PROTEGE

AN-087

BACnet/IP Service

Protégé Integrated System Controller BACnet/IP
Annex J Integration Application Note

31 July 2010

ICT

PUBLICATION INFORMATION

This application note covers the use of the protégé system in a particular configuration and may be used in conjunction with other publications. Specifications may change without notice, for updates visit the Integrated Control Technology website at www.integratedcontroltechnology.com.

CONTENTS

PROTÉGÉ SYSTEM

Introduction

The Protégé System is a powerful integrated alarm and access control management system designed to provide integration with building automation, apartment complex control and HVAC in one flexible package. Communicating through a proprietary high speed protocol across an encrypted local area network and AES Encrypted Proprietary RS-485 module network using modular-based hardware design, system installers have the flexibility to accommodate any installation from small or large, residential or commercial.

Application Note Information

This application note explains the operation of the Protege System Controller when communicating on a BACnet/IP Annex J network. This application note details the connectivity and should be read in conjunction with the PICS statement for the BACnet/IP implementation located on the Integrated Control Technology website

The Protege system can be configured to operate using a number of Protocols and Port Ranges providing many variations to the information provided here. Where possible the author has attempted to keep the IP and Port configurations as default however in most cases these are changed to suit the networking environment the devices are installed on.

Default port used for BACnet/IP communication is UDP/IP 47808 and it is recommended not to change this unless your BACnet/IP network is not standard.

Software Application Version

This application note has been tested with version 2.08 Build 3057 or higher of the controller firmware although the configuration parameters are relevant to versions 2.08 3025/3026. The Protégé System Management Suite User Interface and Server should be Release 449 or higher to take advantage of the configuration parameters.

Hardware Requirements

BACnet/IP is only supported on the SE and GX controllers. The LE panel does not have the BACnet/IP Stack protocols included and can not be used for BACnet/IP integration.

Third Party Software Applications

This application note uses the following products:

- Topserver BACnet to OPC application from Software Toolbox which can be obtained from the vendors website www.softwaretoolbox.com you can download the demo application from http://www.toolboxopc.com/Features/Demo/demo.shtml and it is recommended to only install the Modbus and BACnet components.

- Cimetrics BACnet Explorer the demo version of this application allows you to browse all discoverable devices in the BACnet network and view the appropriate properties.

- Visual Test Shell is a validation suite used to verify a BACnet/IP device and can be used to control the BACnet/IP stack in Protégé however this is a very technical application that is not recommended for general operation.

More information on the BACnet/IP stack, vendor information, documents and a significant amount of data can be obtained from the ASHARE website. You can view the website at www.ashare.org

Linking BACnet/IP and Protege

The BACnet/IP service allows BACnet/IP networks to interact with objects within the Protege System Controller. The Protege System Controller is not a PLC and does not have many of the physical properties that a PLC has rather it is made up of many dynamic objects such as Automation Points, Doors, Programmable Inputs (Zones) and Programmable Outputs (PGMS).

The BACnet/IP service presents 250 binary values that can be controlled by the BACnet/IP system that it is connected. This allows the integration to have a demarcation point that will then let the security professional program the functions on their side and equally allow the BACnet/IP administrator program the relating devices on their side of the integration.

The relationship between the BACnet/IP objects that are presented to other devices on the BACnet/IP network is shown in the following diagram.

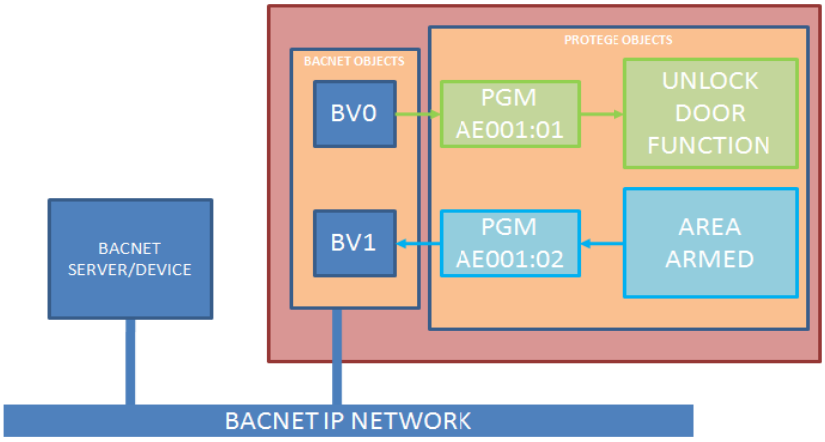


Figure 1 – BACnet/IP Object Relationship

In the later part of this document an example is shown of how to arm an area and also how to show the status of the area using the binary values and linking as shown above. These examples feature heavy use of the programmable functions built into the Protege System Controllers.

As shown above using the BV0 object and setting the BACnet/IP service to link to the AE001:01 PGM which is used as a virtual PGM the Present Value status of the BinaryValue0 will be reflected in the PGM status.

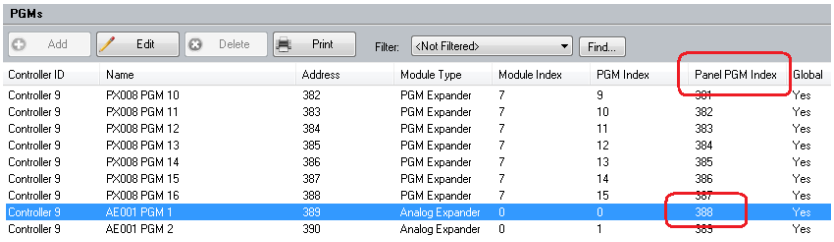
The PGM could be seen as a register in the Protege System that is used to bind functions and status messages to the BACnet/IP object. Performing an action on the Binary Value changes the PGM status and performing an action on the PGM changes the Binary Value status.

BACnet/IP Service Start PGM

The start PGM that is programmed in the following section is the PGM panel index and this here is important as the index is used to link the first PGM to the first binary value tag in BACnet/IP for example it is very unlikely you will use 00000, the simple reason is that the 00000 index is the bell PGM output and it will most likely be used.

It is more typical to link the index to a group of PGM's located on modules that are not registered (virtual PGM's). In most cases the last block on the analog expanders or the output expanders.

In the first configuration you will see we use 0 this allows the demo to show CP001:01 and then in the later part of the document we use AE001:01 so the start PGM needs to be changed to 388 based on a standard profile.



BACNET/IP SERVICE CONFIGURATION

Introduction

The BACnet/IP service has few configuration properties and only needs the IP Port and Device Instance programmed to operate with the start and end range of PGM's that link the binary values with the Protégé System.

BACnet/IP Service Programming - Keypad

In the example below we will use Service 005 however any service can be used. Using Service 001 or Service 004 may limit connectivity to other applications.

Enter user code: ******	Login to the LCD keypad using the installer login user code or a suitable code that has been programmed with the Menu 4 access to the system.
Service to modify: SV005	Go to the service programming settings by selecting the Service Programming Menu. Press **[MENU, 4, 7, 1]**. The display will show you the first service, scroll up to service 005 or enter 005 on the numeric keys.
SV005 State Halted	Make sure the display shows Halted, if it shows running press the **[2]** key to halt the service. Press the **[ENTER]** key to move to the next screen.
SV005 Ser Type BACnet/IP	Press the **[1]** key until the service type shows the BACnet/IP Service then press the **[ENTER]** key to move to the next screen.
SV005 Ser Mode Start with O/S	Press the **[1]** key to change the start up mode to Start with O/S then press the **[ENTER]** key to move to the next screen.
SV005 Primary Port: 47808	Use the numerical keys to enter the primary port for BACnet/IP communications. In our example we are using the default port 47808. Press the **[ENTER]** key to move to the next screen.
SV005 Device ID: 0000115C	The Device ID is entered in HEX. In our example we are using 115C or 4444 decimal. Press the **[ENTER]** key to move to the next screen.
SV005 Start PGM no: 00000	Use the keypad to enter the PGM number to begin the binding of the binary values to. The default of CP001:01 will be used but should be changed to a PGM that is not used on

a physical device however we are using this to test the integration so we have left it set at CP001:01 Press the **[ENTER]** key to move to the next screen. See the previous chapter regarding the start PGM.

SV005 Total PGM
no: 00008

Use the keypad to enter the number of PGMs to allow the BACnet/IP service to control this allows the installer to restrict the PGM's that will be controlled. The BACnet/IP interface will still receive 250 objects regardless of this setting.

Start The BACnet/IP Service

Once you have programmed the above setting return to the service state screen and press the **[1]** key to start the service, the service state should change to running and an event is logged in the review.

BACnet/IP Service Programming – Management Suite

In the example below we will use Service 006 however any service can be used. Using Service 001 or Service 004 may limit connectivity to other applications. Ensure the operator that you are logging in with has access to the administration menu's.

BACnet/IP programming from the Protege System Management Suite is not available in the current release version. The September 2010 release will have this available and the following section updated.

TOPSERVER BACNET/IP INTEGRATION

Introduction

The following shows how to connect to the Protege System Controller to the Topserver OPC Automation server and communicate using BACnet/IP. Topserver is a third party application used to exercise the BACnet/IP control functions and in demo mode will operate for 2 hours. This can be downloaded from the Topserver Website.

The configuration of the Topserver settings for the channel and device are important and should be carefully followed to ensure the correct operation of the system.

Topserver uses IP and networking and firewalls, user access control and other windows security features will interfere with the operation and should have exceptions loaded as required. You must allow communication on the BACnet/IP port 47808/UDP.

Topserver BACnet/IP Configuration

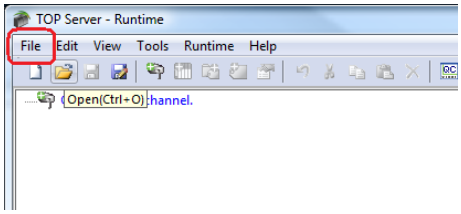
Because the way that BACnet/IP can scan for the objects that are available in a device it is easy to get the objects that are available in the controller and import these as useable tags however this will create a huge tag database that will be very slow. The most important values for the operation of the system is the Present Value for the object.

The project files are specific to the Topserver Application however the tag databases included with the application note are available independently and can be imported in to any suitable application, they are provided in CSV format and are specific for version 5.0 or higher of Topserver.

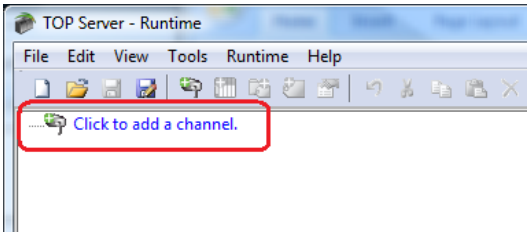
Adding A BACnet/IP Channel

Now it is time to get connected with Top Server, make sure that you have started the BACnet/IP service in the previous chapter and it is running. Once you have confirmed this follow the steps below ensuring your screen shows a similar set of information.

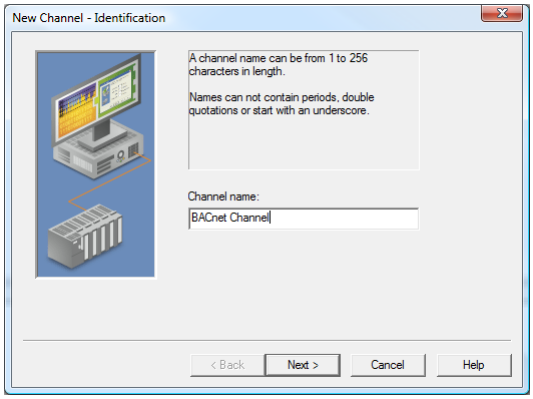
1. Start the topserver application by browsing to the location from your start menu and selecting the topserver application. If this is the first time you have started topserver then it will show by default the sample application project.
2. Select the file menu and then select new from the file menu.



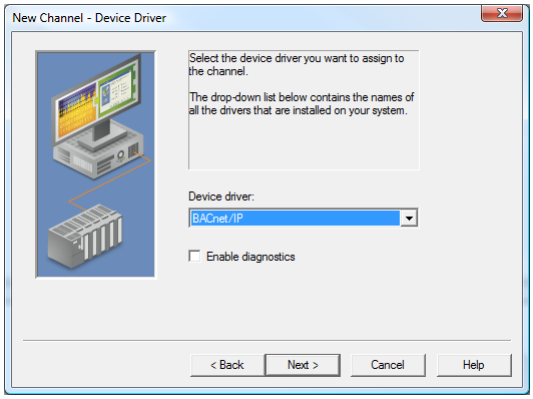
3. Select the text “Click to add channel”. This will add a communications channel to the Topserver that will allow you to talk BACnet/IP.



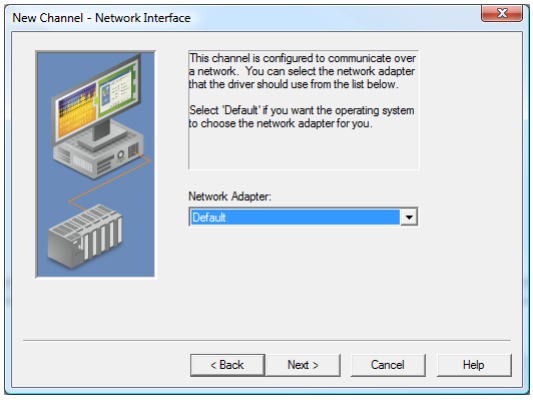
4. Once you have selected the add channel you will be asked to give the channel a name in our example we have used BACnet/IP Channel.



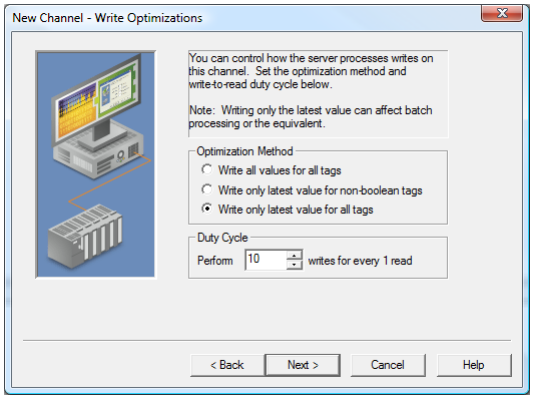
5. Select the next button and then select the BACnet/IP driver from the drop down list. If you do not see this re-run the installation and select BACnet/IP as one of the communication driver options.



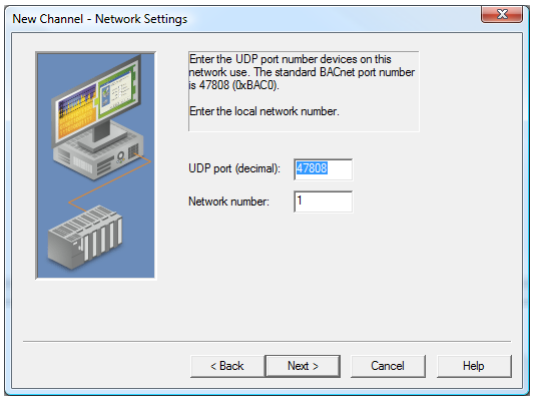
6. The next screen selects your network adapter. If you have more than one operating on the machine then select the one that you have connected the controller to and then select the next button.



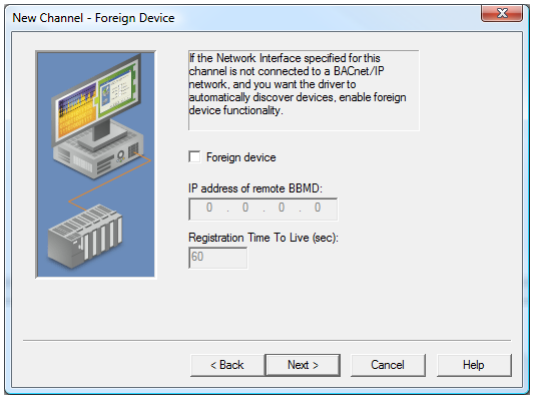
7. The following screens setup many default parameters and should be left at the default configuration values. If you are an experienced BACnet/IP or automation engineer you may want to optimize these configuration files however support is beyond the scope of this application note.



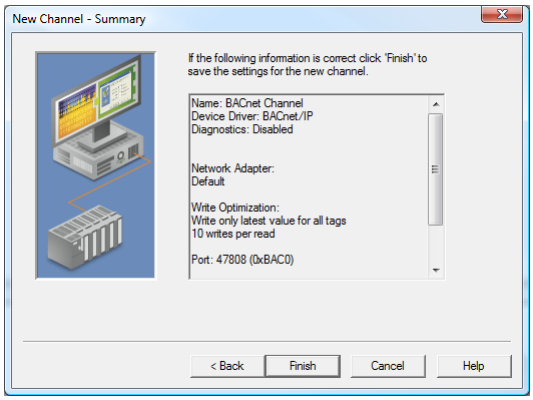
8. Default BACnet/IP port number and the network number should be left at default for this application note operate, if you change the port you must also change the service on the controller.



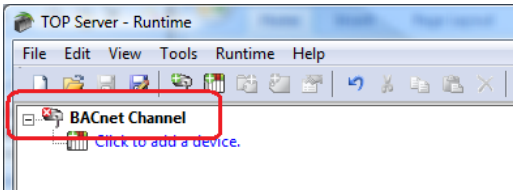
9. The next screen should be left at default and not changed.



10. Click the finish button and the BACnet/IP Channel will be configured and saved. You can adjust these parameters at any time by right clicking the channel and selecting properties.



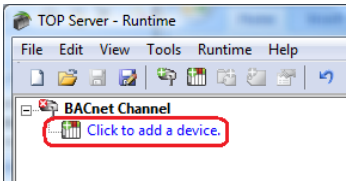
You will now see the channel name in the left side of the top server window. Once this is complete you need to add the Protege Device in the following steps.



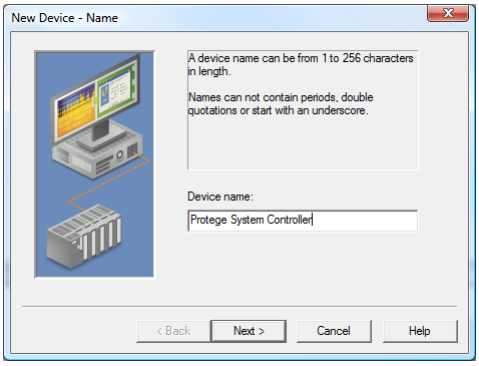
Adding A BACnet/IP Device

A device communicates on a channel. To communicate to the BACnet/IP device you add it to the channel and configure the parameters.

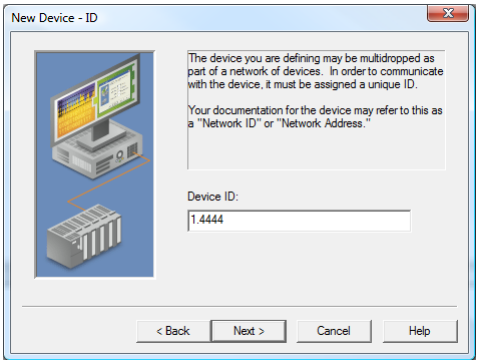
1. Select the 'Click to add device to channel' text that is shown under the channel name we just added in the previous chapter.



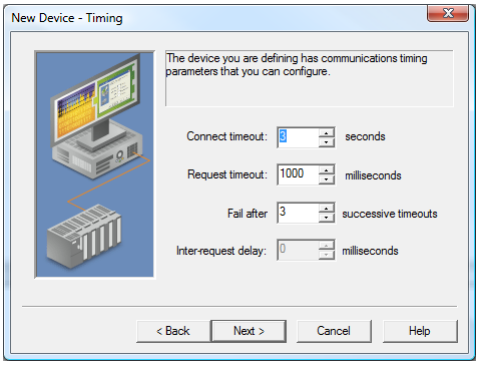
2. There is now a fairly lengthy series of configuration parameters for your device and these must be entered exactly as shown. If your service for BACnet/IP differs from the default you will need to adjust the settings accordingly. Enter the name of the device you are adding.



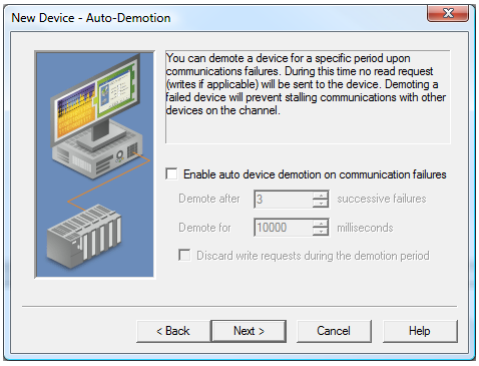
3. Click the next button and then enter the instance of the device and the address. The instance can be thought of as an address or a unique way of contacting the device over BACnet/IP. The default instance is 4444 (115C Hexadecimal).



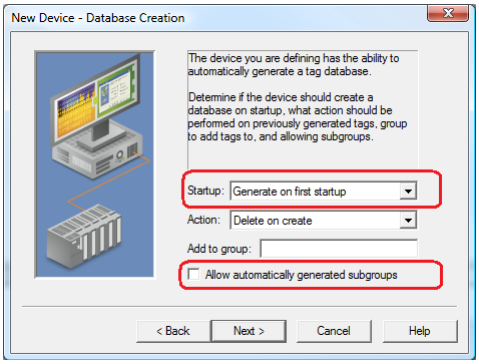
4. Select next and leave the connection timeout and communication settings for the device at default.



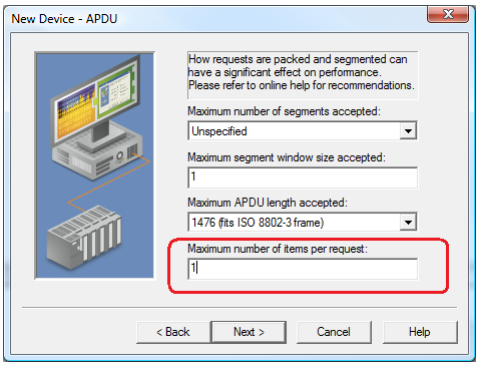
5. Leave auto-demotion disabled.



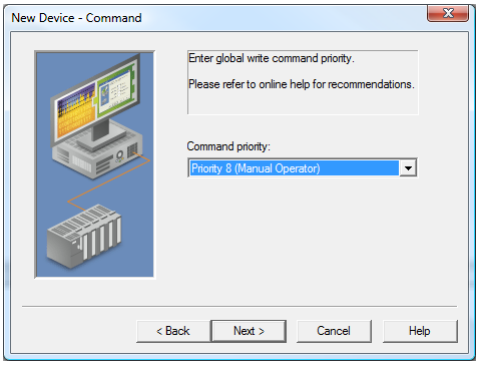
6. Select next. To get the tags automatically from the controller you must specify that you want them generated on first start up. We recommend not to have automatically generated sub groups as this creates a layer and may confuse the application note so disable this option.



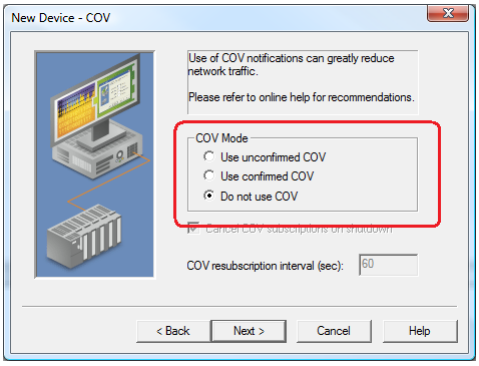
7. The controller has limited resources to allow large packets of data. You must select the single request per packet option by changing the default value of 16 to 1.



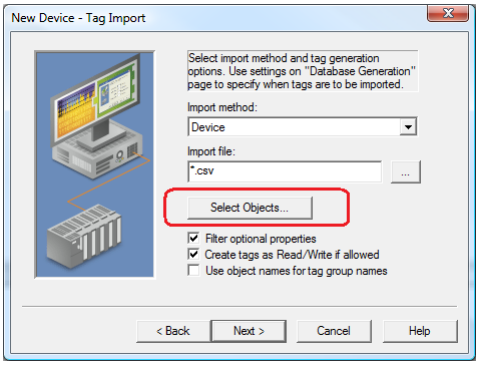
8. Manual control will be done with a priority 8 this can be left at default.



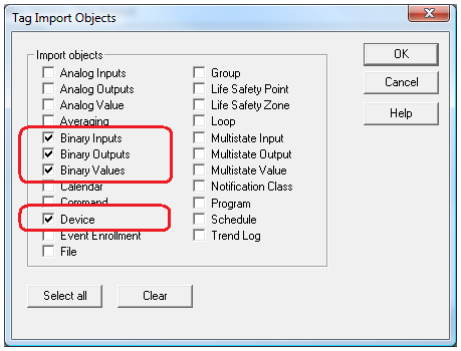
9. The controller does not support COV (Change of Value) at this point in time and must be disabled.



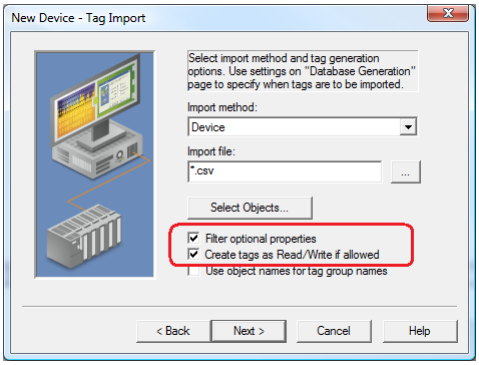
10. This section allows the import of the tags in to the system. Select the “Select Objects” from the screen this will open the next window following.



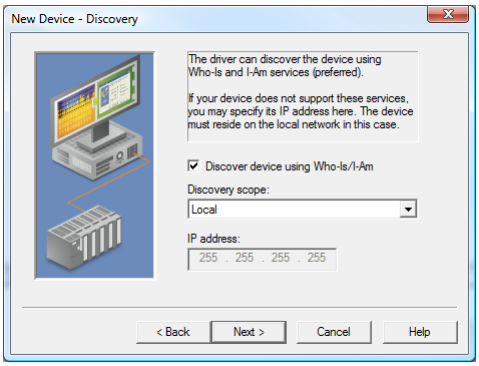
11. From the next window select the Binary objects and the Device Object.



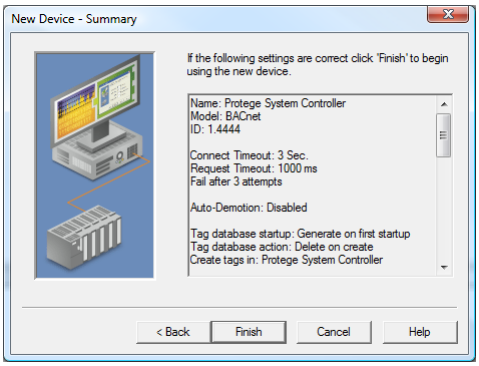
12. Select the OK button then complete the extra options below.



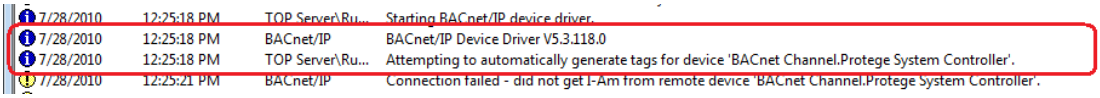
13. Select next and leave the option below as default.



14. You have now configured your Protege System Controller device.

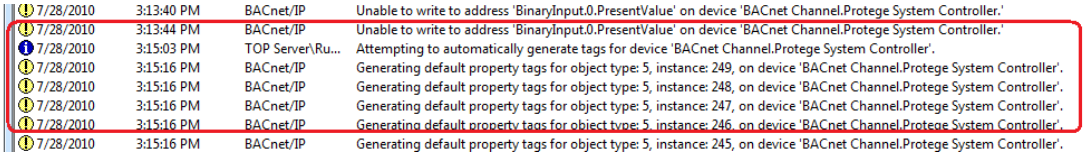


15. Select Finish and the system should then proceed to attempt communication with the System Controller. You will see the event in the system as shown below.

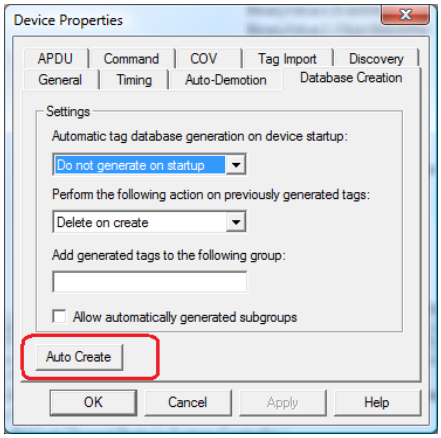


In the case above the controller was not online and you get a time out after 3 seconds which is expected if the controller is not connected. If this happens right click on the Topserver administration server and select reinitialise and verify that the firewall and other items are not blocking the commands.

If you are having difficulty getting the controller online then download Wireshark and view the network traffic. Wireshark has a built in BACnet/IP dissector so packets can easily be seen.



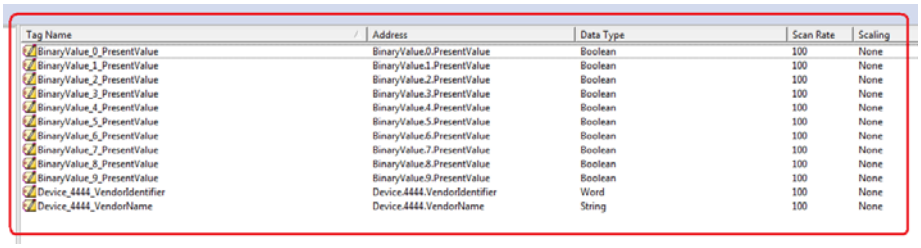
When the system is operational you will see events similar to the above as it begins to populate the tag database. If the system does not find the tags you can select the properties of the device and select auto create as shown below.



When importing tags you should import 250 binary values these link to the associated PGM that you have set in the service (PGM Start = BinaryValue0).

Writing Bell PGM Output 1

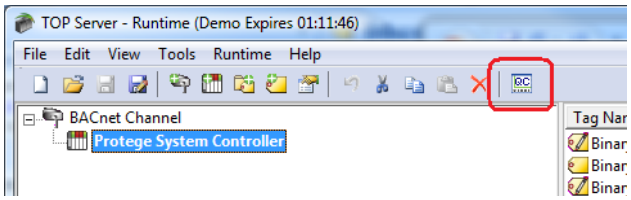
Once you have the tags in the system you will be able to control or write to the outputs on the Protege System Controller from the BACnet/IP device. To do this with Topserver you must open an OPC client and then control the Binary Value associated with the PGM that is to be controlled. Topserver includes a “Quick” OPC client that allows you to exercise your device.



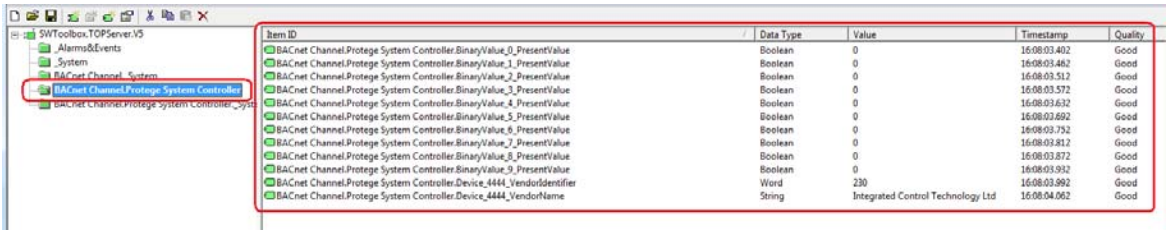
The tag database shown in these examples (above) has all the extra properties deleted. Nearly all the tags are not required with the exception of the Present Value. This reduction in the number of tags also means the objects respond quickly as you do not need to scan every property value. In the example we have also retained Integrated Control Technology Vendor ID (230) and Vendor Name from the Device object.

Not a requirement but recommended. It can take up to 15 seconds to update a tag on a very large database.

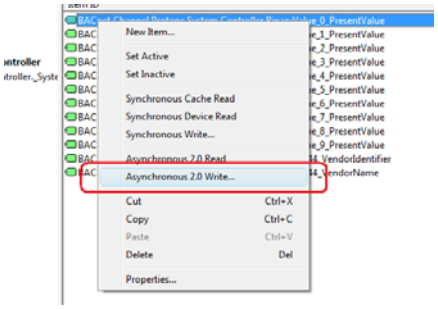
1. Select the OPC quick client button as shown below. This opens another window with the tags in it from the project and it will begin scanning the tags on the controller.



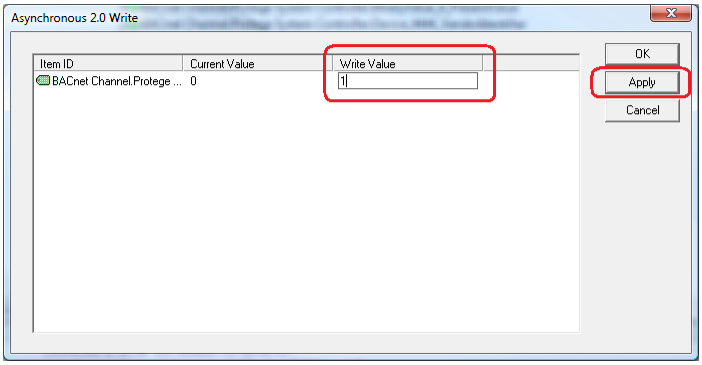
2. When you open the OPC quick client you will get the current tag database listed under the device. Shown below is the example with the smaller tag database. If you have left this at default then there are over 1000 tags and it will take at least 20-40 seconds for the system to scan them and the quality of the data to turn to “Good”.



3. Turning on the Binary Value will result in the associated PGM on the controller turning on. To turn it on a write is performed on the Present Value, right click the binary value to control. The example will use BV0 as this links to CP001:01 on our demo system.

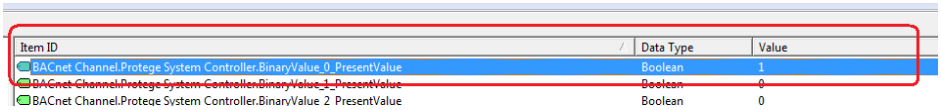


4. Select the option above called Asynchronous Write this will open a new window with the variable. Select the value option and enter 1, then select apply.



Asynchronous Write means that the variable (BV0) will be written between the reads of the other variables and results in a very fast response time, this is related to the Topserver configuration not the BACnet/IP protocol.

Once you select apply the command is sent over BACnet/IP to the controller and the controller will activate the PGM output. If you click OK you will see now the value is updated in the list of Objects in the OPC client as well.



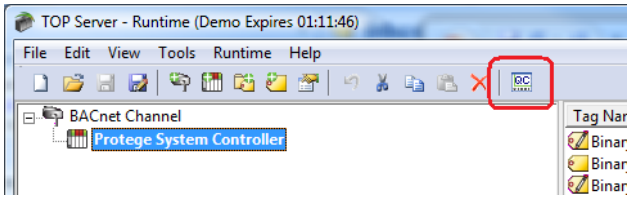
The example shown using Topserver can be done using any BACnet/IP device that can change the property of another device. In most cases this is the Building Management Server or a Building Controller. Although the programming for systems other than Topserver will be different the principles shown throughout this application note will apply.

Reading Bell PGM Output 1

Once you have the tags in the system you have most likely noticed that when you open the Quick Client OPC window the physical status of the outputs is shown. This is because when we configured Topserver we told it to scan the objects every 100 milliseconds which is the default.

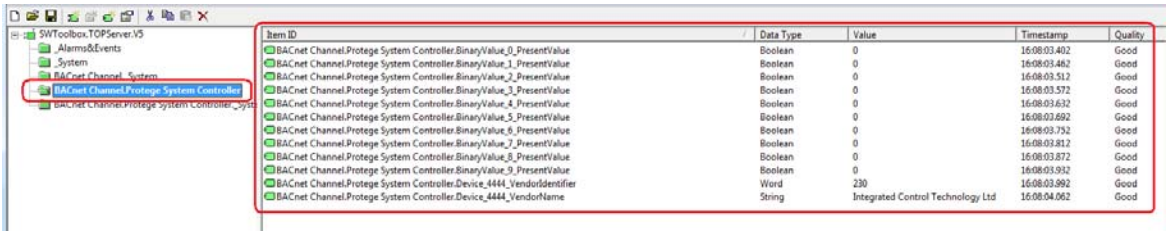
To read the variables you can perform the same as the write using the Asynchronous Read option however if you have reduced the number of tags as we have in our example it should update without the need to force it.

1. Select the OPC quick client button as shown below. This opens another window with the tags in it from the project and it will begin scanning the tags on the controller.



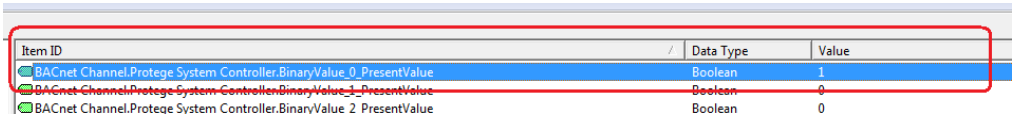
2. When you open the OPC quick client you will get the current tag database listed under the device. Shown below is the example with the smaller tag database. If you have left

this at default there are over 1000 tags and it will take at least 20-40 seconds for the quality of the data to turn to “Good”.



3. Now to show the reading of the BV0 we simply need to control the PGM on our system. Essentially the BVO is using the PGM as the internal register and this is the “Link” between the BACnet/IP Objects and the Protege System Controller Objects.

   Login to the keypad using the installer code and then select MENU, 4, 8, 2, 3 this will show the first PGM, press the 1 key to turn it on or the 2 key to turn it off. You will see the status in the OPC quick client as shown below change.



   You can also control the PGM from the Protege System Management Suite by right clicking the PGM and selecting activate or deactivate. You can also attach the PGM to a floor plan. Controlling the object from the automation system, the controller or the Protege Software allows transparent operation.

CONTROLLING AREAS

Introduction

The following programming shows how a BACnet/IP application can control the arming and disarming of an area so it follows the status of a Binary Value that is linked to a PGM in the Protege System.

In many cases the follow function is not viable because an area may need to be controlled from another source (keypad, touch screen or reader). It may also be required that there is an arm coil and a disarm coil so that if either of these are activated that the area will arm or disarm but will also allow the area to be controlled by a user on a keypad, touch screen or card reader.

This section will cover programming from the Protege System Management Suite only and will not show keypad programming.

The PGM's used for the following exercise will be AE001:01 and AE001:02 these are commonly spare unless analog expanders are used.

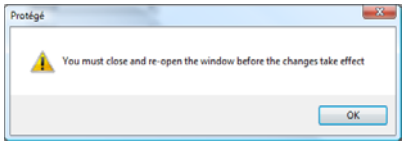
Programmable functions are used extensively in the following examples to link the BACnet/IP Binary Value and PGM being controlled to the resulting activation in the area. It is recommended that the section in the Protege Controller Reference Manual and the Online help system is reviewed in detail with regards to the use of Programmable Functions.

Area Follows PGM Status

When an area is used in a programmable function in the follow state the area will 'Follow' the PGM it is linked to, this will mean that any changes in the PGM will be mimicked by the area. Any changes to the area status (Disarm or Arm from a keypad) will be effective until the programmable function checks the state of the area against the PGM (approximately 30 seconds). In many cases this is not the desired action. If external control is also required please see the area pulse on arming and area pulse on disarming. This allows the area to be controlled by two PGMs each having a specific function (Arming or Disarming).

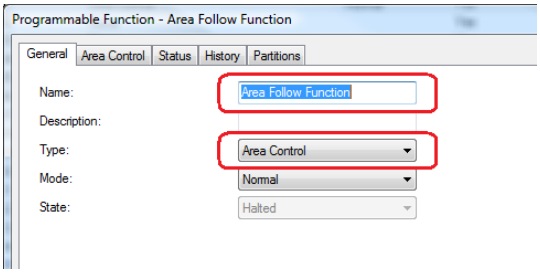
Open the Protege System Management Suite. Select the communications tab and connect to your controller.

1. From the controller tab select the programmable functions. In this example we will use programmable function 1 for the follow arming to arm area 1 and programmable function 2 and 3 for the pulse on/off arming of area 2. DO NOT USE AREA 1 for both programmable functions as they will not work and the programmable functions will interfere with the area control as explained above.

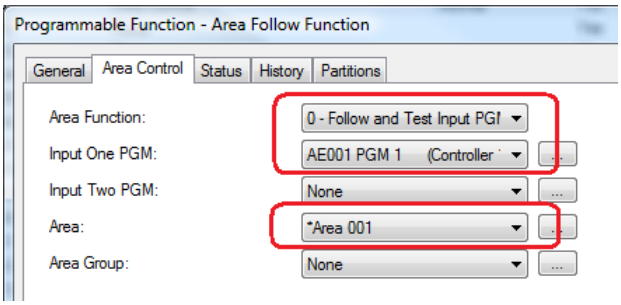


2. Select the first programmable function. Change the type to '*Area Control*' and select the OK button, you will be prompted by the software to close the screen, this allows the system to redraw the configuration settings. Once this is completed open the programmable function again.

3. When you open the function again you will see the Area Control tab is now available. Before selecting the tab complete the name with a descriptive name of the programmable functions action.

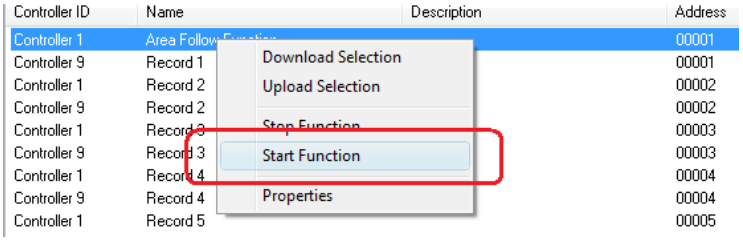


4. Select the Area Control tab as shown and complete the configuration parameters below ensuring that Input Two PGM and Area Group are set to NONE.



Once you have completed the programming select the OK button.

5. Once the programming for the function is completed you need to start the function. Starting a function allows the PLC processing that is internal to the controller to run the programmed settings, much like running a program, once it is run it will remain running until it is stopped and will automatically be started if it was stopped when the controller is restarted for any reason.

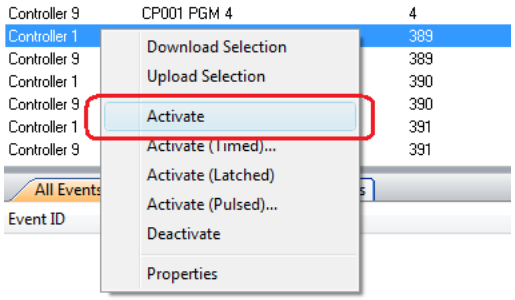


Start the Programmable Function by right clicking the function from the list and select start function.

Once you have started a programmable function YOU CAN NOT edit the settings in the controller and must STOP the function download any changes and then restart the function.

Testing Your Programming

Once you have your programmable function running successfully you will be able to test the operation very easily by controlling the PGM you have used (AE001:01) for the Input PGM One in the programmable function.



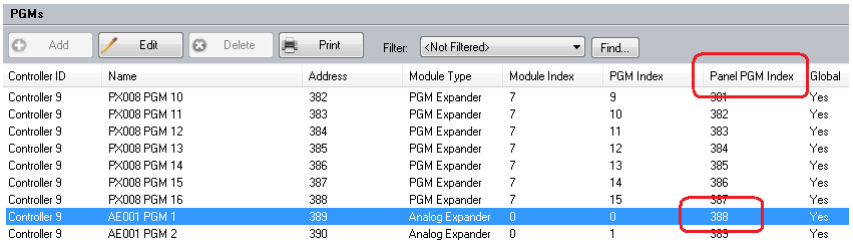
Select the controller tab and then PGMs from the Doors, Zones and PGM's icon. From the PGM programming list right click on the AE001:01 PGM and select activate. You will see that your area will begin to arm a short time later. Allow the area to complete the arming cycle and then select deactivate from the menu and you will observe the area begin a disarm cycle.

It is recommended that when you are testing to select the Log Events option in the PGM configuration that will allow the activation and deactivation of a PGM to be presented in the event window.

Testing From BACnet/IP

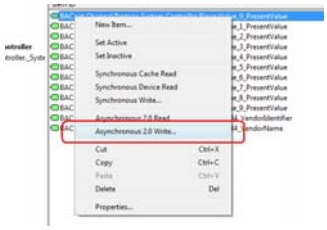
Once you have completed the internal tests on the PGM as shown previous you can now link this to the BACnet/IP interface that you programmed previously however you will need to change the settings in the BACnet/IP service to link to AE001:01.

To change your start PGM it should be set to the Panel Index for the PGM you want. In the examples this needs to be 388 this is the physical or internal address to link the PGM to and to find any PGM address you look this up in the software, see below.

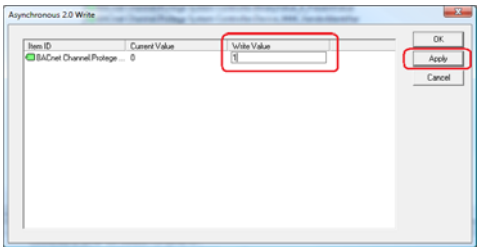


It is recommended that when you are testing to select the Log Events option in the PGM configuration you will see the PGM state change with the appropriate event log being generated.

1. To control the output AE001:01. Right click on the tag in the item window that is labelled '*BACnetChannel.ProtegeSystemController.BinaryValue.0.PresentValue*' this will provide you a menu and select asynchronous write from the context menu. This will open the next window as shown below.



2. Once this is open you can select the Write Value location and put a one. You can then select the apply button which will 'Write' this value to the Modbus register in the Protege System Controller which will in turn send this to the PGM output. You should now also see your area change state from Disarmed to Armed.



3. As you can see in the next window when you write to the output the current value changes this is because the system reads back the value so you are able to see the status.

You should now be able to control the output that controls the area using the programmable function allowing any BACnet enabled device to control the area, this could be from the front screen of the Building Automation System or from a PLC or device.

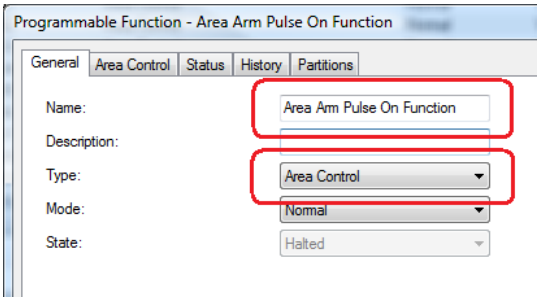
You can obtain the status of the area by reading a Binary Value that is linked to the disarmed PGM.

Area Arm On Pulse PGM

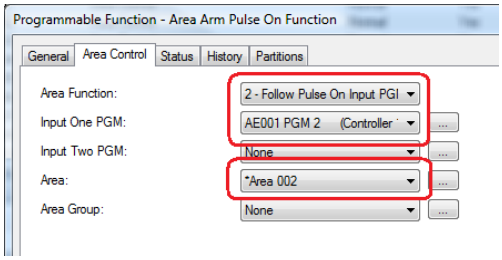
The following two programmable function assignments allow you to control the area from two separate PGM's. One used to arm the Area and the other used to disarm the Area. Activating either one when it is in the resulting state will yield no change in the area status. This level of control is ideal for when an area needs to be controlled from the Modbus system using an operator panel.

Open the Protege System Management Suite. Select the communications tab and connect to your controller.

1. From the controller tab select the programmable functions. In this example we will use programmable function 2 for the pulse on arming to arm Area 2 and programmable function 3 for the pulse on disarming. **DO NOT USE AREA 1** for both programmable functions as they will not work and the programmable functions will interfere with the area control.

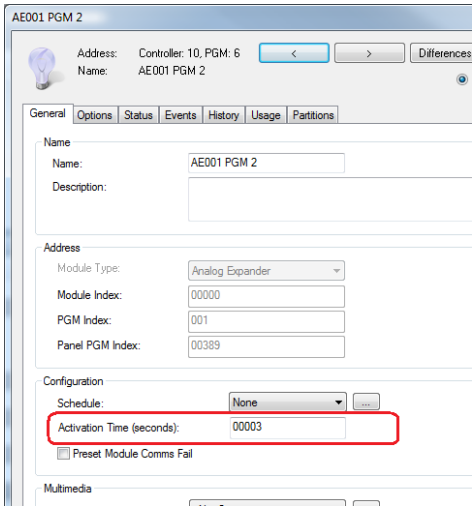


2. Follow the steps to add a new function as shown in the previous section. In this example we have named this Arm Pulse On. Complete the entries above paying special attention to the function which is Follow Pulse On Input PGM meaning that the area will arm (turn on) when the PGM turns on but perform no action when the PGM turns off, this is commonly referred to as edge control.



3. Once programmed select ok and start the function as shown in the previous example.

4. Now before you test your application open the PGM output AE001:02 and change the activation time to 3 seconds. This will mean that when you arm the area the pgm will only turn on for this period of time allowing you to turn it on again to re-activate an arming cycle.

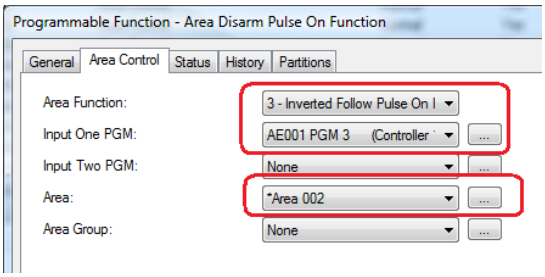


Now test your configuration by activating the PGM using the timed option from the menu for 3 seconds. If you programming is correct the area will arm however when the PGM deactivates the area will remain armed. To disarm the area see the following section.

Area Disarm On Pulse PGM

The disarm programming is once again another programmable function however the operation is inverted. Instead of arming the area the function needs to disarm the area when the PGM is activated.

1. From the controller tab select the programmable functions. In this example we will use programmable function 3 for the pulse on disarming to disarm area 2. Area 2 should only be assigned to programmable function 2 and 3.



2. Follow the steps to add a new function as shown in the previous section. In this example we have named this Area Disarm Pulse On. Complete the entries above paying special attention to the function which is Inverted Follow Pulse On Input PGM meaning that the area will arm (turn on) when the PGM turns on.

3. Once programmed select ok and start the function as shown in the previous example.

4. Now before you test your application open the PGM output AE001:03 and change the activation time to 3 seconds. This will mean that when you arm the area the PGM will only turn on for this period of time allowing you to turn it on again to re-activate an arming cycle.

Now test your configuration by activating the PGM using the timed option from the menu for 3 seconds. If you programming is correct the area will Disarm however when the PGM deactivates will remain Disarmed. Ensure the area is already armed.

INFORMATION

Introduction

Application notes are provided as is without any implied warranty or intended use and are written by Integrated Control Technology as an aid in programming and connecting devices to the Protégé System.

Contact

Integrated Control Technology welcomes all feedback. Please visit our website or use the information below.

Integrated Control Technology
P.O. Box 302-340
North Harbour Post Centre
Auckland
New Zealand

11 Canaveral Drive
Albany
North Shore City
Auckland
New Zealand

Phone: +64-9-476-7124
Fax: +64-9-476-7128

www.incontrol.co.nz

Integrated Control Technology Limited
11 Canaveral Drive
Albany
Auckland
New Zealand

www.incontrol.co.nz