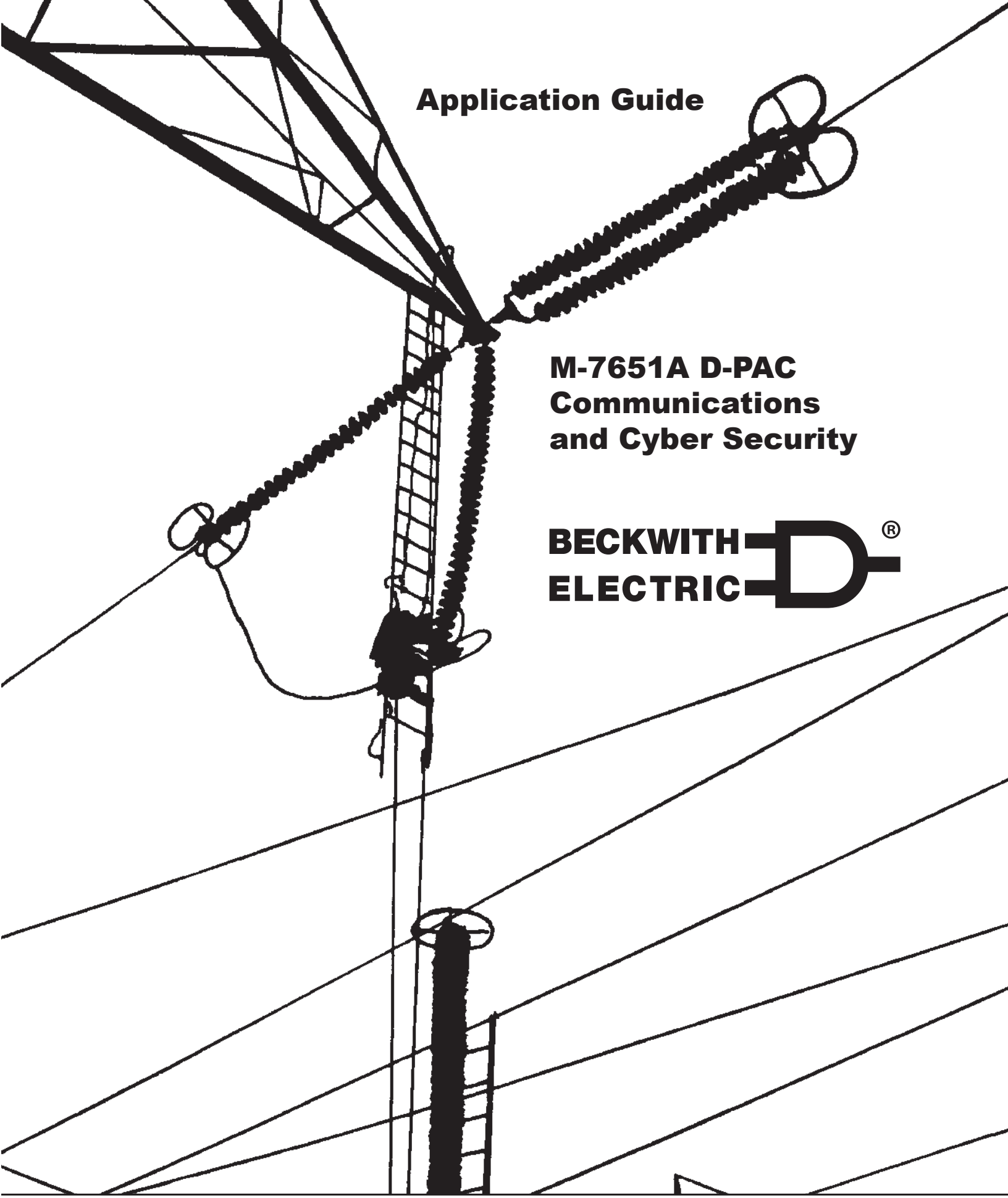
Application Guide



M-7651A D-PAC Communications and Cyber Security

BECKWITH ELECTRIC®

HUBBELL®

A proud member of the Hubbell family.

TRADEMARKS

All brand or product names referenced in this document may be trademarks or registered trademarks of their respective holders.

THIRD PARTY OPEN SOURCE CODE COPYRIGHTS

lwIP (lightweight IP) – lwIP is a widely used open-source TCP/IP stack designed for embedded systems.

Copyright © 2001, 2002. Author/Contributor: Adam Dunkels, *adam@sics.se*.

No Warranty. Software is provided "**AS IS**". No implied warranties available including merchantability & fitness for a particular purpose. Beckwith Electric, a subsidiary of Hubbell Power Systems, Inc. is solely responsible for determining the appropriateness of using or redistributing the work and assumes any risks associated with its exercise of permissions under this License.

In no event shall the Author be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

Racoon – Racoon is the Internet Key Exchange (IKE) library source code used in IPsec/IKE implementation.

Copyright © 2004, 2005, WIDE Project. All rights reserved.

Copyright © 2004. All rights reserved. Author/Contributor: Emmanuel Dreyfus.

Copyright © 2004, SuSE Linux AG, Nuremberg, Germany. All rights reserved. Author/Contributor: Michal Ludvig, *mludvig@suse.cz*.

Copyright © 1991, 1993. All rights reserved. Author/Contributor: The Regents of the University of California.

Copyright © 1998. Author/Contributor: Todd C. Miller, *Todd.Miller@courtesan.com*.

No Warranty. This Software is provided by the Project and contributors "**AS IS**'' and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed.

In no event shall the Contributor be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

ABC – ABC.exe is a Logic Synthesis and Verification tool used in the IPScom IPSlogic editor.

Copyright ©, The Regents of the University of California. All rights reserved.

Permission is hereby granted, without written agreement and without license or royalty fees, to use, copy, modify, and distribute this software and its documentation for any purpose, provided that the above copyright notice and the following two paragraphs appear in all copies of this software.

In no event shall the University of California be liable to any party for direct, indirect, special, incidental, or consequential damages arising out of the use of this software and its documentation, even if the University of California has been advised of the possibility of such damage.

The University of California specifically disclaims any warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The software provided hereunder is on an "**AS IS**" basis, and the University of California has no obligation to provide maintenance, support, updates, enhancements, or modifications.

The content of this Application Guide is provided for informational use only and is subject to change without notice. Beckwith Electric has approved only the English version of this document.

TABLE OF CONTENTS
M-7651A D-PAC
Communications and Cyber Security

© 2013 Beckwith Electric. All Rights Reserved.

1.0 DNP Configuration Editor

■ CYBER SECURITY NOTE:

When Cyber Security is enabled, access to any feature described in this Section is subject to the Access Permissions Policy as designated by the Security Policy Administrator.

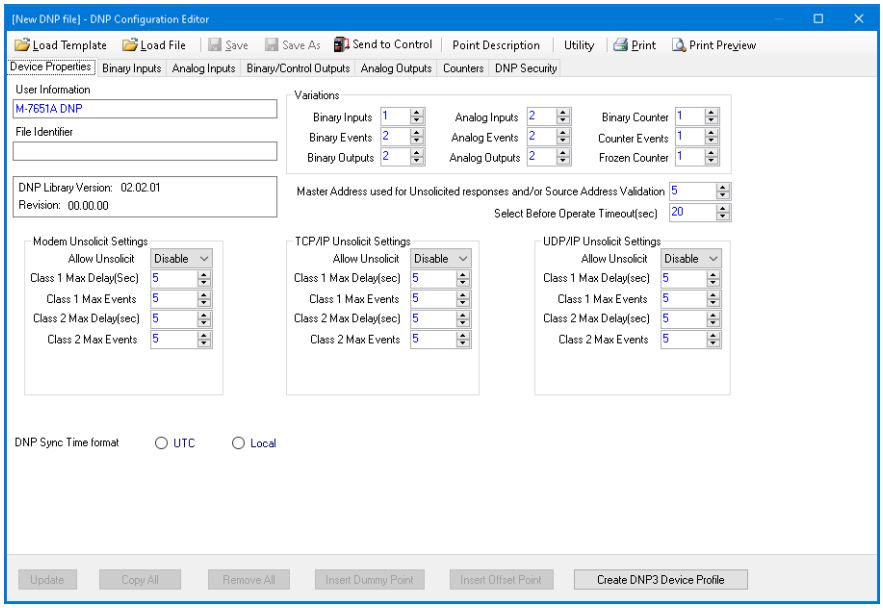


Figure 1-1 DNP Configuration Editor Screen

Variations – The variation of an object gives a different representation of the same data point, such as the size of the object or whether or not the object has flag information. Accordingly, the Variations section will configure listed objects with the desired and supported variations.

Master Address used for Unsolicited responses – This address will be used as the address to send unsolicited responses.

Modem Unsolicit Setting – Applies to TIA-232 interface connected to an Ethernet Modem. TCP/IP and UDP/IP unsolicit settings are used when DNP is being deployed over an Ethernet network.

- Allow Unsolicit: Determines whether unsolicited null responses will be sent when session comes online. If enabled, subsequent unsolicited responses will be enabled through function code 0x14 (Enable unsolicited responses) and disabled through function code 0x15 (Disable unsolicited responses). If "Allow Unsolicit" is disabled, then function codes 0x14 and 0x15 will be responded to with an error.
- Class 1 Max Delay (Sec): If unsolicited responses are enabled, this parameter specifies the maximum amount of time after an event in the corresponding class is received before an unsolicited response will be generated.
- Class 1 Max Events: If unsolicited responses are enabled, the parameter specifies the maximum number of events in the corresponding class to be allowed before an unsolicited response will be generated.
- Class 2 Max Delay (Sec): If unsolicited responses are enabled, this parameter specifies the maximum amount of time after an event in the corresponding class is received before an unsolicited response will be generated.
- Class 2 Max Events: If unsolicited responses are enabled, the parameter specifies the maximum number of events in the corresponding class to be allowed before an unsolicited response will be generated.

DNP Sync Time Format – The user may select the DNP Sync Time as UTC (Universal Time Coordinated), or Local Time. The DNP point value is "0" for UTC, and "1" for Local.

Choosing Points – The Available Points window is populated when a DNP source file is opened. The selection of points from the DNP window tabs can be accomplished by either individually selecting, dragging and dropping points in the Selected Points window or utilizing the "Copy All" feature. The Copy All feature only copies the points in the open tab to the Selected Points window. The "Remove All" feature removes all the points displayed in the Selected Points window for the tab that is open.

Search – The Search fields allow the user to search the Available Points as well as Selected Points for specific terms. Points containing these search terms are listed in numerical order.

Ordering Selected Points – Selected points can be reordered to match the users SCADA, RTU or Master setup by selecting, dragging and dropping the desired point within the Selected Points window.

Adding Dummy Points – The purpose of the Dummy Point is to allow the user to match other device DNP maps that contain points that are not supported in the control. This feature allows the user to communicate with the M-7651A D-PAC control when it is connected to an RTU that contains other brands of controls and eliminates the need to re-configure the RTU or the other controls.

To insert a Dummy point, select **Insert Dummy**. The Dummy Point will be inserted at the end of the Selected Points list. To move the Dummy Point, select, drag and drop the point at the desired location in the Selected Points list. The Dummy point will assume the Index Position and the remaining Selected Points will be modified to accommodate the Dummy Point.

Insert Offset – This allows an offset to be created in the DNP map without the point number being transmitted, thus providing the ability to construct a DNP profile that has non-consecutive point numbers within a group.

Editing Binary Input Points – The Binary Input "Value" and "Mask" values can be edited by double left clicking on the desired point Value or Mask elements. The default value for Value is TRUE, which means that the point will return a High or True when the item being monitored is active in the control. It can be changed to "FALSE" to match a SCADA Master if necessary. The "Mask" value defaults to "CLASS ONE" and defines what polling class type the point is mapped to. The Mask value can also be set to CLASS TWO or THREE by double left clicking on the desired point Mask element.

Editing Analog Input Points – The Analog Input "Deadband" and "Mask" values can be edited by double left clicking on the desired point Deadband or Mask elements. The Deadband can be set to define when the point will report by exception under the class type in the Mask setting. When the point value exceeds the deadband value, it will initiate a report by exception to the master. The "Mask" value defaults to "CLASS TWO" and defines what polling class type the point is mapped to. The Mask value can also be set to CLASS ONE or THREE by double left clicking on the desired point Mask element.

A "Scale" factor may be programmed for any selected Analog Input point. Double left click in the "Scale" column to adjust. This allows a SCADA system that can only display 16-bit numbers to properly scale display values without going out of range.

Editing Binary/Control Output Points – The Binary/Control Output Point "Crob", "Mask" and "Inverse" values can be edited by double left clicking on the desired point Crob, Mask or Inverse elements. The Crob (Control Relay Output Block) setting is used to define what control method will be used to operate the point. The possible settings for **Crob** are listed below:

- Latch On
- Latch Off
- Latch OnOff
- Latch OnOff_TC
- Pulse On
- Pulse Off
- Pulse OnOff
- Pulse OnOff_TC
- Paired Close
- Paired Trip
- Paired TripClose

The **Mask** value defaults to "CLASS ZERO" and defines what polling class type the point is mapped to. The Mask value can also be set to CLASS NONE by double left clicking on the desired point Mask element.

Inverse defines whether the command to be sent would be inverted, meaning that when TRUE is selected, sending a Trip, Close, etc will have the opposite effect. This was implemented due to variations seen in RTU manufacturer's implementation of direct control with DNP to allow full compatibility the widest possible number of RTU's.

Editing Analog Output Points – The Analog Output "Mask" value can be edited by double left clicking on the desired point Mask element. The "Mask" value defaults to "CLASS ZERO" and defines what polling class type the point is mapped to. The Mask value can also be set to CLASS NONE by double left clicking on the desired point Mask element.

Editing Counters – The Counters "Mask" value can be edited by double left clicking on the desired point Mask element. The "Mask" value defaults to "CLASS THREE" and defines what polling class type the point is mapped to. The Mask value can also be set to CLASS ZERO, CLASS ONE, CLASS TWO, CLASS NONE, CLASS ONE NOT CLASS 0, CLASS TWO NOT CLASS 0 or CLASS THREE NOT CLASS 0 by double left clicking on the desired point Mask element.

DNP Security – DNP authentication is now available and can be independently enabled in the DNP security tab for either serial or Ethernet (both TCP or UDP) interfaces.

The concepts of the Hashed Message Authentication Code (HMAC) and challenge-response as defined in the DNP3 specification for Secure Authenticate Version 2.0 document is employed.

When authentication is enabled, the following settings should be selected:

- HMAC Algorithm and Update key
- Challenge Response timeout
- Duration of session key
- Aggressive Mode
- Critical Request Function Codes

■**NOTE:** Before IPScom allows a user to change the Update key, the user has to enter the old update key.

HMAC Algorithm and Update Key – The HMAC algorithm is either SHA1 (4 OCT) or SHA1(10OCT). An Update key is necessary to provide secure SESSION key negotiation. Once a SESSION key is obtained any subsequent challenge/response session will employ that session key. The Update key can be up to 32 hex characters (0123456789ABCDF) (128 bits).

Challenge Response Timeout – The range is from 0-100 seconds. This is the response time within which the control is expecting a response to a challenge.

Duration of Session Key – This duration must be configured in minutes (0-100) and in count 0-65535. This duration represents the maximum time or the maximum number of challenges a particular session key is used before key negotiation is again performed.

Aggressive Mode – Full challenge/response exchanges increase the number messages in the protocol, which affects throughput performance. Therefore, DNP Secure Authentication provides an aggressive mode in which the data from a single challenge can be used to authenticate many subsequent messages. The sender of the critical message includes the HMAC at the end of the critical message without having to be challenged. At least one challenge must occur, however, before aggressive mode can be used.

Critical Request Function Codes – This represents the function codes that will require authentication if selected. If none is selected, authentication will not be performed on any function code although authentication has been enabled.

M-76XX DNP Implementation Features

■**NOTE:** The user must reference the **Point Name** when creating a new DNP map, and especially when editing an existing DNP map. Do not rely on the Index Number, as these numbers will shift as points are added or deleted.

- DNP commands will not be executed while in Local mode.
- No profile changes are permitted while Remote Disable is active.
- When Remote is Disabled, all DNP Binary Output commands will not be executed, except the following points:
  - OPEN ABC with Remote Disabled
  - OPEN A with Remote Disabled
  - OPEN B with Remote Disabled
  - OPEN AC with Remote Disabled

DNP Configuration Editor Object Tabs – Each DNP Object can be configured by selecting the applicable tab from the Editor main window: Binary Inputs, Analog Inputs, Binary/Control Outputs, Analog Outputs, and Counters.

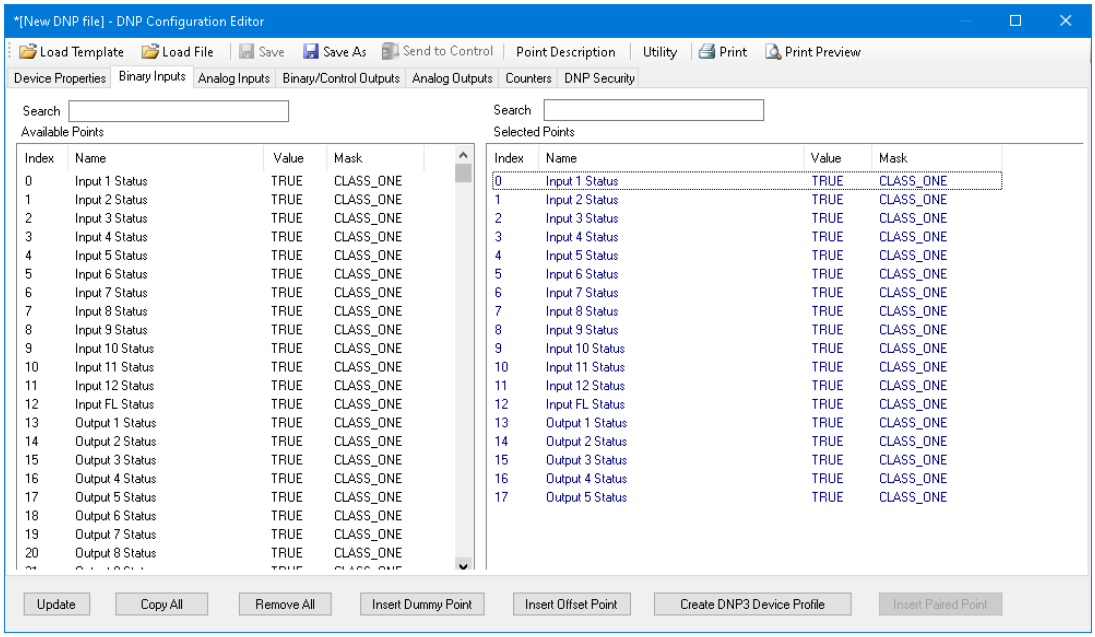


Figure 1-2 DNP Configuration Editor – Binary Inputs Tab

DNP Analog Inputs Scale Values

The Analog Inputs Scale value can be added and saved as a floating point value, with a Scale Factor of 100. Select any point in the right side of the DNP Configuration Editor, Analog Inputs screen, and double-click in the Scale column to edit the value (Figure 1-3)

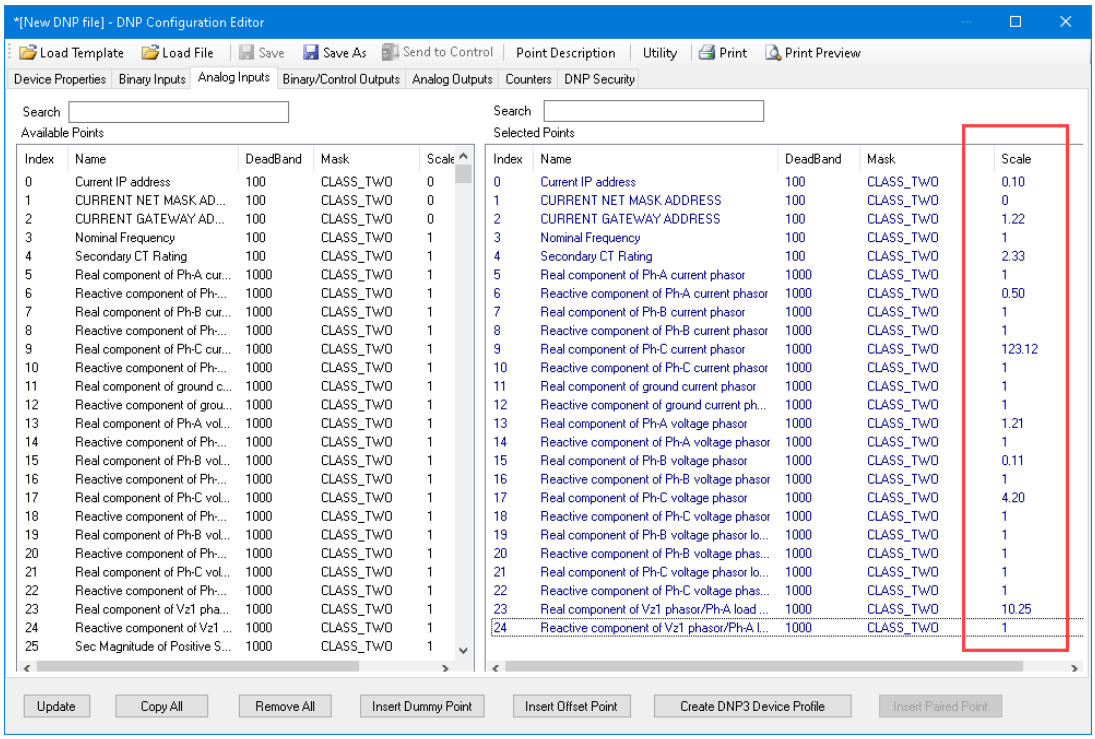


Figure 1-3 DNP Configuration Editor – Analog Inputs Tab (Scale Values)

DNP Security Options

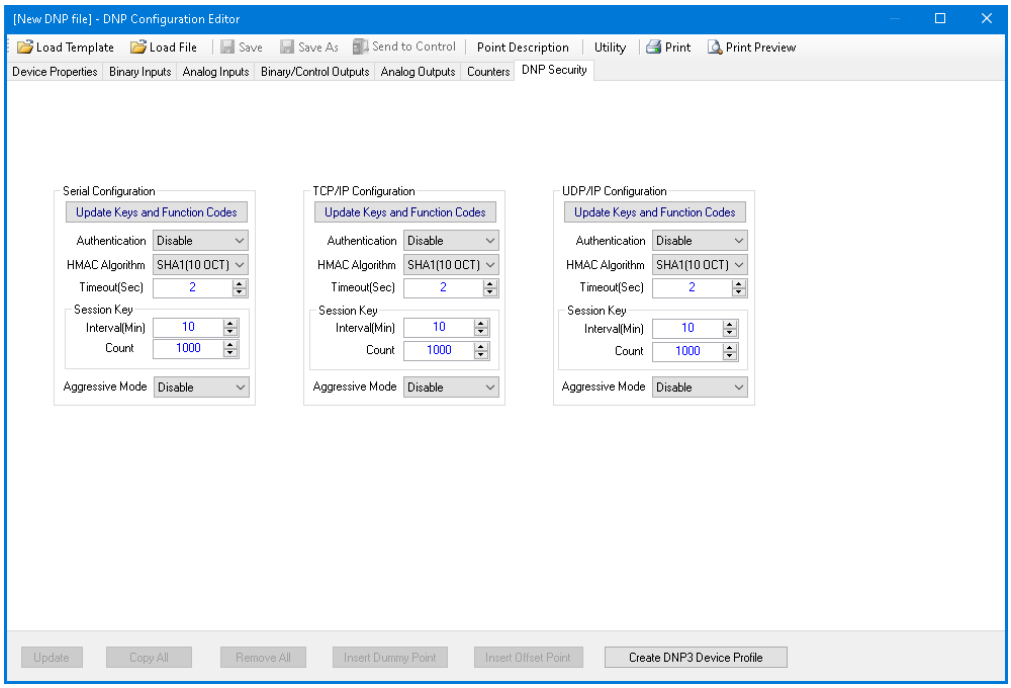


Figure 1-4 DNP Configuration Editor – DNP Security Tab

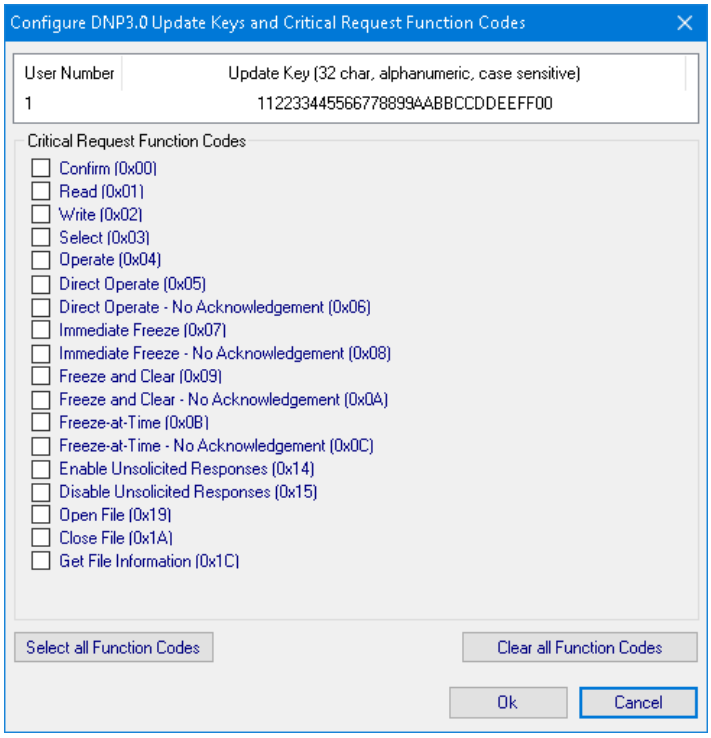


Figure 1-5 DNP Update Keys and Critical Request Function Codes Screen

Example of DNP Configuration Editor Use – The following sequence of steps provides an example of using the DNP Configuration Editor.

1. From the IPScom S-7600 Communications Software Main Screen select **Communication/ Protocol/DNP/DNP Configuration Editor**. IPScom will display the DNP Configuration Editor screen (Figure 1-1).
2. Select **Load Template/M-7651A Default** from the DNP Configurator menu bar. Select **Binary Inputs** tab, Figure 1-2 is displayed. The Available Points list for each DNP Points Group tab will also be populated.
3. Select the Binary Input points you wish to include in the DNP map by selecting Copy All or dragging the desired point(s) to the Selected Points window.
4. Edit the Selected Points for each tab as necessary to match your SCADA, RTU or Master setup.
5. Select **Save File** from the DNP Configurator menu bar. IPScom will display a "Save As" Screen with a *.xml file extension.
6. Name the file and then select **Save**.
7. If IPScom is connected to the target control then the "Send to Control" menu item can be used as follows:
    a. Select **Send to Control**. IPScom will display the "Open File" screen with a *.xml file extension.
    b. Select the file to be sent to the control, then select **Open**. IPScom will initiate the file transfer as indicated by the "Upload" status screen (Figure 1-6), followed by a "DNP File sent successfully" confirmation screen.

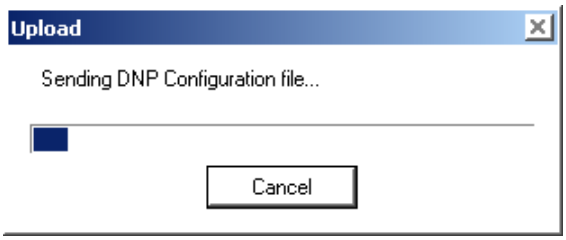


Figure 1-6 Sending DNP Configuration File Status Screen

2.0 S-1100 Remote Ethernet File Update Utility

■ CYBER SECURITY NOTE:

When Cyber Security is enabled, access to any feature described in this Section is subject to the Access Permissions Policy as designated by the Security Policy Administrator.

S-1100 Remote Ethernet File Update (REFU) Utility

The REFU Utility is a stand-alone PC application. The REFU Utility utilizes a file transfer algorithm that Beckwith Electric has implemented in the M-7651A firmware for transferring files such as User Access, IPsec Policy, and DNP device map files. The REFU Utility is capable of operation behind any secure firewall or within any IT security policy imposed by a local administrator.

Figure 2-1 Remote Ethernet File Update Utility Program Icon

Remote Ethernet Firmware Update

The Remote Ethernet Firmware Update element of the Remote Ethernet File Update (REFU) Utility application allows the user to remotely update one or more control's firmware to a new version, utilizing an ethernet connection. The Remote Ethernet File Update (REFU) Utility screen is presented in Figure 2-2.

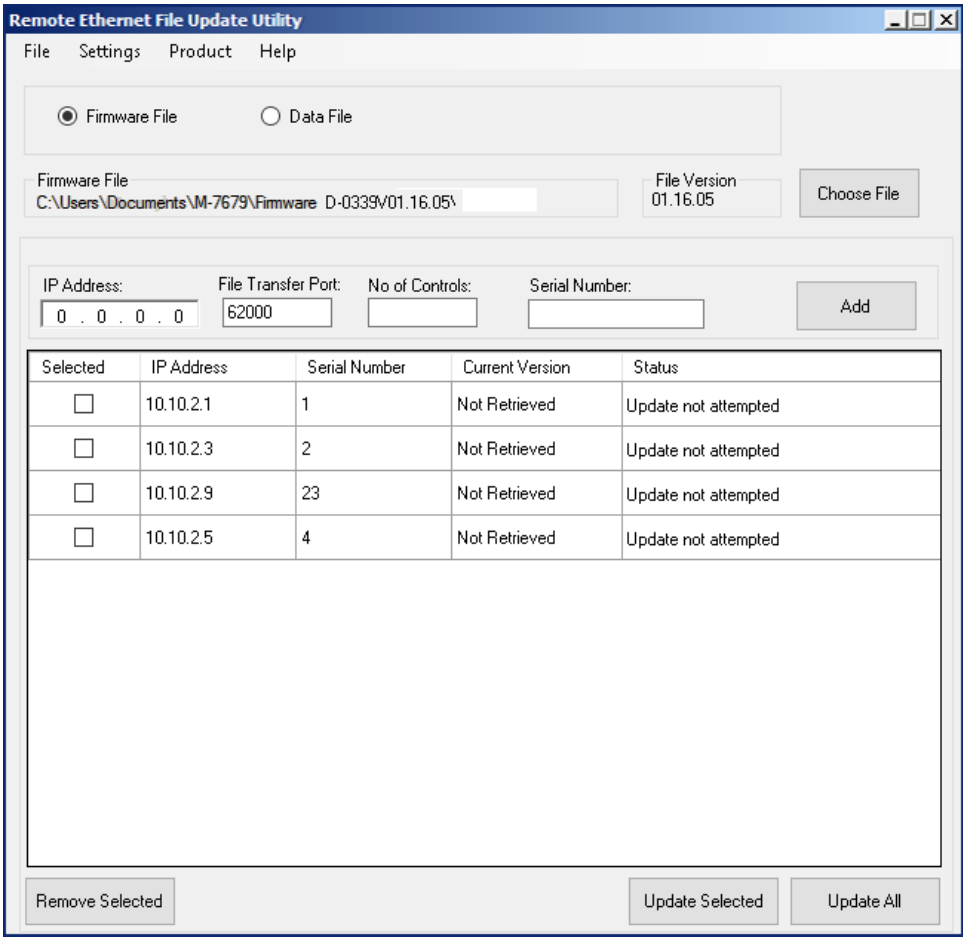


Figure 2-2 Remote Ethernet File Update Utility (Firmware File) Screen

Remote Ethernet File Update and Cyber Security

To comply with Cyber security requirements, the REFU Utility will prompt for a password when launched. The default password is "BecoUpdate". This password is user settable (alphanumeric and special characters) upon launching the program for the first time and can also be changed from the **File/Password** menu.

Due to the sensitive nature of this utility, it is highly recommended not to distribute this application to unauthorized users. Therefore, this application will not be available for download from the Beckwith Electric website. Furthermore, it is only available upon written request from authorized personnel.

The Remote Ethernet Firmware Update application allows the user to remotely update the firmware of targeted controls. As an additional security measure, the REFU protocol must be enabled utilizing IPScom or the front panel HMI. To enable the REFU protocol in IPScom, navigate to the Protocol Access screen **Communication/Setup/Comm Port Security/Protocol Access**. Select **Enable REFU** (Figure 2-3).

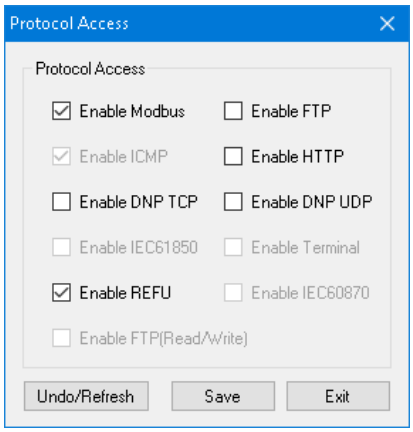


Figure 2-3 Comm Port Security/Protocol Access Screen

To enable the REFU protocol utilizing the HMI, navigate to the **Remote FW Update** menu screen **Communication/Comm Ports Security/Protocol Access**. Select **ENABLE**.

```
Remote FW Update
ENABLE
```

Additional Features

These features apply to both Firmware and Data File modes:

- The user can select for each control, which file(s) to be updated by selecting the appropriate check boxes.
- The utility can automatically generate consecutive IP Addresses, given a start IP Address and the number of controls in that IP Address range. It is important to note that the serial number verification by the utility is not performed when this feature is used.
- Users can also copy and paste IP address and serial number from a Microsoft® Excel® spreadsheet into the datagrid view of the REFU utility. Data may be pasted using "Ctrl+V" or by using a right mouse click and selecting "Paste".

■**NOTE:** The user cannot Copy/Paste only the serial number. The selection must be either (IP address + serial number) or (IP address only).

The information in the spreadsheet must be stored as shown below to use the Copy/Paste feature:

10.10.2.1	1
10.10.2.3	2
10.10.2.9	23
10.10.2.5	4

Remote Ethernet Firmware Update Procedure

■NOTE: These instructions describe the steps necessary to accomplish a remote firmware update utilizing the user interface provided by the Remote Ethernet File Update Utility. The actual dialog between the REFU Utility and the Control is described in detail in the Firmware Update Sequence section of this Section.

To remotely update the firmware of a control or a series of controls on an ethernet network proceed as follows:

1. Verify that the following conditions exist:
   - The Remote Ethernet File Update (REFU) Utility is installed and running on a PC with access to the target ethernet network.
   - A ".ppf" file (Program Package File) that contains the firmware to be updated is available.
2. Launch the Remote Ethernet File Update (REFU) Utility. The utility will display Figure 2-4 allowing the user to select the applicable product.

■NOTE: Product type can also be selected from "Product" in the REFU menu bar (see Figure 2-2).

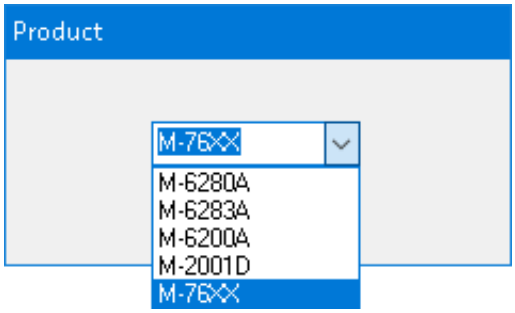


Figure 2-4 REFU Select Product Dropdown List

3. The REFU screen (Figure 2-2) will be displayed. Select "Firmware File".
4. Select "Choose File".
5. Select the ".ppf" file. The utility will:
   - Populate the "Firmware File" field with the path/file name
   - Open the selected file and retrieve and decrypt the version information and populate the "File Version" field with the firmware version
6. Enter the IP Address and the Serial Number of the control to be updated.
7. Select "Add". The information will be added to the list of controls to be updated. Repeat Step 6 for any other controls to be updated.

   The user can create a list of controls that will have their firmware updated. This list can be saved if desired and can be retrieved for use at a later date. The list of controls and their associated information (except for the "Update to Version") is stored in an encrypted format.
8. From the Settings dropdown menu select the number of "Retries" to be attempted if there is any failure to update the firmware on any control.

   The maximum number of retries is 10. The default number of retries is 3. The range is from 0 to 10.
9. Select the controls to be updated.
10. Select either "Update Selected" or "Update All" to start the update sequence.

    The REFU Utility will start the update sequence for each control. The sequence is described in detail in the Firmware Update Sequence described below.

Firmware Update Sequence Summary

1. The REFU Utility opens a TCP connection on port 62000.

■**NOTE:** Port 62000 must be available through the user's firewall for REFU to operate.

2. The REFU Utility initiates the Authentication session by sending an encrypted hash signature.
3. The Control verifies the received encrypted hash string.
4. If the Control can not verify the received encrypted hash string, then the connection is automatically closed by the Control.
5. If the received hash string verification is successful, then the Control goes into the programming mode.
6. The REFU Utility will then query the Control for the firmware version installed on the Control and if selected, the serial number of the Control.
7. The REFU Utility will compare the installed firmware version received from the Control, and if selected, the serial number to the REFU Utility internal serial number and version filter, and continue as follows:
   - If the installed firmware version is found to be a firmware version that does not support remote ethernet firmware update, and/or if selected, the serial number does not match, then after the selected number of attempts have also failed then the REFU Utility will close the connection.
   - If the comparison is successful, then update procedure continues.
8. The REFU Utility starts the file upload to the control.
9. When the file is completely uploaded to the Control, the control will verify the digital signature of the firmware.
10. Based on the results of the verification, the control will proceed as follows:
    - If the digital signature verification is unsuccessful, then the Control will send the appropriate error message to the REFU Utility and terminate the update session.
    - If the digital signature verification is successful, then the programming sequence will continue.
11. Prior to programming the flash, the following steps are taken:
    a. A block of all automatic and remote operations is activated, leaving the Control state unchanged.
    b. All ongoing operations are terminated.
    c. All setpoints and calibration data is backed up into internal data flash memory.

▲**CAUTION:** The update process, from erasing the Program Flash to complete reprogramming takes approximately 15 seconds. Any error or loss of power after the flash has been erased will be fatal to the control.

12. The flash programming is initiated. If for any reason the erasing or programming of the Program Flash is unsuccessful, then the Control will terminate the update process and return to normal program execution without rebooting.

    The Control will also notify the REFU Utility by sending the appropriate error message when queried. This type of error can result in the Program Flash not being completely programmed. Therefore, the user should retry to update the firmware again. A power loss in this condition will result in the Control not being able to reboot properly.
13. When the burning of the firmware into the program flash has been completed, the Control will Reboot.
14. When the Control has completed the reboot process, the Control will commence normal operation subject to the previously saved setpoints and calibration data.
15. After the Control has completed its rebooting process the REFU Utility will reopen a TCP connection on port 62000 and query for the firmware version number.
16. If the queried version number does not match the programmed version number, the REFU Utility application will notify the user of the status of the process and allow the user to repeat the update if desired.
17. If the queried version number matches the programmed version number, the programming process has been successful.

Remote Data File Update Procedure

To remotely update selected data files of a control or a series of controls on an ethernet network proceed as follows:

1. Verify that the following conditions exist:
   - The Remote Ethernet File Update (REFU) Utility is installed and running on a PC with access to the target ethernet network.
   - The desired "User Access", "IPsec Policy", or "DNP Configuration" file is available.
2. Launch the Remote Ethernet File Update (REFU) Utility. The REFU screen (Figure 2-2) will be displayed.
3. Select "Data File". The REFU Data File screen will be displayed (Figure 2-5).
4. Select "Choose File" for the file(s) to be updated. The utility will prompt for the desired file location and file name.
5. Select the desired file. The utility will populate the "DNP Configuration" field with the path/file name.
6. Enter the IP Address and the Serial Number of the control to be updated.
7. Select "Add". The information will be added to the list of controls to be updated. Repeat Step 6 for any other controls to be updated.

   The user can create a list of controls that will have their data files updated. This list can be saved if desired and can be retrieved for use at a later date. The list of controls and their associated information (except for the "Update to Version") is stored in an encrypted format.
8. From the Settings dropdown menu select the number of "Retries" to be attempted if there is any failure to update the data files on any control.

   The maximum number of retries is 10. The default number of retries is 3. The range is from 0 to 10.
9. Select the controls to be updated.
10. Select the desired file types to be updated on each individual control.
11. Select either "Update Selected" or "Update All" to start the update sequence.

    The REFU Utility will start the update sequence for each control. The sequence is described in detail in the File Update Sequence described below.

File Update Sequence Summary

1. The REFU Utility opens a TCP connection on port 62000.

■NOTE: Port 62000 must be available through the user's firewall for REFU to operate.

2. The authentication sequence is started with the control. The authentication sequence is similar to the firmware update authentication.
   - If the authentication sequence fails, then the connection is automatically closed by the Control.
   - If the authentication sequence is successful, then the Control starts the update procedure.
3. The REFU Utility starts the file upload.
4. File transfer is complete.

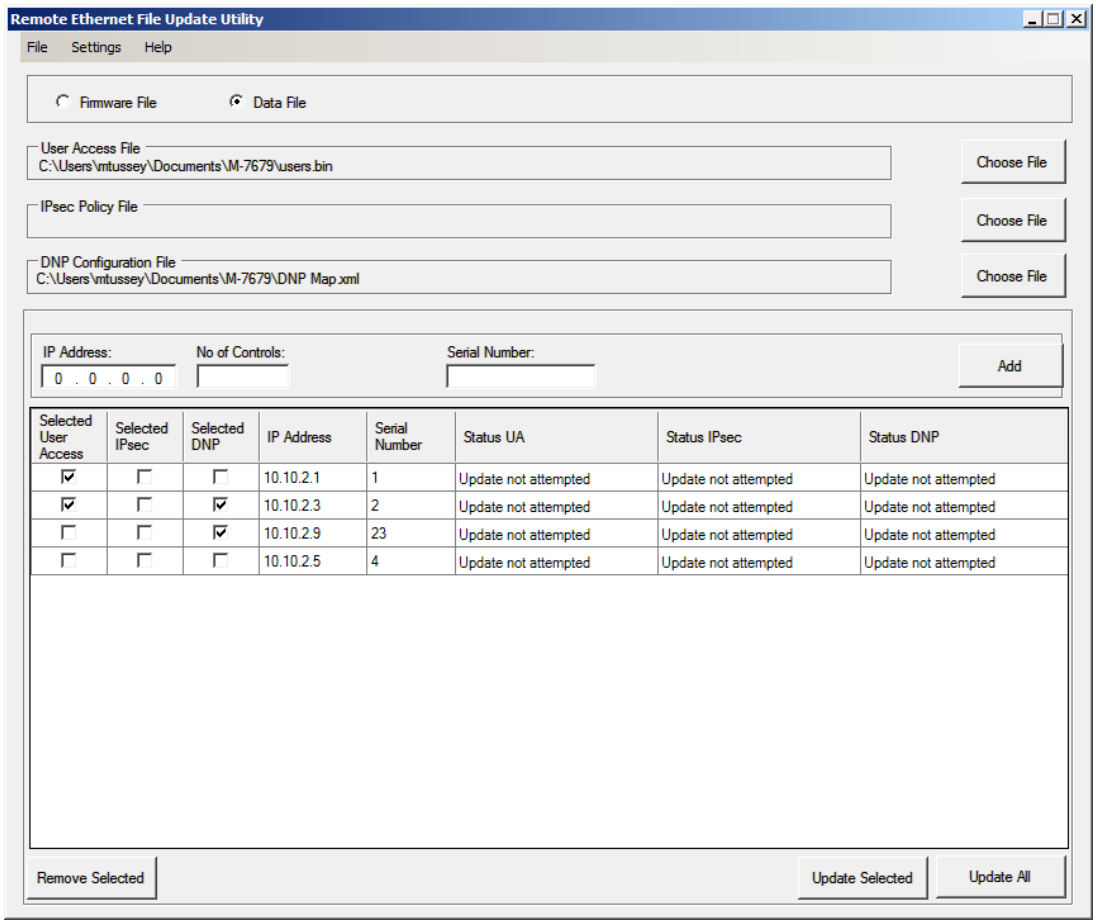


Figure 2-5 Remote Ethernet File Update Utility (Data File) Screen

3.0 Cyber Security

■ CYBER SECURITY NOTE:

When Cyber Security is enabled, access to any feature described in this Section is subject to the Access Permissions Policy as designated by the Security Policy Administrator.

This section describes the security elements incorporated in the M-7651A D-PAC, and the settings and configuration choices that are necessary to allow the unit to communicate securely over Virtual Private Networks (VPN).

The M-7651A is compliant with the applicable requirements of:

- IEEE 1686™-2007 Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities
- IPsec/IKE
- Radius

IEEE 1686 STANDARD

The M-7651A meets or exceeds the requirements established in IEEE Std 1686, IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities. Table 1 represents the M-7651A Table of Compliance (TOC).

Permissions

IEEE Standard 1686 for the most part defines the standards for User Name, Passwords and the Permissions associated with each user. The specific permission categories are listed in Table 2 "Permissions Implemented for IEEE 1686 Standard".

IPSEC/IKE OVERVIEW

IPsec/IKE is supported directly by the M-7651A. Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec is a suite of protocols specified by the Internet Engineering Task Force (IETF) that add security to the IP layer of internet traffic.

Implementing IPsec in the M-7651A secures internet traffic, including TCP and UDP packets. The important elements that are necessary to provide robust network data security include encryption and equally important authentication. Communication security cannot exist without a combination of both encryption, to prevent unauthorized monitoring of sensitive data, and authentication which validates the identity of all the parties involved in the communication scheme.

Clause/ subclause	Clause/subclause Title	Status	Comment
5	IED cyber security features	Acknowledge	
5.1	Electronic access control	Comply	
5.1.1	Password defeat mechanisms	Comply	
5.1.2	Number of individual ID/ passwords supported	Exceed	Product provides for 32 individual ID/password combinations
5.1.3	Password construction exception uppercase and lowercase letters are Interchangeable.	Comply	
5.1.4	Authorization levels by Password	Comply	
5.1.4.1	View data	Comply	
5.1.4.2	View configuration settings	Comply	
5.1.4.3	Force values	Comply	
5.1.4.4	Configuration change	Comply	
5.1.4.5	Firmware change	Comply	
5.1.4.6	ID/password management	Comply	
5.1.4.7	Audit log	Comply	
5.1.5	Password display	Comply/Exception	Except on local LCD
5.1.6	Access time-out	Comply	
5.2	Audit trail	Comply/Exception	Can only view audit trail events on computer
5.2.1	Storage capability	Comply	
5.2.2	Storage record	Comply	
5.2.2.1	Event record number	Comply	
5.2.2.2	Time and date	Comply	
5.2.2.3	User ID	Comply	
5.2.2.4	Event type	Comply	
5.2.3	Audit trail event types	Comply	
5.2.3.1	Login	Comply	
5.2.3.2	Manual logout	Comply	
5.2.3.3	Timed logout	Comply	
5.2.3.4	Value forcing	Comply	
5.2.3.5	Configuration Access	Comply	
5.2.3.6	Configuration change	Comply	
5.2.3.7	Firmware change	Comply	

Table 1 IEEE Std 1686 Table of Compliance (1 of 2)

Clause/ subclause	Clause/subclause Title	Status	Comment
5.2.3.8	Firmware change	Comply	
5.2.3.9	ID/password deletion	Comply	
5.2.3.10	Audit-log access	Comply	
5.2.3.11	Time/date change	Comply/Exception	Indicated as a forced value change
5.2.3.12	Alarm incident		
5.3	Supervisory monitoring and control		
5.3.1	Events	Exception	Done through use of DNP unsolicited events
5.3.2	Alarms	Exception	
5.3.2.1	Unsuccessful login attempt		
5.3.2.2	Reboot	Exception	However, users can deduce that a reboot has taken place by examining the DNP3.0 initialization bit being set followed by a DNP3.0 request for time.
5.3.2.3	Attempted use of unauthorized configuration software	Comply	A public encryption key shall be sent by the control to the client software upon request. This is used to authenticate whether the software is valid by encrypting the user id and password with the correct algorithm and key. This feature can enabled/ disabled by not choosing "Encrypted password" for access level.
5.3.3	Alarm point change detect	Comply	DNP 3.0
5.3.4	Event and alarm grouping	Comply/Exception	DNP 3.0 Class poll
5.3.5	Supervisory permissive control	Exception	(TBD)
5.4	Configuration software	Acknowledge	
5.4.1	Authentication	Comply	See 5.3.2.3
5.4.2	ID/password control	Exceed	Initially password is created by administrator. Once changed by the user, password cannot be read by anyone.
5.4.3	ID/password-controlled features	Comply	
5.4.3.1	View configuration data	Comply	
5.4.3.2	Change configuration data	Comply	
5.4.3.3	Full access	Comply	
5.5	Communications port access	Comply	
5.6	Firmware quality assurance	Comply	

Table 1 IEEE Std 1686 Table of Compliance (2 of 2)

Permission Categories (Access Permitted)	Default Permissons (X = Permission Category Included in Default Permission Set)										
	View Data	View Setpoints	Change Setpoints	Read Files	View Config	Change Config	Firmware Update	Manage Users	View Audit Log	Remote Control	Change Date/Time
Monitor Data	X										
View setpoints		X									
Change setpoints		X	X								
View configuration					X						
Change configuration					X	X					
Copy Profiles		X	X	X	X	X					
Datalog setup					X	X					
Datalog download				X							
SOE setup					X	X					
SOE download				X							
OSC setup					X	X					
OSC download				X							
Security events log									X		
Manage users*								X			
Firmware update							X				
Remote control										X	
Change Date/Time											X
Get LED file				X							
Write LED file											
Get Button file				X							
Write Button file											
Write Wakeup Screens											
*User can change own password without manage users permissions set											

Table 2 Permissions Implemented for IEEE 1686 Standard

RADIUS OVERVIEW

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service. Authentication and Authorization RADIUS are described in RFC 2865 while Accounting is described in RFC 2866.

RADIUS is a client/server protocol that runs in the application layer, using UDP as transport. The following UDP ports are used:

- For Authentication and Authorization UDP port 1812 (previously 1645)
- For Accounting UDP port 1813 (previously 1646)

RADIUS serves three functions:

1. Authenticate users or devices before granting them access to a network
2. Authorize those users or devices for certain network services
3. Account for usage of those services

Password Authorization Mechanism

The M-7651A includes the capability to use Authentication based on IEEE 1686. When IEEE 1686 password security is disabled, the RADIUS protocol although settable is not functional. When Authentication based on IEEE 1686 is implemented, then the full functionality of the RADIUS protocol is available. The following features are available if RADIUS is enabled:

- The M-7651A provides local authentication capability if and ONLY if there is no other remote authentication server available to the device. An example of a remote authentication server is the RADIUS server.
- The M-7651A has the capability of being configured to use two remote authentication servers. Examples are 2 RADIUS servers. In case the primary server is down and not responding, the secondary server shall be used, and finally if both servers are down, the device shall fall back to the local server which is the IEEE 1686 password authentication.

The device is shipped with a default password file configured with one Super User ID and password. It is up to the end user to change this default password to ensure the security of the network. Usually the local password should match security policy of the RADIUS server.

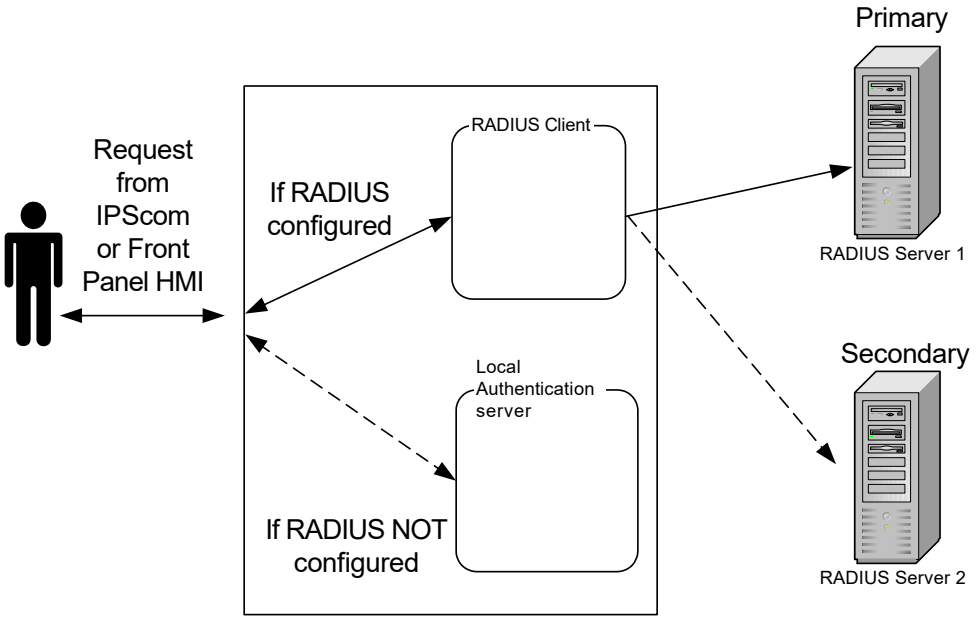


Figure 3-1 RADIUS Server Configuration

Authentication and Authorization

The M-7651A firmware includes the client and the Remote Access Server (RAS) component of the RADIUS protocol implemented. The unit sends a request to a RADIUS Server to gain access to a particular network resource using access credentials. The credentials are internally passed to the RAS.

In turn, the RAS sends a RADIUS Access Request message to the RADIUS server, requesting authorization to grant access via the RADIUS protocol. This request includes access credentials, typically in the form of user name and password provided by the user. The UDP port 1812 is used to communicate with the RADIUS server.

The RADIUS server checks that the information is correct using the defined authentication schemes. The User identification is verified along with the user's network address and user privileges.

The RADIUS server returns one of three responses to the client:

- Access Reject
- Access Challenge
- Access Accept

Accounting

RADIUS Accounting Flow Accounting is described in RFC 2866. The UDP port 1813 is used to communicate with the RADIUS server for accounting purpose.

When network access is granted to the user by the client, an Accounting Start (a RADIUS Accounting Request packet containing an Acct-Status-Type attribute with the value "start") is sent by the client to the RADIUS server to signal the start of the user's network access. "Start" records typically contain the user's identification, network address, point of attachment and a unique session identifier.

Periodically, Interim Update records (a RADIUS Accounting Request packet containing an Acct-Status-Type attribute with the value "interim-update") may be sent by the client to the RADIUS server, to update it on the status of an active session. "Interim" records typically convey the setpoint changes by the user.

Typically, the client sends Accounting-Request packets until it receives an Accounting-Response acknowledgement, using some retry interval.

In general the primary purpose of this data is to log user activity (Login/logout, setpoint changes, file transfer).

Channel ID	Description
0	USB interface
1	Comm interface on UART 0
2	Serial interface on UART 1
3	HMI interface
4	MODBUS Ethernet (starts from Channel 4 and may run through Channel 11 since eight MODBUS Ethernet connections at a time are supported)

Table 3 RADIUS Accounting – Channel ID Table

CYBER SECURITY SETUP (IEEE STANDARD 1686) FROM IPSCOM

1. Start IPScom, then establish communications with the target unit.
2. Select **Utility/Cybersecurity/Manage Accounts/Set Access Password Type** from the IPScom tool bar. IPScom will display the "Access Password Type" screen (Figure 3-2).

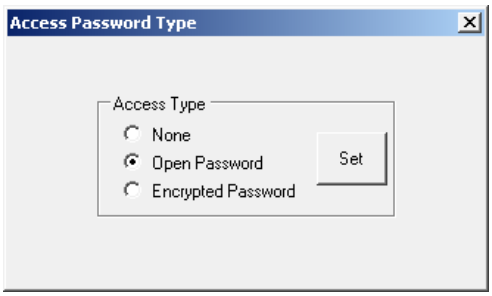


Figure 3-2 Access Password Type Screen

■NOTE: The default User Name is "admin1"
The default password is "admin1@M76XX"

3. Select the desired Access Level, and then select **Set**:
   - **None –** Cyber Security is not enabled. The user will not be prompted to enter a User Name and Password and will have access to ALL features and functions.
   - **Open Password –** The password is not encrypted. This option should be chosen when IPScom is not the sole method of communication to the unit.
   - **Encrypted Password –** The password is encrypted and is authenticated by the unit to allow the user to log on to the unit. However, this selection only controls password encryption for a user login. Setpoints files and passwords contained in Account Permissions files are encrypted.

Compliance with 2020 California Password Law

As of July 1st, 2020 all Beckwith Electric IED's with network communication capabilities shipping to the state of California will comply with California Password Law (SB-327). M-7651A controls will ship with the enhanced IEEE 1686 Standard Cyber Security feature **Enabled** and with a single pre-loaded default administrator account and password. Under this law, default passwords are not permitted to be used.

The first time the control is accessed using the default pre-loaded administrator account, the control will prompt the administrator to change the default password. The control will not allow any setting changes until the default password is changed.

■NOTE: The default pre-loaded administrator account User Name is "admin1"
The default Password is "admin1@M76XX"

When the user connects to the unit the first time, IPScom will request the Administrator login information:

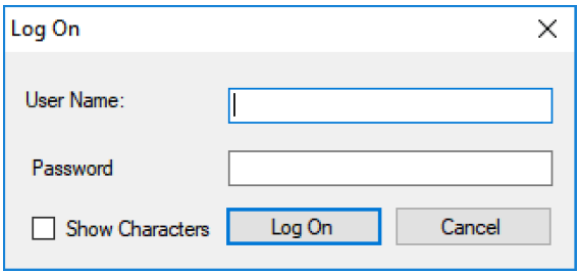


Figure 3-3 Initial Log On Screen with CA Password Law Compliance

Enter the pre-loaded administrator account User Name and Password as shown in the **NOTE**. IPScom will display a message that the default administrator password MUST be changed.

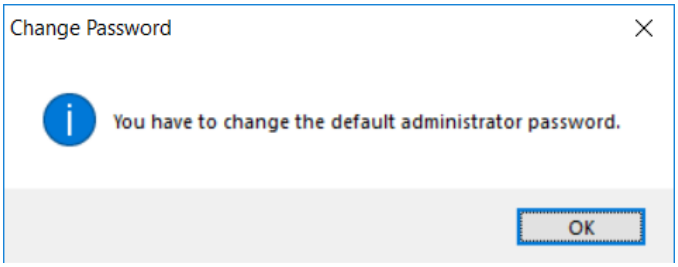


Figure 3-4 Default Administrator Password Must Be Changed Message

Enter the new password as described in the **"Change Password"** section. The new password must meet the criteria defined in the Change Password screen (Figure 3-13). If this operaton is Cancelled, the process will repeat when the user connects again. When the password has been changed successfully, IPScom will display a confirmation screen and allow full access to the control.

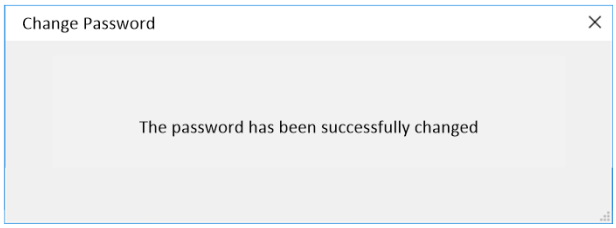


Figure 3-5 Default Password Changed Successfully Confirmation Screen

USER ACCOUNTS

■**NOTE:** The default User Name is "admin1". The default password is "admin1@M76XX"

The unit contains default User Names, Passwords, and Roles. A user with the **Manage Users** permission can perform the following:

- Add/Delete a user
- Change the permissions associated with a user
- Assign a user to a specific Role
- Add/Delete a Role
- Open/Save/Save As, a (.bin) file
- Retrieve (Save As) and View an Audit Log (.bkp)

While the Manage Users permission allows the user to control all aspects of a User, the Manage Users permission does not allow changing or viewing a user's password beyond initially establishing the password when the User is created. However, the Manage Users permission can delete the user account, effectively canceling the password.

User Account information resides on the unit in flash memory. When retrieving (IPScom only), the data is saved to a file with a (.bin) file extension. The file contains all user(s) information for display and editing.

When initially establishing a password or when changing a password, the password syntax must conform to the following criteria:

- Minimum length must be 8 characters
- Maximum length is 20 characters
- Must include at least one uppercase letter
- Must include at least one lowercase letter
- Must include at least one number
- Must include at least one non-alphanumeric character (e.g. @, %, *, etc.)

IPScom presents the password criteria in red type in the "Change Password" (Figure 3-13) and "Add User" (Figure 3-10) screens. As the criteria is met for the entered password, the "type" that states the criteria that has been met changes to black.

During "Retrieve Account Permissions from Control" and "Send Account Permissions to Control" operations, all User Account information is included. However, when a Password is changed, only the password is written to the unit.

■**NOTE:** The instructions in this section assume that the user has been granted the appropriate permission (Manage Users) to access and make changes to these features and capabilities.

User Account Modification and Setup

The unit contains default User Accounts. The following instructions describe:

- Modifying Account Permissions retrieved from the unit
- Modifying an existing Account Permissions (.bin) file
- Setting up a new User Account in an Account Permissions file.

Modifying Account Permissions Retrieved from the Unit

1. Start IPScom, then establish communications with the target unit.
2. Select **Utility/Cybersecurity/Manage Accounts/Retrieve Account Permissions from Control** from the IPScom tool bar. Save the Account Permissions file as desired.
3. From the Manage Account Permissions screen menu bar select **File/Open**.
4. Navigate to the file location and select the file that contains the retrieved Account Permissions to be modified.
5. Select **Open**. Follow the IPScom prompts to enter the User Name and Password associated with the selected file. After login is accepted, IPScom will display the Manage Account Permissions screen.

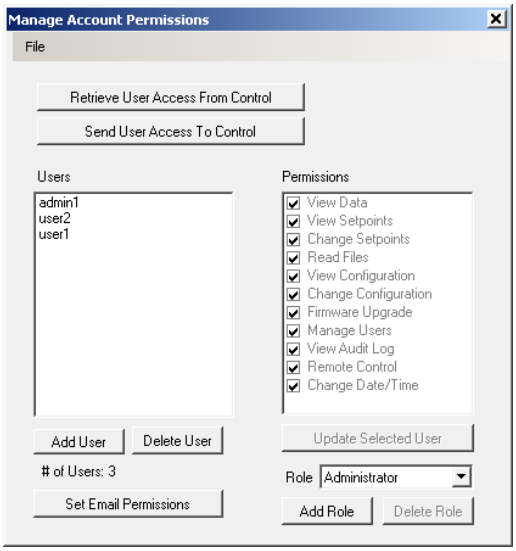


Figure 3-6 Manage Account Permissions Retrieved from Control Screen

6. Select the **User** to be modified.
7. Select the desired Permissions for the User:
   - Check or uncheck the desired Permissions
   - Select "Set Email Permissions" to automatically add the permissions required to access the E-mail Support feature:
     - View Data
     - View Setpoints
     - Read Files
     - View Configuration
     - Manage Users
     - View Audit Log

- Select a **Role** with pre-defined Permissions from the Role dropdown menu (Figure 3-7)

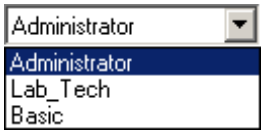


Figure 3-7 Pre-defined Roles

8. When all permissions have been entered, select **Update Selected User**. The original (.bin) can be saved (File/Save) or saved to a different file name and/or location (File/Save As).
9. From the Manage Account Permissions screen menu bar select **File/Save** or **Save As**. IPScom will display a "Send File" screen to allow the user to save the file to the unit or to the computer (Figure 3-8).

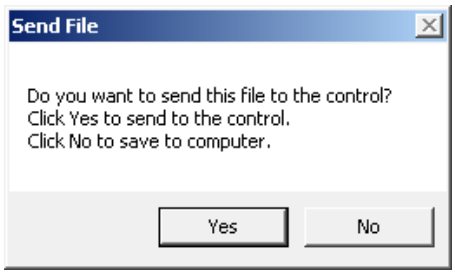


Figure 3-8 Send User File Screen

10. Select **Yes** to send the User File to the unit. IPScom will display a confirmation screen. Select **OK**, IPScom will close communications.
11. Select **No** to save the User File to the computer. If **File/Save As** was selected, IPScom will display the "User Access File" Save As screen.

▲CAUTION: It is very important to record the User Name and Password associated with the saved file. The only way to access the file is to have the correct User Name and Password. In the case of writing the file to a unit, the unit will not be able to be accessed and will require the user to contact the factory to restore default User Name and Password.

Modifying Account Permissions in an Existing User Access (.bin) File

1. Start IPScom, select **Utility/Cybersecurity/Manage Accounts/Manage Account Permissions** from the IPScom tool bar. IPScom will display a "Manage Account Permissions" screen (Figure 3-9).

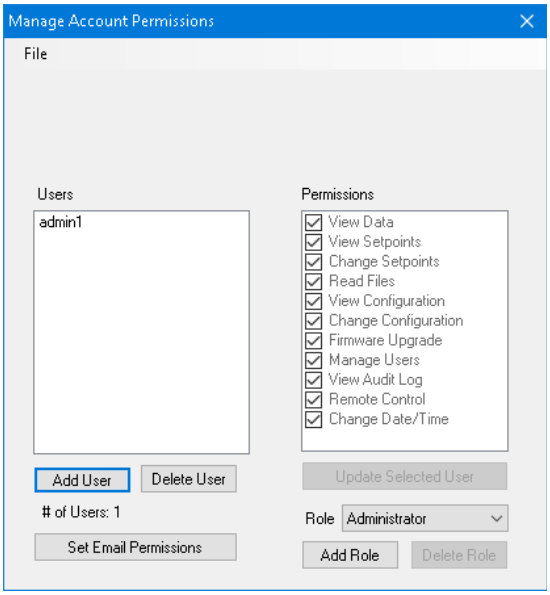


Figure 3-9 Manage Account Permissions Screen

2. From the Manage Account Permissions screen menu bar select **File/Open**. IPScom will display the Binary File Open screen.
3. Navigate to the file location and select the existing User Access (.bin) file to be modified.
4. Select **Open**. IPScom will display a prompt for the User Name and Password associated with the selected file. After login is accepted, IPScom will display the Manage Account Permissions screen.
5. Select the **User** to be modified.
6. Select the desired Permissions for the User:
   - Check or uncheck the desired Permissions
   - Select a **Role** with pre-defined Permissions from the Role drop down menu (Figure 3-7)
7. When all permissions have been selected/deselected, select **Update Selected User**. The original Binary File can be saved (File/Save) or saved to a different file name and/or location (File/Save As).

▲CAUTION: It is very important to record the User Name and Password associated with the saved file. The only way to access the file is to have the correct User Name and Password. In the case of writing the file to a unit, the unit will not be able to be accessed and will require the user to contact the factory to restore default User Name and Password.

Setting Up a New User Account in a User Access File

1. Start IPScom, then establish communications with the target unit.
2. Select **Utility/Cybersecurity/Manage Accounts/Manage Account Permissions** from the IPScom tool bar. IPScom will display a "Manage Account Permissions" screen (Figure 3-9).
3. From the menu bar select **File/Open**. IPScom will display the Binary File Open screen.
4. Navigate to the file location and select the User Access (.bin) file to be modified.
5. Select **Open**. IPScom will display a prompt for the User Name and Password associated with the selected file. After login is accepted, IPScom will display the Manage Account Permissions screen.
6. Select **Add User**. IPScom will display the "Add User" screen (Figure 3-10).

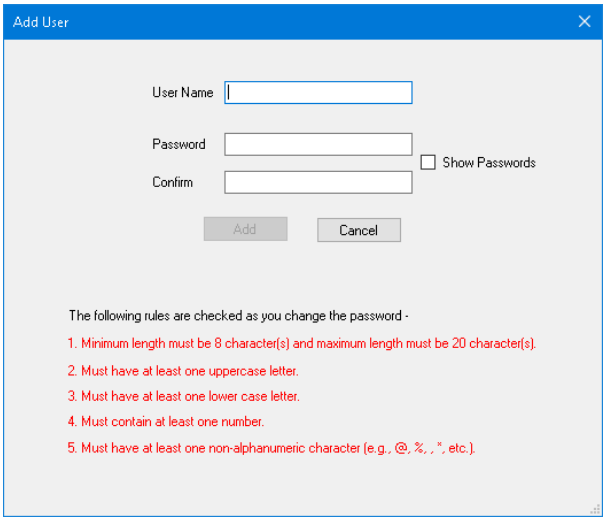


Figure 3-10 Add User Screen

7. Enter a valid User Name and Password consistent with criteria presented in the User Accounts section earlier in this Section.

   IPScom presents the password criteria in red type. As the criteria is met for the entered password, the "type" that states the criteria that has been met changes to black.
8. When all Password criteria have been met, then select **Add**. IPScom will return to the "Manage Account Permissions" screen (Figure 3-6) and display the new User.

9. Select the new User, then select the desired Permissions:
   - Check or uncheck the desired Permissions
   - Select a **Role** with pre-defined Permissions from the Role drop down menu (Figure 3-7)
10. When all permissions have been selected/deselected, then select **Update Selected User**.

▲CAUTION: It is very important to record the User Name and Password associated with the saved file. The only way to access the file is to have the correct User Name and Password. In the case of writing the file to a unit, the unit will not be able to be accessed and will require the user to contact the factory to restore default User Name and Password.

Roles

When the S-7600 IPScom is installed on the host PC, a Role file is created that contains the default Roles. Changes to existing Roles and creation of new Roles are captured in this file. However, Roles created on other IPScom PC installations may have different permissions for the same Role name. Adding and deleting "Roles" is accomplished from the "Manage Account Permissions" screen (Figure 3-9).

Retrieving Account Permissions from the Control

1. Start IPScom, then establish communications with the target unit.
2. Select **Utility/Cybersecurity/Manage Accounts/Retrieve Account Permissions from Control** from the IPScom tool bar. IPScom will display a Binary File Save As screen.
3. Choose the **Save As** location and enter the desired file name that will contain the Account Permissions retrieved from the unit.
4. Select **Save**. IPScom will save the (.bin) file to the selected location.

Sending Account Permissions to the Control

1. Start IPScom, then establish communications with the target unit.
2. Select **Utility/Cybersecurity/Manage Accounts/Send Account Permissions to the Control** from the IPScom tool bar. IPScom will display a Binary File Open screen.
3. Navigate to the file location and select the desired file name that contains the Account Permissions to be sent to the unit.
4. Select **Open**. IPScom will attempt to send the selected (.bin) file to the target unit.
5. If IPScom returns a "Failed to send Users.bin file to Control" confirmation (Figure 3-11), then select **OK** and repeat Steps 2 through Step 4.

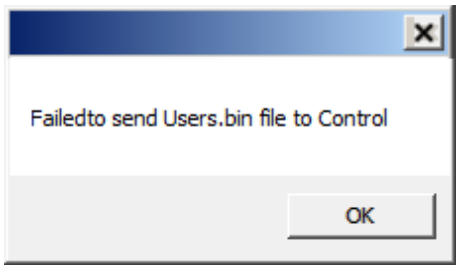


Figure 3-11 Failed to Send Users.bin File to Control Confirmation Screen

6. If file transfer is successful, IPScom will display a "User Permission file sent to control" confirmation screen. Select **OK**, IPScom will close communications.

   If any changes were made to the permissions that were sent to the unit, the changes will take effect the next time the user logs on to the unit.

AUDIT LOG

The Audit Log captures security events in the order in which they occur. The Audit Log can be retrieved and viewed in IPScom. The Audit Log is saved to the PC with a (.bkp) file extension. The Audit Log can also be saved as a Comma Separated Values file (.csv).

Each Audit Log entry includes:

- Date (Month, Day, Year)
- Time (Hour, Minute, Second)
- User Name
- Event Description regarding:
  - USB interface
  - Comm interface on UART 0
  - Serial interface on UART 1
  - HMI interface
  - MODBUS Ethernet: MODBUS Ethernet starts from Channel 4 and may run through Channel 11 since the M-7651A supports eight MODBUS Ethernet connections at a time.

Audit Log Retrieval, Viewing and Saving

The following sequence of steps describes retrieving, viewing and saving the Audit Log as a (.bkp) file.

1. Start IPScom, then establish communications with the target unit.
2. Select **Utility/Cybersecurity/Manage Accounts/Audit Log/Retrieve** from the IPScom tool bar. IPScom will display the "Save As" screen with the default (.bkp) file extension.
3. Choose the **Save As** location and enter the desired file name that will contain the Audit Log retrieved from the unit.
4. Select **Save**. IPScom will display a confirmation screen that the file has been saved.
5. Select **OK**. IPScom will automatically display the Audit Log screen (Figure 3-12).
6. To view a previously saved Audit Log, select **Utility/Cybersecurity/Manage Accounts/Audit Log/View**. IPScom will display the "Audit Log file" Open screen with the default (.bkp) file extension.
7. Navigate to the desired file, and select **Open**. IPScom will display the Audit Log Screen (Figure 3-12).

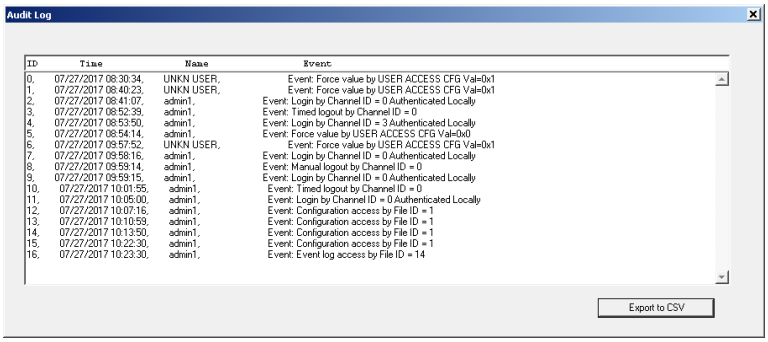


Figure 3-12 Audit Log Screen

8. To save the displayed Audit Log to a (.csv) formatted file select **Export to CSV**. IPScom will display a File Saved confirmation screen.

■**NOTE:** It may be necessary to select **View Hidden Folders** in Windows to locate the CSV file.

9. Select **OK**. IPScom will return to the Audit Log screen.

CHANGE PASSWORD

The Password associated with a specific User Name can only be changed by successfully connecting to the target unit. When **Change Password** is selected (Figure 3-13), only the new Password is written to the unit.

To change the Password for a specific User, proceed as follows:

1. Start IPScom, then establish communications with the target unit.
2. Select **Utility/Cybersecurity/Manage Accounts/Change Password** from the IPScom tool bar. IPScom will display the "Change Password" screen (Figure 3-13).

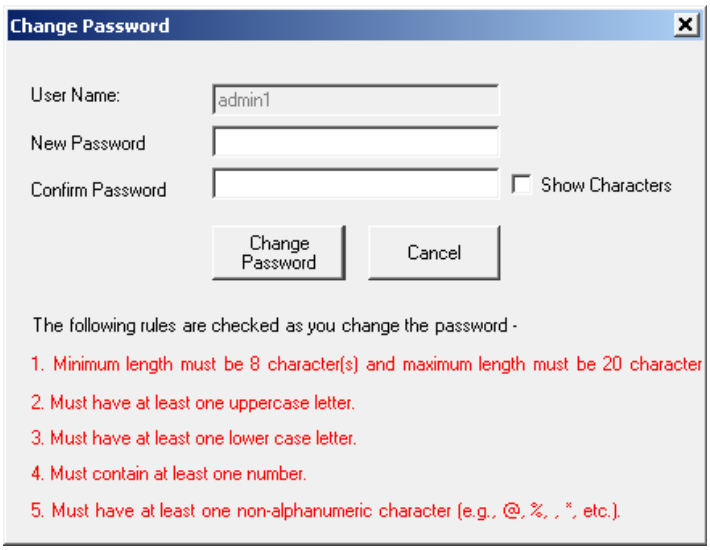


Figure 3-13 Change Password Screen

3. Enter a new Password consistent with criteria presented in the User Accounts section earlier in this Section.

   IPScom presents the Password criteria in red type. As the criteria is met for the entered password, the "type" that states the criteria that has been met changes to black.
4. Re-enter the new Password to confirm.
5. When all Password criteria have been met, then select **Change Password**. IPScom will display the "Changing Password" status screen.
6. When the Password has been changed on the unit, IPScom will display the "Password Changed Logout" confirmation screen (Figure 3-14).

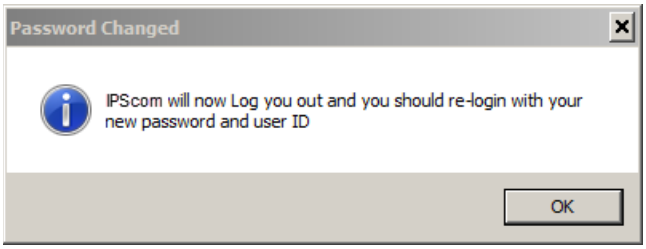


Figure 3-14 Password Changed Logout Confirmation Screen

7. Select **OK**. IPScom will log off the current user. In order to re-login to the unit, the new Password must be entered.

SECURITY MODE SETUP

■**NOTE:** The instructions in this section assume that IEEE Standard 1686 has been enabled and the user has been granted the appropriate permissions to access and make changes to these features and capabilities.

RADIUS Configuration from IPScom

To setup the RADIUS elements of the Cyber Security scheme perform the following:

1. Obtain the following information from the Network Administrator:
   - Primary Server IP Address/ Authentication Port/ Accounting Port
   - Secondary Server IP Address/ Authentication Port/ Accounting Port
   - Secret Key
2. Start IPScom, then establish communications with the target unit.
3. Select **Communication/Setup/Communication Security/Radius Configuration** from the IPScom tool bar. IPScom will display a "Radius Configuration" screen (Figure 3-15).

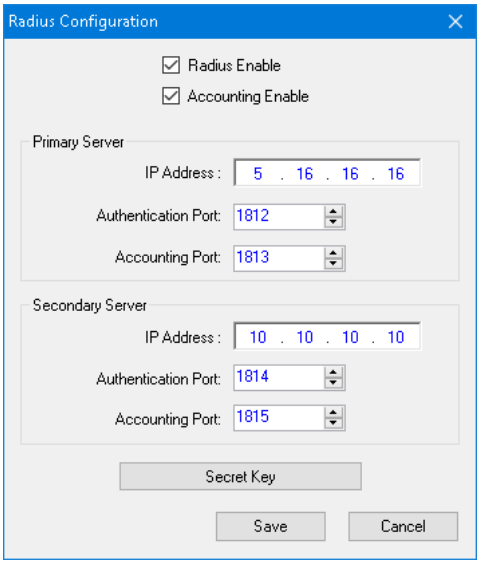


Figure 3-15 Radius Configuration Screen

4. Enter the required settings in the Radius Configuration screen.
5. From the Radius Configuration screen select **Secret Key**. IPScom will display the "Radius Configuration Key" screen (Figure 3-16).

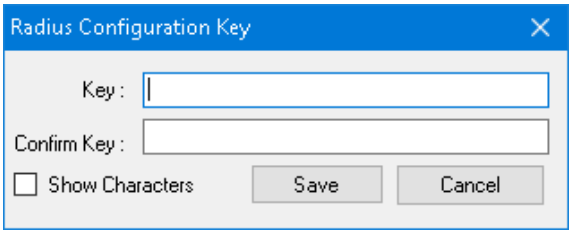


Figure 3-16 Radius Configuration Key Screen

▲**CAUTION:** It is very important that the Configuration Key is entered correctly. In the event that it is not entered correctly and Radius is "Enabled" the Radius server will deny access to the unit because the Password will be encrypted in a way that the Radius server can not decrypt it properly.

6. Enter the Radius Configuration Key.
7. Select **Save**. IPScom will write the Radius Configuration settings to the unit.

Enable and Configure RADIUS Security from the HMI

RADIUS Security can also be enabled and configured from the front panel HMI. The settings to enable RADIUS Security are located in the COMMUNICATIONS/Port Settings/Comm Ports Security/Protocol Access menu. The RADIUS configuration settings are located in the COMMUNICATIONS/Port Settings/Ethernet/Settings menu.

IPsec Configuration from IPScom

1. Start IPScom, then establish communications with the target unit.
2. To enable IPsec from IPScom, from the **Communication/Setup/Communication Security/IPSEC Configuration** dropdown menu, select **Enable**. IPScom will display the "IPSec Enable" confirmation screen (Figure 3-17).

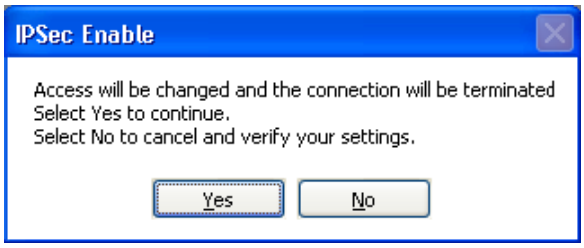


Figure 3-17 IPSec Enable Confirmation Screen

3. To configure IPsec, select **IPSEC Configuration/Configure Endpoint**. IPScom will display the "Configure Endpoint" (Figure 3-18) screen which allows the user to add, edit, delete, or save IPsec Endpoints.

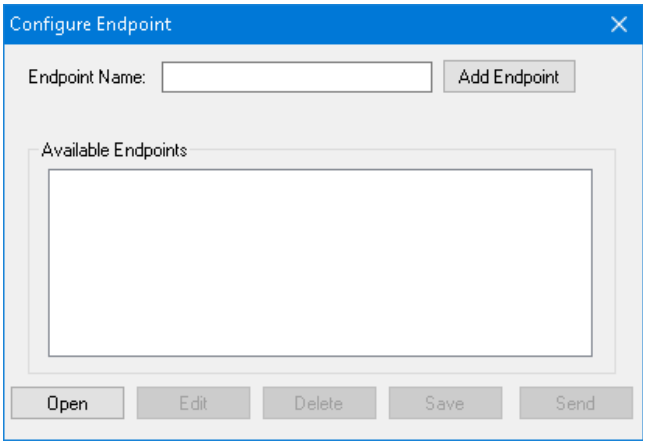


Figure 3-18 IPsec Configure Endpoint Screen

4. Select an available Endpoint from the "Configure Endpoint" screen and then select **Edit**. IPScom will display the "IPsec General Settings" screen (Figure 3-19) which allows the user to configure IPsec security settings, including IKE (Internet Key Exchange) Policy, IPsec Policy, Policy Lifetimes and Identities.
5. Enter the required settings in the IPsec General Settings screen tabs (Figure 3-20 through Figure 3-22).

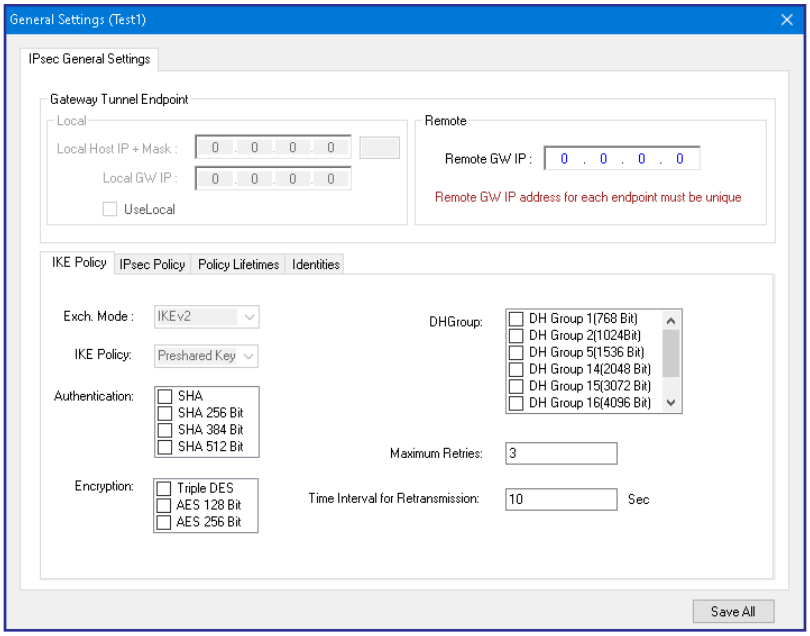


Figure 3-19 IPsec General Settings Screen

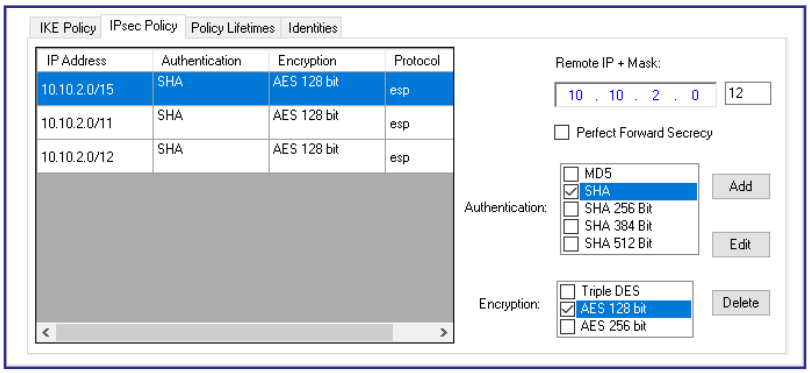


Figure 3-20 IPsec General Settings – IPsec Policy Tab

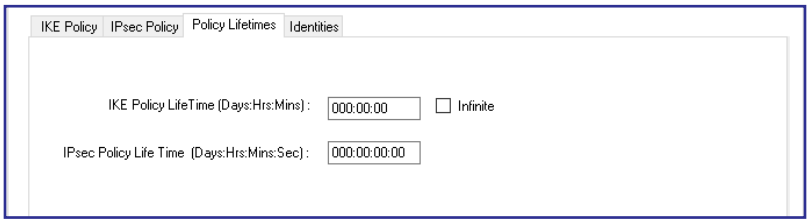


Figure 3-21 IPsec General Settings – Policy Lifetimes Tab

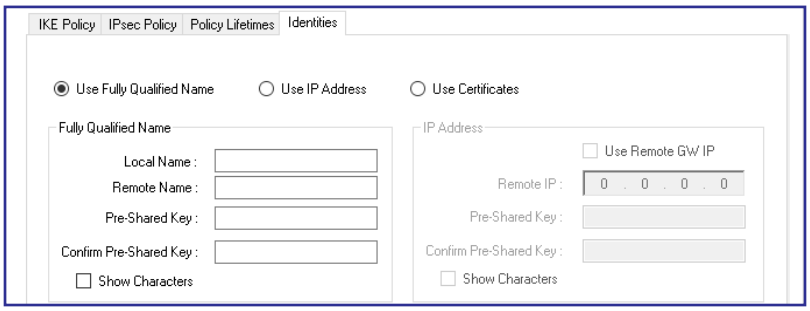


Figure 3-22 IPsec General Settings – Identities Tab

6. Select **Save All**. IPScom will display an Error Message alerting the user to any required settings which have not been entered (Figure 3-23).

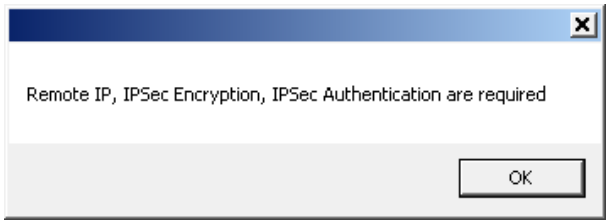


Figure 3-23 IPsec Configuration Error Screen

7. If applicable, enter all required settings and select **Save All**.
8. Close the "General Settings" screen and return to the "Configure Endpoint" screen.
9. Add and/or edit any additional endpoints and select **Save**. IPScom will display the "Save As" screen.
10. Enter the desired IPsec Configuration filename and select **Save**. IPScom will display a confirmation screen.
11. Select **OK**. IPScom will return to the "Configure Endpoint" screen.

■**NOTE:** IPsec configuration files may be sent to the control from the Configure Endpoint screen.

Sending the IPsec Configuration File to the Unit

1. Start IPScom, then establish communications with the target unit.
2. Select **Communication/Setup/Communication Security/IPsec Configuration/Send Configuration File** from the IPScom tool bar. IPScom will display the "IPsec Configuration File" Open screen.
3. Select the file name that contains the IPsec Configuration to be sent to the unit.
4. Select **Open**. IPScom will send the selected file to the target unit.
5. IPScom will display a confirmation screen. Select **OK** IPScom will return to the main screen.

Retrieving the IPsec Configuration File from the Unit

1. Start IPScom, then establish communications with the target unit.
2. Select **Communication/Setup/Communication Security/IPsec Configuration/Retrieve Configuration File** from the IPScom tool bar. IPScom will display the "IPsec File" Save As screen.
3. Choose the **Save As** location and enter the desired file name that will contain the IPsec Configuration retrieved from the unit.
4. Select **Save**. IPScom will save the (.ifg) file to the selected location and display a confirmation screen.

Enable IPsec Security from the HMI

IPsec Security can also be enabled from the front panel HMI. The settings to enable IPsec Security are located in the COMMUNICATIONS/Port Settings/Comm Ports Security/Protocol Access menu.

Legal Information

Patent

The units described in this manual are covered by U.S. Patents, with other patents pending.

Buyer shall hold harmless and indemnify the Seller, its directors, officers, agents, and employees from any and all costs and expense, damage or loss, resulting from any alleged infringement of United States Letters Patent or rights accruing therefrom or trademarks, whether federal, state, or common law, arising from the Seller's compliance with Buyer's designs, specifications, or instructions.

Warranty

Seller hereby warrants that the goods which are the subject matter of this contract will be manufactured in a good workmanlike manner and all materials used herein will be new and reasonably suitable for the equipment. Seller warrants that if, during a period of ten years from date of shipment of the equipment, the equipment rendered shall be found by the Buyer to be faulty or shall fail to perform in accordance with Seller's specifications of the product, Seller shall at his expense correct the same, provided, however, that Buyers shall ship the equipment prepaid to Seller's facility. The Seller's responsibility hereunder shall be limited to replacement value of the equipment furnished under this contract.

Seller makes no warranties expressed or implied other than those set out above. Seller specifically excludes the implied warranties of merchantability and fitness for a particular purpose. There are no warranties which extend beyond the description contained herein. In no event shall Seller be liable for consequential, exemplary, or punitive damages of whatever nature.

Any equipment returned for repair must be sent with transportation charges prepaid. The equipment must remain the property of the Buyer. The aforementioned warranties are void if the value of the unit is invoiced to the Seller at the time of return.

Indemnification

The Seller shall not be liable for any property damages whatsoever or for any loss or damage arising out of, connected with, or resulting from this contract, or from the performance or breach thereof, or from all services covered by or furnished under this contract.

In no event shall the Seller be liable for special, incidental, exemplary, or consequential damages, including but not limited to, loss of profits or revenue, loss of use of the equipment or any associated equipment, cost of capital, cost of purchased power, cost of substitute equipment, facilities or services, downtime costs, or claims or damages of customers or employees of the Buyer for such damages, regardless of whether said claim or damages is based on contract, warranty, tort including negligence, or otherwise.

Under no circumstances shall the Seller be liable for any personal injury whatsoever.

It is agreed that when the equipment furnished hereunder are to be used or performed in connection with any nuclear installation, facility, or activity, Seller shall have no liability for any nuclear damage, personal injury, property damage, or nuclear contamination to any property located at or near the site of the nuclear facility. Buyer agrees to indemnify and hold harmless the Seller against any and all liability associated therewith whatsoever whether based on contract, tort, or otherwise. Nuclear installation or facility means any nuclear reactor and includes the site on which any of the foregoing is located, all operations conducted on such site, and all premises used for such operations.

Notice:

Any illustrations and descriptions by Beckwith Electric are for the sole purpose of identification.

The drawings and/or specifications enclosed herein are the proprietary property of Beckwith Electric, and are issued in strict confidence; therefore, shall not be used as a basis of reproduction of the apparatus described therein without written permission of Beckwith Electric.

No illustration or description contained herein shall be construed as an express warranty of affirmation, promise, description, or sample, and any and all such express warranties are specifically excluded nor shall such illustration or description imply a warranty that the product is merchantable or fit for a particular purpose. There shall be no warranties which extend beyond those contained in the Beckwith Electric terms of sale.

All rights reserved by Beckwith Electric. No reproduction may be made without prior written approval of the Company.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

BECKWITH ELECTRIC
6190 118th Avenue North • Largo, Florida 33773-3724 U.S.A.
PHONE (727) 544-2326
beckwithelectricsupport@hubbell.com
www.beckwithelectric.com
ISO 9001:2015

© 2013 Beckwith Electric. All Rights Reserved.