rainforest
a u t o m a t i o n

EMU™
Energy Monitoring Unit

Technical Manual

Version 1.27
Sep 2012

Trademarks
Third-party brands and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Notice
The author(s) assumes no responsibility for any errors or omissions that may appear in this document nor does it make a commitment to update the information contained herein.

EMU™ – Energy Monitoring Unit

RFA-Z105
Version 1.27

Technical Manual

Table of Contents

Regulatory information

FCC Notices

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

FCC/IC RF Exposure Statement

This equipment complies with FCC and Industry Canada radiation exposure limits set forth for an uncontrolled environment. The antenna(s) used for this equipment must be installed to provide a separation distance of at least 8 inches (20cm) from all persons.

ICES-003 Compliance

This Class B digital apparatus complies with Canadian ICES-003.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Compliance Regulations For Australia and New Zealand

This equipment complies with the C-Tick labeling requirements for Australia and in New Zealand. As a radio transmitter, this device complies with the requirements of AS/NZS 4268:2008 as designated in the Radiocommunications (Short Range Devices) Standard 2004 for Australia and as required by the Radiocommunications Regulations (General Users Radio License for Short Range Devices) Notice 2011 for New Zealand. This device is a Category A device as defined in the Radiocommunications (Compliance Labeling - Electromagnetic Radiation) Notice 2003.

About This Manual

This manual is intended for those needing detailed technical information about the **EMU**™ product, such as customer support engineers and laboratory and field engineers performing evaluations and trials involving the **EMU**™. This manual is a companion to the *EMU*™ *User Manual*, and both documents should be consulted.

None of the information contained in this manual should be required by the average consumer to operate the **EMU**™ product under normal conditions.

About the EMU™

The **EMU**™ is a ZigBee endpoint that acts as an In-Home Display. It implements the ZigBee Smart Energy Profile 1.1. The supported clusters are shown on the next page.

The **EMU**™ is battery operated, and conserves power by going into Sleep Mode after four minutes of inactivity. In Sleep Mode, the display screen will be blank, but the Indicator LED Lights will continue to flash as documented in the Price Tier Indication section of this manual. The **EMU**™ also "pings" the smart meter once a minute while it is in Sleep Mode to ensure that meter is aware that the **EMU**™ is still in the network.

The Active Mode and Configuration Mode screens are described in detail in the *EMU™ User Manual*. This manual provides information about Diagnostic Mode, which is not intended to be used by non-technical users.

Supported Clusters

Cluster	clid	Client/Server	Commands	cmdid	Attribute Set	setid	Attributes read	atrid	
Basic	0x0000	Server	*Mandatory Commands*						
Identify	0x0003	Server	*Mandatory Commands*						
Time	0x000a	Client	Read Attributes	0x00			Time	0x0000	
							TimeStatus	0x0001	
							LocalTime	0x0007	
Key Establishment	0x0800	Client/Server	*Mandatory Commands*						
Simple Metering	0x0702	Client	GetProfile	0x00					
			GetProfileResponse (received)	0x00			EndTime		
							Status		
							ProfileIntervalPeriod		
							NumberOfPeriodsDelivered		
							Intervals		
			Read Attributes	0x00	Reading Information	0x00	CurrentSummationDelivered	0x00	
							CurrentSummationReceived	0x01	
							CurrentBlockPeriodConsumptionDelivered	0x0c	Block Price
					Meter Status	0x02	Status	0x00	
					Formatting	0x03	UnitofMeasure	0x00	
							Multiplier	0x01	
							Divisor	0x02	
							SummationFormatting	0x03	
							DemandFormatting	0x04	
							MeteringDeviceType	0x06	
					Historical Consumption	0x04	InstantaneousDemand	0x00	
Price	0x0700	Client	GetCurrentPrice	0x00					
			PublishPrice (received)	0x00			Price Trailling Digit and Tier		
							Start Time		
							Duration		
							Price		
							Currency		
							Number Of Price Tiers & Register Tier		
							Rate Label		
							Number Of Block Thresholds		Block Price
							Price Control		
			Attributes		Tier Label	0x00	Tier1PriceLabel	0x00	Price Label
							Tier2PriceLabel	0x01	
							Tier3PriceLabel	0x02	
							Tier4PriceLabel	0x03	
							Tier5PriceLabel	0x04	
							Tier6PriceLabel	0x05	
					Block Threshold	0x01	BlockNThreshold (1 <= N <= 5)	0x01-0x05	Block Price
					Block Period	0x02	StartOfBlockPeriod	0x00	
							BlockPeriodDuration (minutes)	0x01	
							ThresholdMultiplier	0x02	
							ThresholdDivisor	0x03	
					Commodity	0x03	Standing Charge	0x01	
					Block Price Information	0x04	NoTierBlockN+1Price (1 <= N <= 5)	0x00-0x05	
Message	0x0703	Client	GetLastMessage	0x00					
			Cancel Message (received)	0x01			MessageID		
							MessageControl		
			Message Confirmation	0x01					
			DisplayMessage (received)	0x00			MessageID		
							MessageControl		
							StartTime		
							Duration		
							Message		
Prepayment	0x0703	Client	Attributes		Prepayment Information Set	0x00	Payment Control	0x00	Prepay
							Credit Remaining	0x01	
							Credit Status	0x03	

Prepay	only enabled for prepayment support
Price Label	only enabled if Price Labels are used instead of Rate Label
Block Price	only enabled for block pricing support

Startup Procedure

Once the **EMU**™ has successfully completed its initialization procedures, the display will show the *Startup* screen. Normally, this is the Rainforest Automation logo:
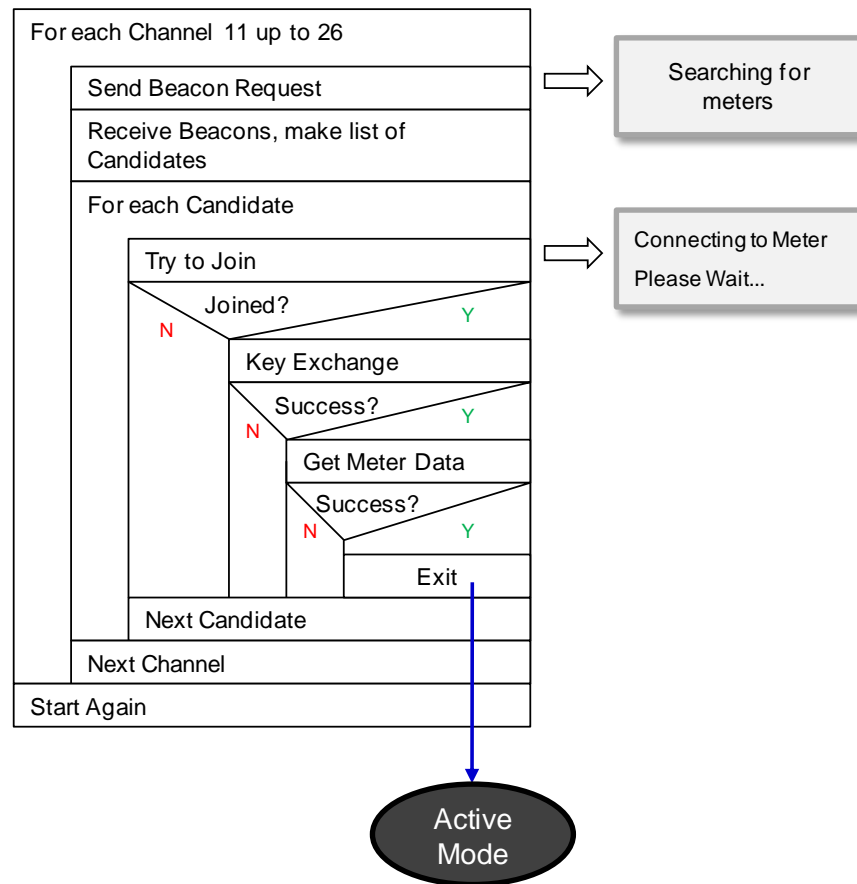

Then the Joining Procedure will begin.

The procedure is as follows:

- Send Beacon Request, and look for a device that has the 'join' flag enabled in its beacon.

- After joining the network, wait for the Coordinator to send the network key encrypted with our link key (derived from the install code).

- Look for the Key Establishment Cluster using match descriptor.

- Perform Key Exchange.

- If successful, look for the time cluster and the metering cluster.

- If successful, ask for time. The time needs to be a valid value.

- If successful, ask for metering, pricing, and messaging.

The flowchart for this procedure is shown below, along with the output screens that are displayed during the procedure:

The Joining Procedure is repeated continuously, cycling through all the channels (11-26), looking for candidates to join. If it has not joined after 6 minutes, the device will enter Sleep Mode, and the screen will go blank.

While in Sleep Mode, the device will initiate one scan of all the channels every 60 seconds. If a successful join occurs while in Sleep Mode, the device will enter Active Mode.

If one of the buttons is pressed during Sleep Mode, the device will enter Active Mode and will again loop continuously through all the channels, looking for a candidate to join. If it has not joined after 4 minutes, the device will return to Sleep Mode.

It is important that the device not be restarted (by removing and re-inserting the batteries, as described in the Troubleshooting Guide section of the *EMU™ User Manual*) during the Joining Procedure. This has unpredictable results, and may cause the device to be decommissioned, as if it had a Hard Reset.
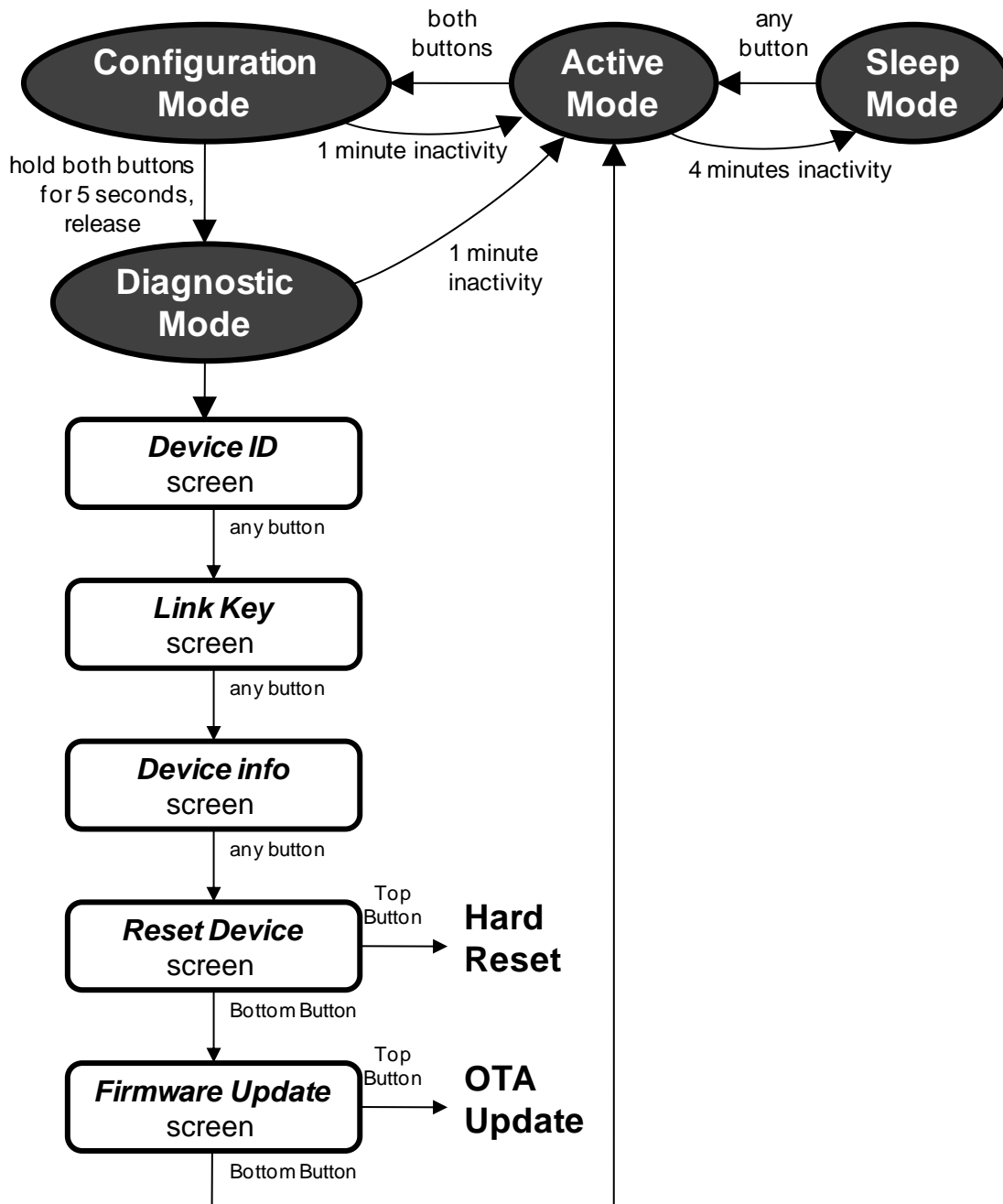
Diagnostic Mode

Diagnostic Mode provides a number of screens that give you technical details about the **EMU**™, and also provide access to advanced functions, such as Hard Reset and Firmware Update.

To get into Diagnostic Mode, you must first put the **EMU**™ into Configuration Mode. This is done by pressing and releasing both buttons simultaneously (note that this should not be attempted until the **EMU**™ has successfully connected to the smart meter). Once in Configuration Mode, hold down both buttons for at least five seconds. When the buttons are released, Diagnostic Mode will be initiated.

Note that the unit will automatically return to Active Mode after one minute of inactivity.

Navigation Flowchart

```
   both                                    any
  buttons                                 button

Configuration  ◄────────── Active ◄────────── Sleep
    Mode                    Mode               Mode
    │              1 minute inactivity
    │         ◄──────────────────►   ──────────────────►
    │ hold both buttons                4 minutes inactivity
    │ for 5 seconds,
    │ release
    ▼
 Diagnostic  ──── 1 minute
    Mode          inactivity
    │
    ▼
 Device ID
  screen
    │ any button
    ▼
  Link Key
  screen
    │ any button
    ▼
 Device info
  screen
    │ any button
    ▼              Top Button
 Reset Device ─────────────► Hard
  screen                     Reset
    │ Bottom Button
    ▼              Top Button
 Firmware Update ──────────► OTA
  screen                     Update
    │ Bottom Button
    └─────────────────────────►
```

EMU™ Diagnostic Mode Screens

Device ID

The *Device ID* screen shows the Install Code (IN) and MAC Address (MAC) for this particular device. Both are 16 digit hex numbers. Pressing any button sends you to the *Link Key* screen.

> Device ID
> IN:ee6d785b8006db6d
> MAC:00158d00001a56d7

Link Key

The *Link Key* screen shows the Preconfigured Link Key for this **EMU**™. It consists of 16 pairs of hex digits. Pressing any button sends you to the *Device Info* screen.

> Link Key
> 78:af:a4:da:a3:e9:0b:24
> 9d:15:20:0e:da:a8:74:d2

Device Info

The *Device Info* screen shows the revision number of the firmware (FW) installed on the device, as well as the hardware version (HW) of the **EMU**™. Pressing any button sends you to the *Hard Reset* screen.

> Device Info
> HW: 3.0.1
> FW: 1.2.12 (3094)

Hard Reset

The *Hard Reset* screen allows you to perform a Hard Reset by pressing the Top Button. Pressing the Bottom Button sends you to the *Firmware Update* screen.

> Hard Reset?
> Reset ➤
> Skip ➤

Firmware Update

The *Firmware Update* screen allows you to perform an OTA Upgrade by pressing the Top Button.

Note that this should only be done after carefully reading the Firmware Update section.

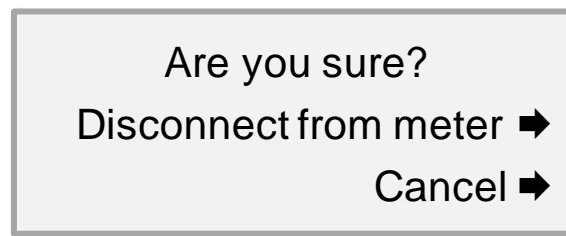Pressing the Bottom Button sends you Active Mode.

> Firmware Update?
>
> Update ➡
>
> Skip ➡

Hard Reset

A Hard Reset will erase all existing data and configurations on the **EMU**™. The device will be decommissioned and will not be able to immediately rejoin the smart meter. The smart meter will not allow the **EMU**™ to join until the meter has also decommissioned the **EMU**™, and then reregistered **EMU**™ for joining.

A Hard Reset can be initiated from the *Hard Reset* screen in Diagnostic Mode (see the previous section). Selecting "Reset" (Top Button) in the *Hard Reset* screen brings up the following screen that confirms that you intend to perform a Hard Reset and disconnect from the meter:

> Are you sure?
> Disconnect from meter ➡
> Cancel ➡

Pressing "Cancel" (Bottom Button) will abort the process and send you to Active Mode. Pressing the Top Button will erase all existing data and configurations, disconnect from the meter, and reset the **EMU**™.
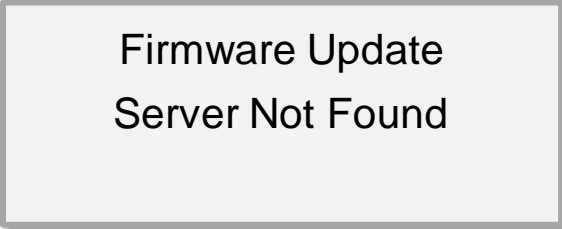
If for some reason the **EMU**™ is unresponsive and it is not possible to get to the *Hard Reset* screen, then this alternative procedure can be used:

a) Open the battery cover

b) Remove **all** of the batteries

c) Wait 10 seconds

d) Press and hold down the Top Button

e) While holding down the Top Button, replace the batteries and cover

f) Once the display comes on, release the Top Button (this will be almost immediately after replacing the batteries)

g) The **EMU**™ will have performed a Hard Reset, and will be disconnected from the meter.
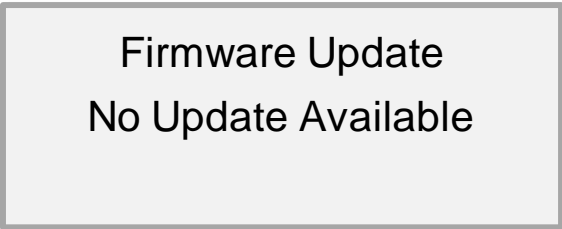
Firmware Update

A Firmware Update will replace all of the application code contained in the program memory of the **EMU**™. Once the process is started, it cannot be stopped; therefore, it is important that the charge level of the batteries is enough to complete the process. If there is any doubt, you should replace the batteries first.

The Firmware Update process is initiated by selecting "Update" (Top Button) in the *Firmware Update* screen in Diagnostic Mode (see the Diagnostic Mode Screens section). If the meter the **EMU**™ is joined to does not support firmware upgrades, you will see this screen:
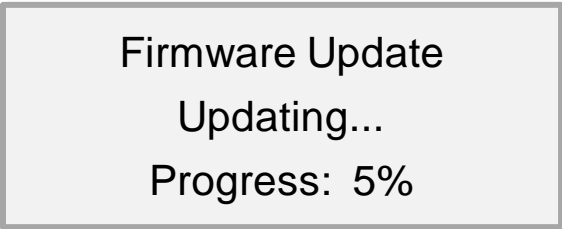
> Firmware Update
>
> Server Not Found

If the meter does support over-the-air upgrades, but there is no firmware image to upload at this time, you will see:

> Firmware Update
>
> No Update Available

Otherwise, the upload process will begin, and you will see:

> Firmware Update
>
> Updating...
>
> Progress: 5%

Once the update process has begun, it must be allowed to complete uploading the new code in order for the **EMU**™ to function correctly.

Do not attempt to reset the EMU™ during a Firmware Update!

The unit may reset itself during the upload procedure. If this happens, you can get back to the *Firmware Update* screen the same way as before, and you should see that the update is progressing.

After about 20 minutes, you should see the progress reach 100%. At this point the unit will return to active mode, and will reset to activate the update. The reset may be delayed if the update has been programmed by the utility to activate at a future time.

Manual Update Procedure

The **EMU**™ can also be updated using a USB Programming Dongle. The dongle emulates a meter, and acts as an update server. The dongle is available as a separate product (RFA-Z106-HP) from Rainforest Automation. The procedure below assumes that the dongle is being used with a PC running Windows XP or newer.

1. **Get Flash Programming Software**

   Go to this link: http://www.jennic.com/support/software/jn-sw-4007_flash_programmer

   Click on the download icon in the lower left corner of the web page and save the .ZIP file. Extract the files. You will have a folder named "JN-SW-4007-Flash-Programmer_*version*" (where *version* is the current revision number). Open the folder. Open "Tools". Open "flashprogrammer". Double click "FlashGUI.exe". You should see a screen like this:
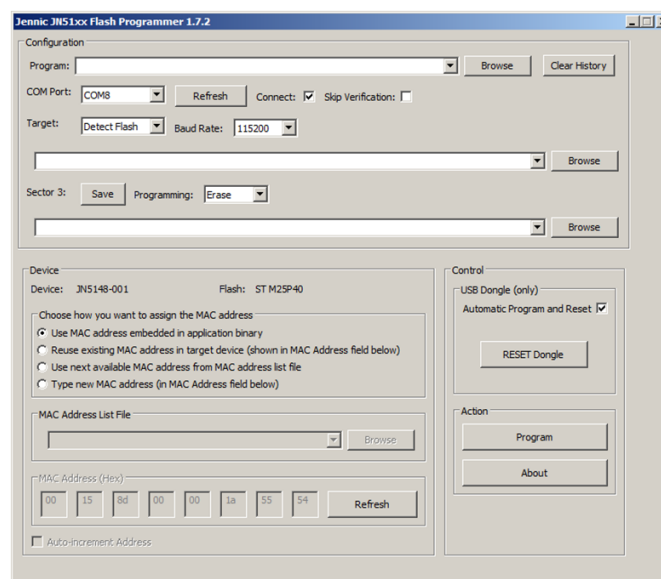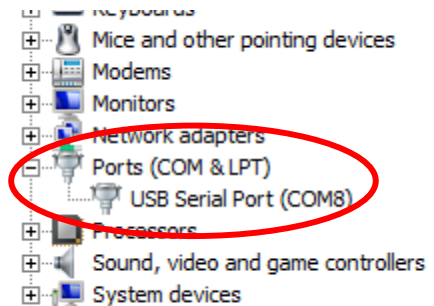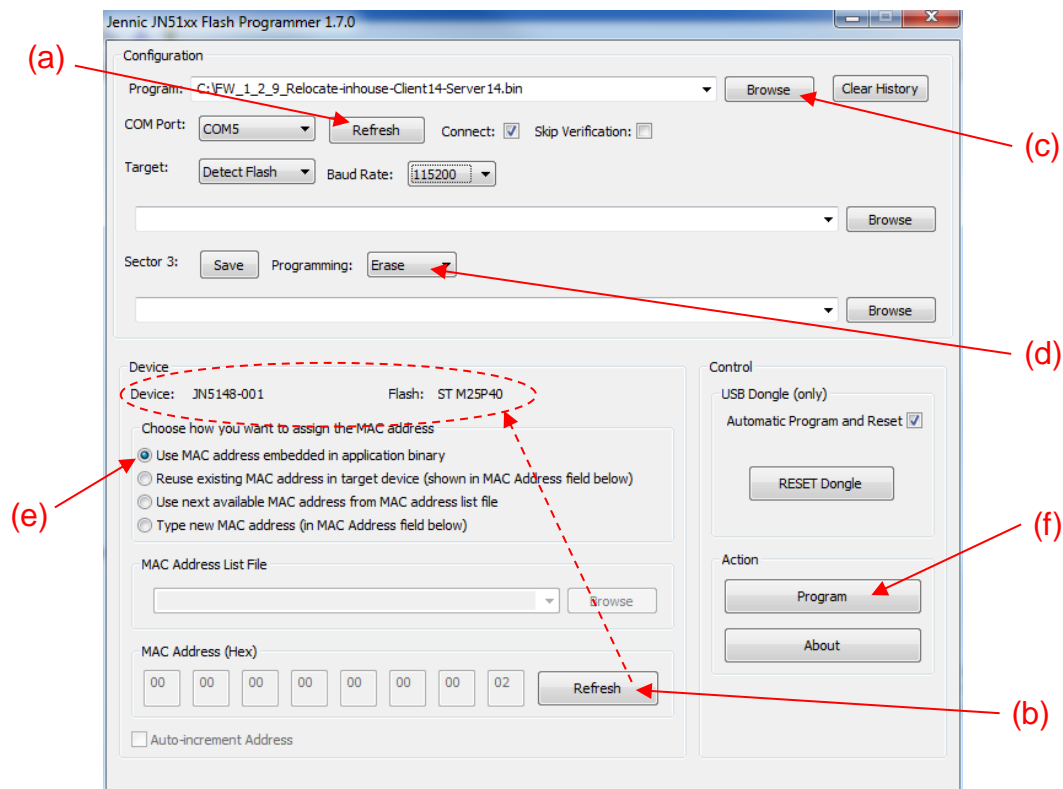
2. Connect the Dongle

Plug the dongle into an available USB port on the PC.

Open the Windows Device Manager (found in the Control Panel). Look for a USB Serial Port under "Ports (COM & LPT)" to find out which COM port has been assigned to the dongle. It should not be COM1 or COM2.

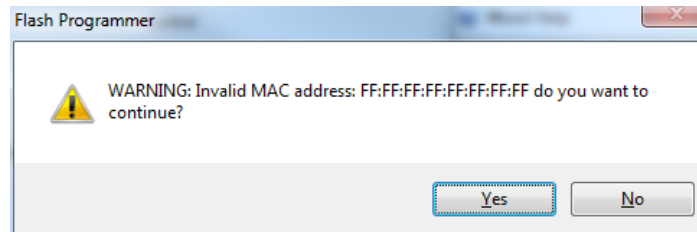## 3. Load Firmware Image onto the Dongle

Perform the following steps in the Flash Programming Software ("FlashGUI.exe"):

(a)   Click the COM Port Refresh button, and ensure that the correct COM port for the dongle is selected.

(b)   Click the MAC Address Refresh button, and ensure that a Device type and Flash number are indicated above.

(c)   Click the Browse button to select the .BIN firmware image file that you want to load onto the dongle.

(d)   Select "Erase" for Programming.

(e)   Select "Use MAC address embedded in application binary".

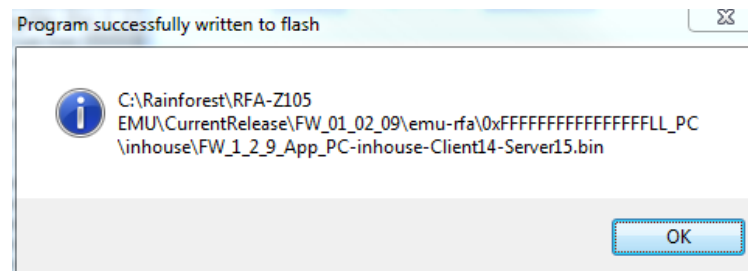(f)   Click the "Program" button.

You may see the following warning message. If so, just click "Yes".

A window will pop up showing the progress loading the dongle, followed by another that shows the program being verified:
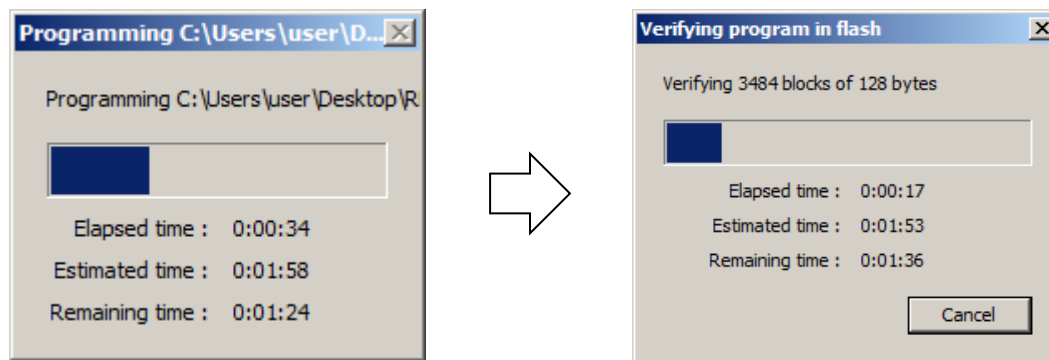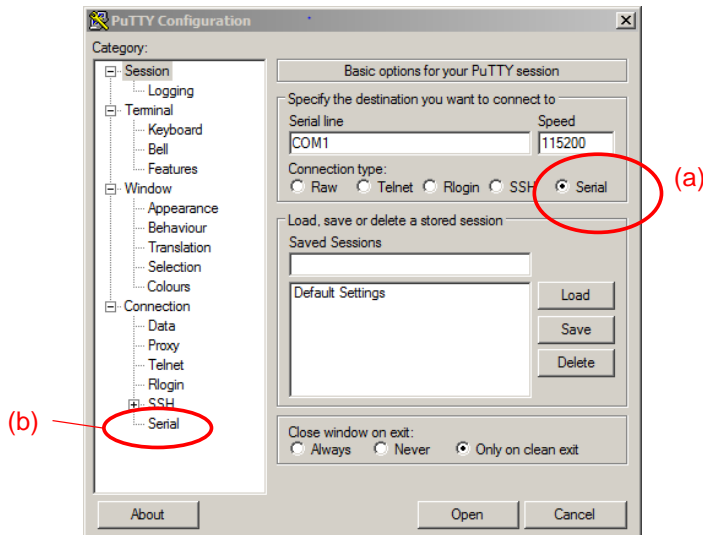

Eventually you will see a message like this. Click "OK".

The dongle is now loaded with the firmware image.

4. Connect a Terminal Emulator to the Dongle

The following steps describe how to use "PuTTY", a free terminal emulator, but any simple terminal emulator can be used.
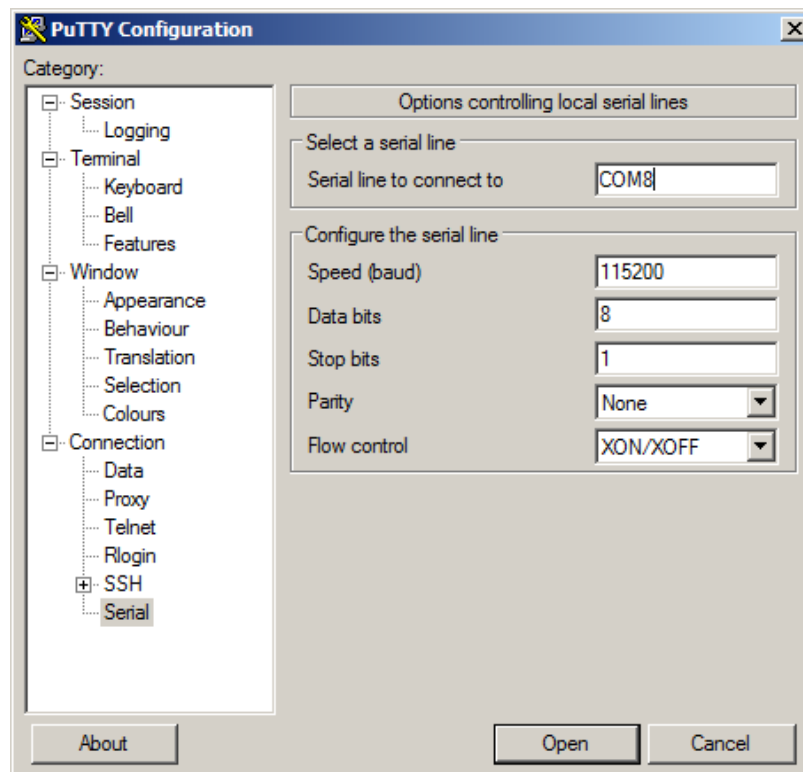
Go to this link:
http://www.putty.org/

Download "putty.exe", and run the file.

(a) Select "Serial" for the Connection type.

(b) Click on the "Serial" Category.

You should see the "Options for controlling local serial lines" (see below).

Ensure that "Serial line to connect to" is set to the correct COM port for the dongle, and the "Speed (baud)" is set to "115200". Click on "Open".

You should see a black PuTTY terminal window with a curser.

Copy this text into the terminal window (to paste into PuTTY, click the right mouse button):

```
<Command>
  <Name>factory_reset</Name>
</Command>
```

This should reset the dongle, and you will see text similar to this appear in the terminal window:

```
<Information>
  <Text>Network started</Text>
  <Channel>16</Channel>
  <PanId>0x7131</PanId>
</Information>
```

5. Join the EMU™ to the Dongle

Put the **EMU**™ into Diagnostic Mode, as described in the Diagnostic Mode section of this manual. Go to the *Link Key* screen, and record the two rows of numbers you see there.

Proceed to the *Hard Reset* screen and reset the **EMU**™, as described in the Hard Reset section of this manual. After the **EMU**™ has reset it will begin to beacon, and you will periodically see this type of announcement in the terminal window:

```
<Information>
  <Text>New node joined</Text>
  <NwkAddr>0x000059bd</NwkAddr>
  <MacId></MacId>
</Information>
```

Type the following text into a text editor and copy and paste it into the terminal window:

```
<Command>
  <Name>add_device</Name>
  <MacId>0x1234567890abcdef</MacId>
  <LinkKeyHi>0xfedcba0987654321</LinkKeyHi>
  <LinkKeyLo>0xabcdef0123456789</LinkKeyLo>
</Command>
```

Where: 1234567890abcdef is the 16-digit MAC Address shown on the label of the **EMU**™; and fedcba0987654321 is the 16 digits shown in the upper row of the *Link Key* screen; and abcdef0123456789 is the 16 digits shown in the lower row of the *Link Key* screen.

This will add the **EMU**™ to the dongle, and you should see this response in the terminal window:

```
<ApsTable>
<MAC>1234567890abcdef</MAC>
<KEY>fe:dc:ba:09:87:65:43:21:ab:cd:ef:01:23:45:67:89</KEY>
<MAC>ffffffffffffffff</MAC>
<KEY>00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00</KEY>
<MAC>ffffffffffffffff</MAC>
<KEY>00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00</KEY>
<MAC>ffffffffffffffff</MAC>
<KEY>00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00</KEY>
<MAC>ffffffffffffffff</MAC>
<KEY>00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00</KEY>
</ApsTable>
```

The **EMU**™ will then find the dongle and join to it, and you should see the three stages of the key exchange:

```
<Information>
  <Text>KEC Status</Text>
  <Type>1</Type>
  <CmdId>0</CmdId>
  <Status>0</Status>
</Information>
<Information>
  <Text>KEC Status</Text>
  <Type>1</Type>
  <CmdId>1</CmdId>
  <Status>0</Status>
</Information>
<Information>
  <Text>KEC Status</Text>
  <Type>1</Type>
  <CmdId>2</CmdId>
  <Status>0</Status>
</Information>
```

It is important that you see CmdId=0,1,2. At this point the **EMU**™ is joined to the dongle.

6. **Update the EMU™**

Put the **EMU**™ into Diagnostic Mode again and go to the *Firmware Update* screen. Press the Top Button to start the update, and you should see:
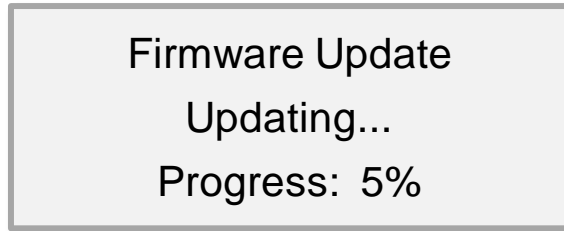
> Firmware Update
>
> Updating...
>
> Progress: 5%

Once the update process has begun, it must be allowed to complete uploading the new code in order for the **EMU**™ to function correctly.

After about 20 minutes, you should see the progress reach 100%. At this point the unit will return to active mode, and will reset to activate the update.

Price Tier indication

The **EMU**™ has three Indicator LED Lights arranged in a "stoplight" pattern; that is, red at the top, yellow in the middle, and green at the bottom:
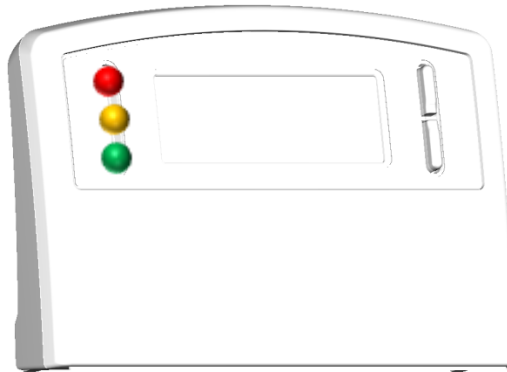
These lights flash, even when the **EMU**™ is in sleep mode, to indicate the current price tier. There can be up to 6 price tiers. For most tiers, a single light will flash; the duration and period of the flash depends upon the LED colour:

- Green – 20 millisecond flash every 60 seconds
- Yellow – 30 millisecond flash every 30 seconds
- Red – 30 millisecond flash every 5 seconds

The top tier is always considered Critical Peak, and is indicated by a double flash of the Red LED every 3 seconds.

# of tiers	tier 1	tier 2	tier 3	tier 4	tier 5	tier 6
6	green	green	yellow	yellow	red	double red
5	green	yellow	red	red	double red	
4	green	yellow	red	double red		
3	green	yellow	double red			
2	red	double red				
1						
0						

If the number of tiers is 1 or 0, then there is no tier indication flash from the Indicator LED Lights.

Note that if the price is set manually using the *Set Rate* screen, then the Green Indicator LED Light will flash once every 60 seconds while the manually set price is in effect.

Prepay Support

A firmware option is available for **EMU**™ to read the Prepayment Cluster (see the Supported Clusters diagram in the About the EMU section in this manual). If this is enabled in the firmware build, then the *Prepayment Information* attribute set is read from the meter. If the meter provides this information, then a new *Prepaid Balance* screen is shown between the *Current Price* screen and the *Message* screen:
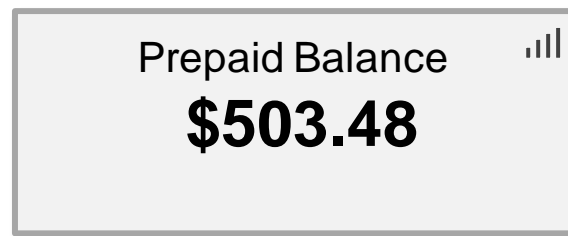
If the meter does not support the Prepayment Cluster, the **EMU**™ can still receive the *Prepaid Balance* information by using specially formatted text messages. This technique is called Message Tunneling. A text message can be sent to the Meter Control System, containing the account balance information, as well as a time stamp and corresponding meter reading, along with the appropriate meter number. The Meter Control System can forward the text message in the usual way to the meter, and the meter will deliver the text message via ZigBee to the **EMU**™.
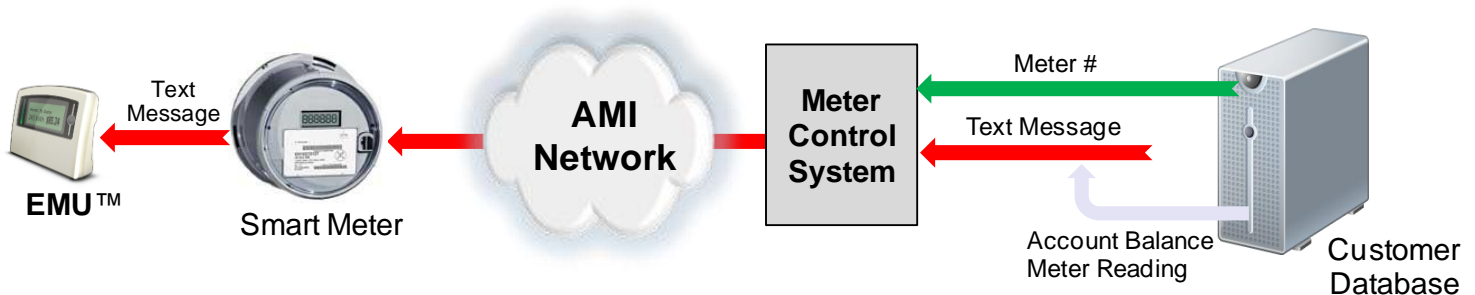
If Message Tunneling support is enabled in the **EMU**™, then the incoming text message is scanned, looking for the following pattern:

PREPAID BALANCE= $*xxx.xx* **(***mm/dd/yyyy-hh:mm:ss***)** *zzzzz***kWh**

Where:
- *xxx.xx* is the account balance in dollars
- *mm/dd/yyyy-hh:mm:ss* is the date and time stamp
- *zzzzz* is the last 5 digits of the meter reading

The information in the text message provides the data necessary for the **EMU**™ to provide the *Prepaid Balance* screen. The **EMU**™ can even estimate the up-to-date instantaneous balance between text message updates by calculating the difference in the meter reading from the last update, multiplying it by the effective price, and subtracting this from the last update balance.

Price Input Options

The **EMU**™ provides a number of methods to allow the input of a value for the commodity Price. This flexibility allows it to work with a variety of smart meter deployment configurations.

There is a hierarchy of Price input methods. Listed highest priority first, they are:

1) Meter Price Cluster support – this input overrides any of the others.

2) Text Message parsing – this input overrides manual input.

3) Manual input – this is the default for most deployments.

This hierarchy makes it easy to migrate from the simplest type of meter deployment (no Price support in the meter) to more sophisticated Price options with no changes to the **EMU**™.

Manual Input

For smart meter deployments with no pricing in the meter, the users can simply enter the commodity price themselves using the *Set Rate* screen in Configuration Mode, as described in the *EMU™ User Manual*. Besides being prone to user error, this method is only really practical for flat rate tariffs.

Text Message Input

A firmware option is available for **EMU**™ to allow the commodity Price and Price Tier to be set (simulating a Price Cluster *PublishPrice* Command) using specially formatted text messages. This technique is called Message Tunneling, and is much the same as alternative method for Prepay support mentioned in the previous section.

If Message Tunneling support is enabled in the **EMU**™, then the incoming text message is scanned, looking for the following pattern

CURRENT TIER *y*=**$***x.xxxx***/kWh**

Where:
- *y* is the Price Tier (1-5)
- x.xxxx is the Price in dollars ($0.0000 - $9.9999)

Using this method will overwrite any Price value that has been set manually using the *Set Rate* screen.

This method is particularly useful for implementing dynamic and/or Time of Use pricing in deployments where the price cluster has not been enabled in the meters.

Meter Input

The **EMU**™ issues a GetCurrentPrice command to the meter every 2 minutes. If the meter responds with a PublishPrice Command with pricing information, this new Price value will override any value that has been input manually or via text message. This makes migration to full in-meter pricing transparent and painless.