use the default location to store the PTI alarm file, or click the second "Browse" button to select a new location or file name.

5. Click on the button "Convert Door Alarm Information" to start the conversion process.

6. Scroll up through the information displayed in the text window to verify the data converted. If successful, the last line should indicate a return value of 0. Close the converter program.

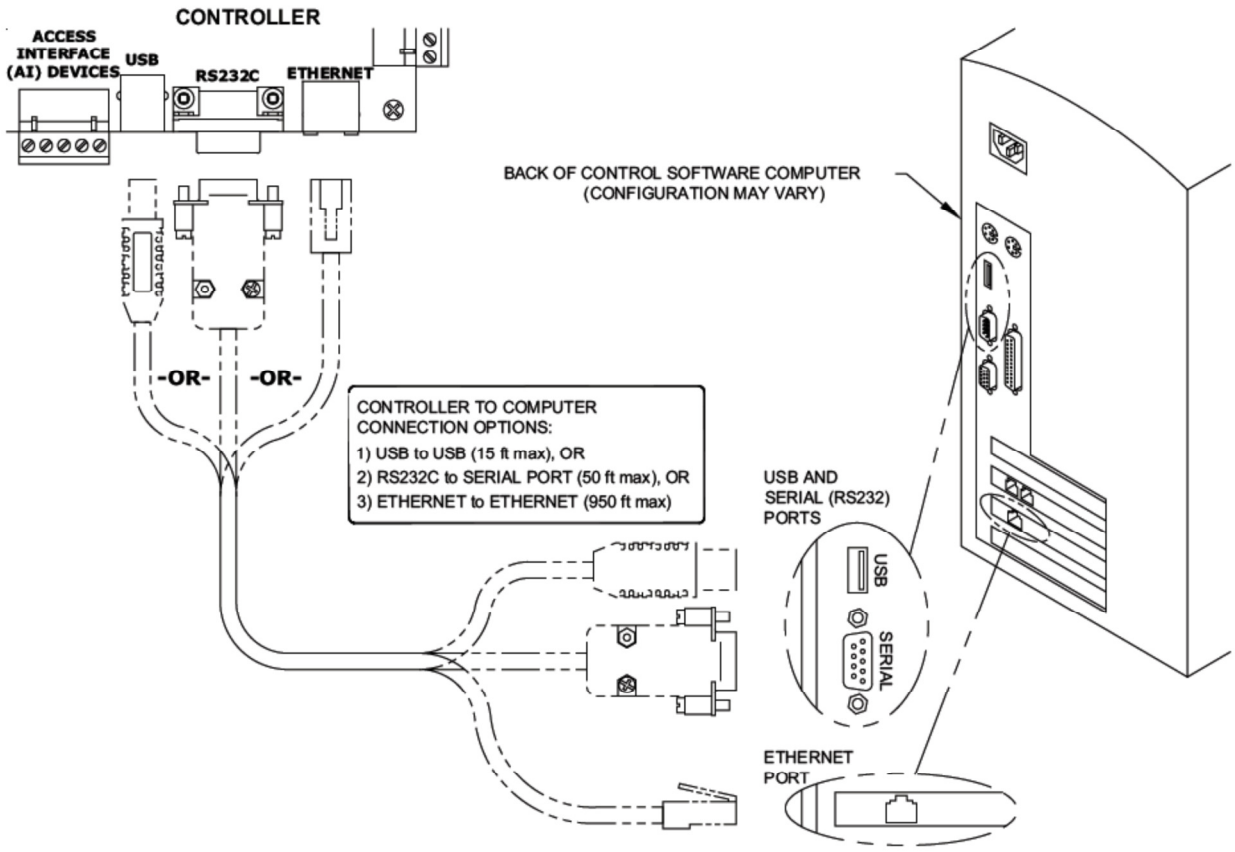
7. Open StorLogix.

8. Click on "Protected Site Setup" and enter the password to access that menu. The default password is "1234". Select "Mux and Channel Assignment".

9. Click the "Import" button and select the alarm file that was generated in step 3 above and click "Open".

10. The mux and slot data will be transferred into the StorLogix program.

Appendix A: Communications connections between the PC and the XT



For Direct Ethernet connections

1. Make or purchase an Ethernet cable using CAT5 Twisted Pair Network cable (100 meters maximum). Connect one end to the Ethernet port in the bottom right corner of the controller circuit board.

2. If needed, run the cable through conduit to the control software computer.

3. Connect the other end to the Ethernet port located on the back of the computer.

For Router/Switch Ethernet connections

1. Make or purchase two (2) Ethernet cables using CAT5 Twisted Pair Network cable (100 meters maximum). Connect the end of one cable to the Ethernet port in the bottom right corner of the controller circuit board.

2. Connect the other end of the cable to the router / switch.

3. Connect one end of the second cable to the software computer.

4. Connect the other end of the cable to the router / switch.

5. Power-up the router / switch.

For USB connections

1. Use the USB cable provided with the controller. Connect the smaller end of the USB cable to the USB port located on the bottom middle of the controller circuit board.

2. Run the USB cable through a knockout on the controller housing to the control software computer.

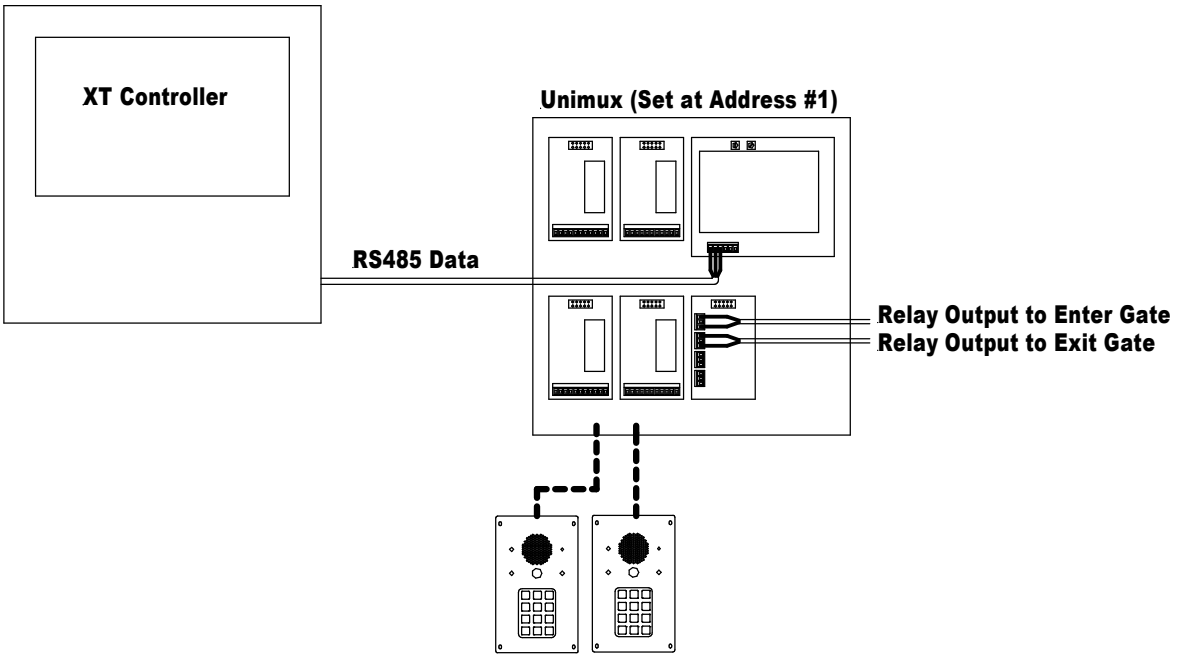
3. Connect the larger end of the USB cable to a USB port located on the back of the computer.

RS-232 connections should not be used.

Appendix B: Examples of interface device layouts

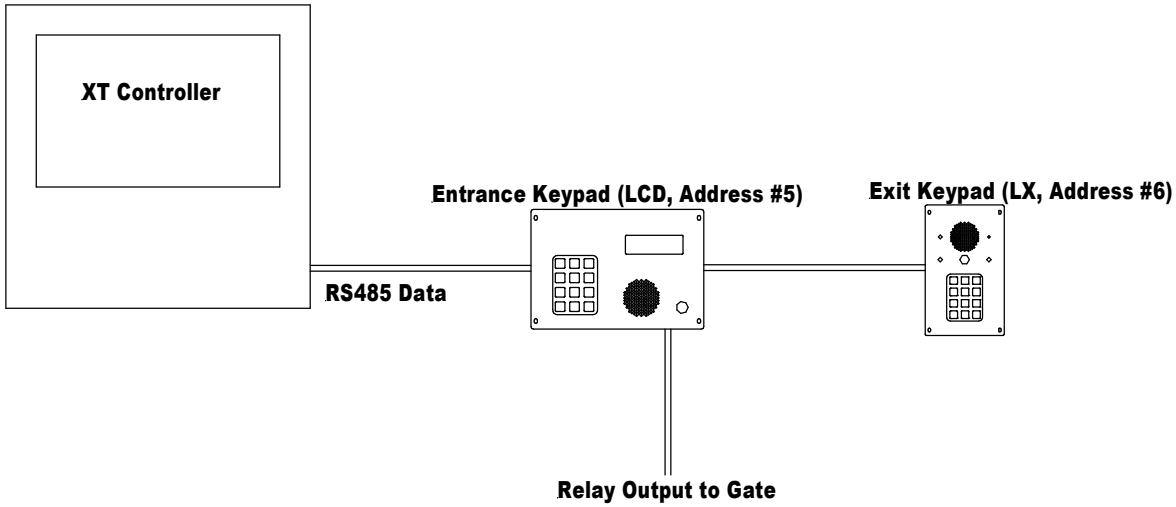
The most common layout encountered will be 2 keypads (one entry and one exit) connected to a single gate operator. These keypads may be standard 700 type keypads, or 700-LX / 700-LC keypads. Sometimes a site will have an LC keypad for the entrance and an LX keypad for the exit.

Below is an example of a Falcon XT connected to a DigiGate system. The Syscon has been replaced by a keypad UniMux set to address #1. Two standard 700 keypads are connected to this UniMux. There are two gate operators connected to relay outputs on the UniMux.

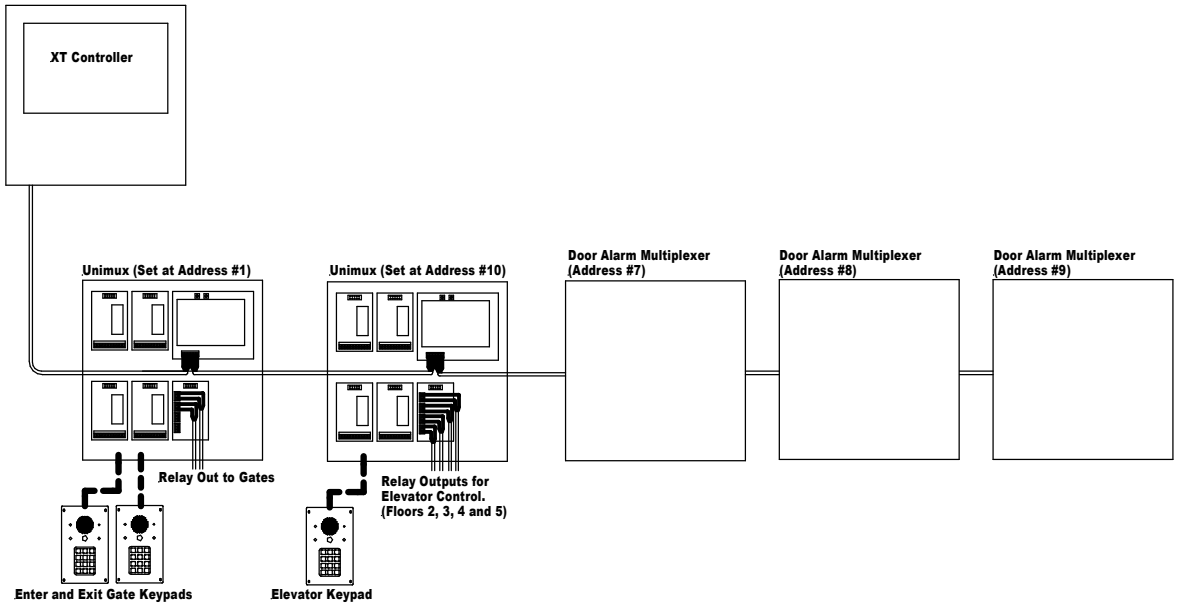


Standard 700 Keypads plugged into daughterboards A and B

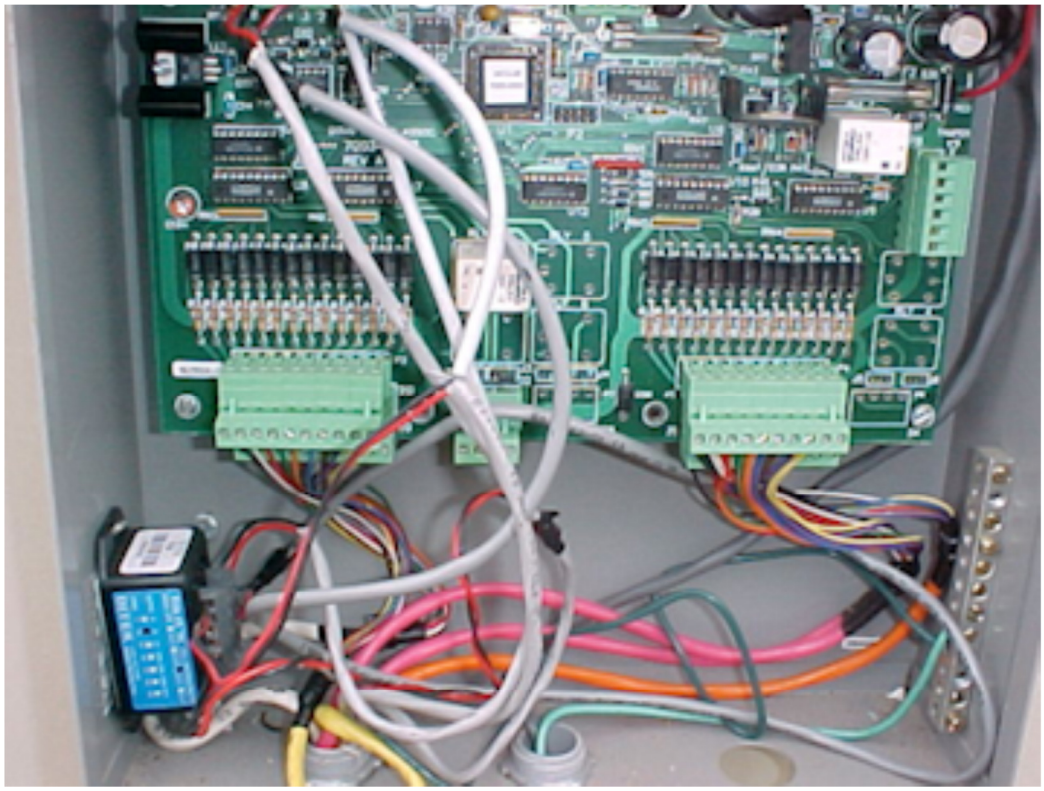
This example shows a LCD keypad used at the entrance, with an LX at the exit. The single gate operator is connected to the entrance keypad. In this case the exit keypad would be set up to activate the relay on the entrance keypad.



The next example shows a system that had a Keypad Expansion MUX at address #6, to plug in a standard keypad being used for in-car elevator control. Also, the system had 3 Door Alarm Muxes addressed as devices 7, 8 and 9. Because the expansion MUX is an older style and does not have a changeable address (see picture on next page), it was replaced with a UniMux and its address moved to #10. In the setups, all items that were assigned to board #6 are changed to board #10.



Below is a picture of an older version of the Keypad Expansion MUX.



Note at the top of the board there is a square chip with a label. This label has the RS485 address of the mux listed on it, and this address is permanently programmed into that chip and cannot be changed. The chips are no longer available.

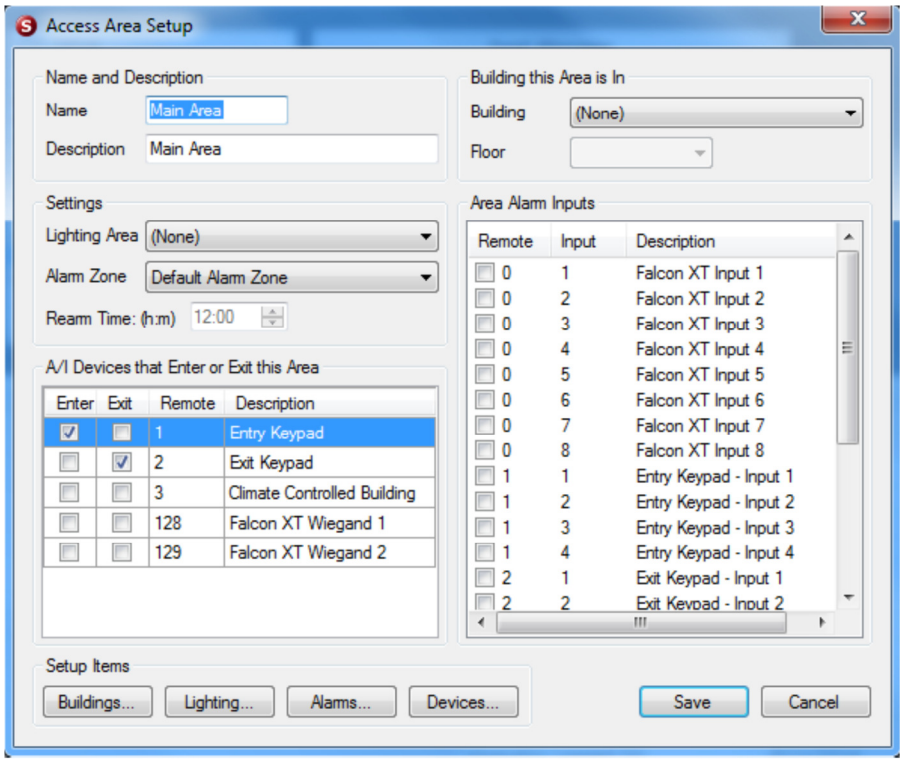
Appendix C: Translating Digigate "Keypad Zones" to StorLogix "Access Areas" and "Access Levels"

In a DigiGate system, a "Keypad Zone" is assigned to each tenant and defines which devices the tenant can use to enter or exit the facility. The corresponding settings in StorLogix are the "Access Area" and "Access Level".

For example, a site may have two keypads at a gate to get in and out of the facility. It also has a keypad at a door to get into a climate controlled building, and only tenants that have a unit inside the building are allowed to use that keypad.

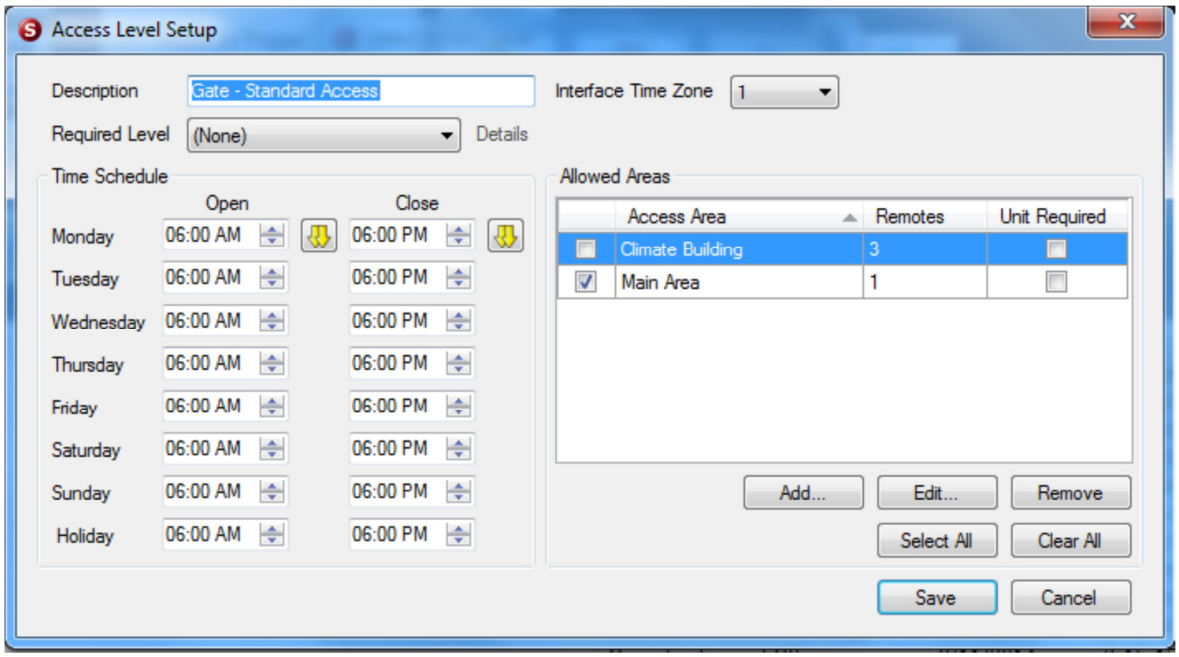
In DigiGate, this situation would result in two Keypad Zones, one would be set up at the Main Area, and have the enter and exit keypad selected. The second one would be set up as the Climate Controlled building, and have all three keypads selected. The tenants would be assigned the area appropriate for the location of their unit. Note that the Time Zone for each tenant is handled separately in DigiGate.

In the StorLogix program, you have two settings that are interlocked together, and then assigned to the tenant. The first is the "Access Area" setup. Below is an example of how the Main Area would be set up in the situation described above.



You can see that the Enter Keypad is selected to “Enter” the area, and the exit keypad to “Exit”. For our example site, a second Access Area would be added to the setups, that has the Climate Controlled Building keypad set to “Enter” the area.

After these items are set up, the Access Levels will need to be added. An Access Level combines the Access Area with a time of day setting, to show both when and where a tenant assigned that level can access the facility. Below is an example of an Access Level for the Main Area with standard operating hours of 6 AM to 6 PM.



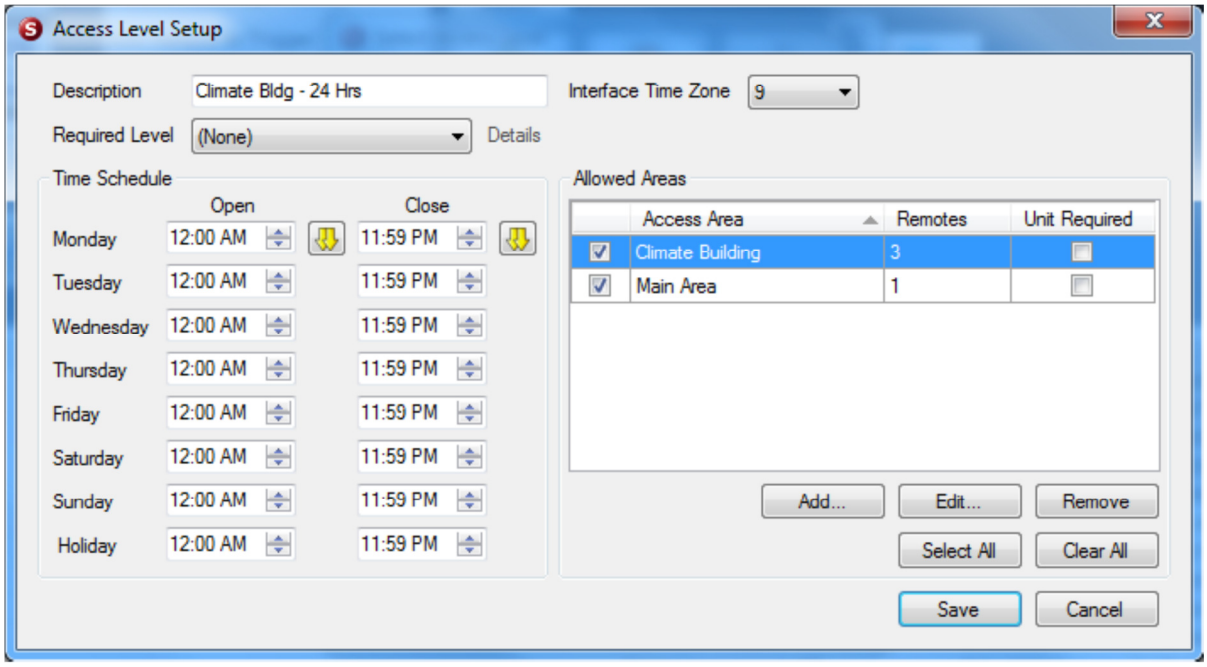
Note that the “Main Area” box is selected in the “Allowed Areas” list. This specifies that a tenant assigned this Access Level can use keypads assigned to this area only.

Also note the “Interface Time Zone” setting. This is the value sent by any Management application to StorLogix, that defines the Access Level assigned to a tenant. This should be noted so that this value can be correctly assigned to the tenant in that application.

Lastly, note the “Time Schedule” for the level. This is the hours of each day that the tenant can use the keypads to enter the facility[1]. In the example above the tenant would be allowed to use the gate keypads from 6AM until 6PM each day.

[1] Exiting the facility is handled by the “Late Exit” global setting in the “Falcon XT Setup” menu item. The default setting is that the keypads stop allowing exit at the “Close” time.

Below is an example of how an Access Level would be set up to allow a tenant access to the climate building, with a 24 hour a day time zone.



A tenant assigned this level would be allowed to use both the keypads at the gate, in addition to the keypad into the building, at any time of day.

Appendix D: Testing the System

After installation and setup has been completed, the system should be tested to ensure proper operation. Because of the wide variety of system configurations, these instructions are written to cover general testing and are not specific to a particular site.

1. Use your management application to download all of your tenants and their access codes into StorLogix.

2. Select some valid user codes and try them at each access control device. Make sure that the code is accepted and the controlled device is activated. Depending on the equipment used at your facility, this may also involve testing card readers or remote controls.

3. Change the close time for your Time Schedule to a time earlier than the current PC time and test codes to see that they are prevented from entering. Reset the schedule close time back to the correct time after this test.

4. Verify that the Event Log in StorLogix updates with the correct information for the codes that were used, and the access device that was used.

5. Select a tenant code that is suspended and verify that the access device does not allow entry when this code is used.

6. If your site has door alarms, open several vacant units and verify that the alarms are activated and that the Event Log shows the correct units.

7. If your site has an optional DigiGraphics display, verify that the display shows the units with the correct status (i.e. vacant, rented or delinquent). If equipped with door alarms, the graphics should also show alarm status when a unit is opened without entering an access code.