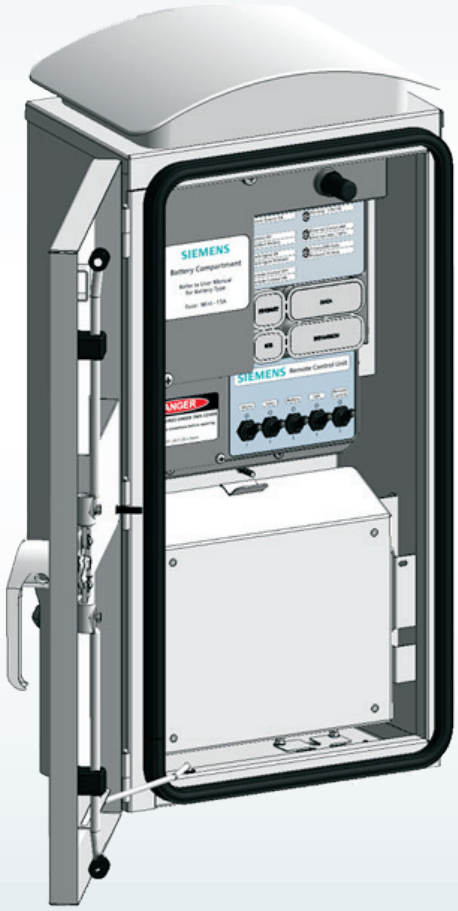
SIEMENS



www.usa.siemens.com/fusesaver

Instruction manual

Type 3AD8 remote control unit (RCU) probe instructions

Installation operation maintenance IC1000-F320-A201-X-4A00

Answers for infrastructure and cities.

Note:

These instructions do not purport to cover all details or variations in equipment, or to provide for every possible contingency to be met in connection with installation, operation or maintenance. Should further information be desired or should particular problems arise which are not covered sufficiently for the purchaser's purposes, the matter should be referred to the local Siemens sales office.

The contents of this instruction manual shall not become part of or modify any prior or existing agreement, commitment or relationship. The sales contract contains the entire obligation of Siemens Industry, Inc. The warranty contained in the contract between the parties is the sole warranty of Siemens Industry, Inc. Any statements contained herein do not create new warranties or modify the existing warranty.

Table of contents

Introduction	03
Installation and configuration instructions	04 – 07
Starting remote control unit (RCU) Probe	08 – 09
Using RCU Probe to view internal database	10 – 15
Diagnostics	16 – 17
Troubleshooting	18
RCU SCADA protocol testing	19
Support	19

Introduction

The Siemens remote control unit (RCU) enables communication between a power line protected by Fusesavers and a Utility's control room using a SCADA network. In order to help verify the correct configuration and operation of the SCADA communications to the RCU, the RCU Probe utility may be utilized.

The RCU maintains an internal protocol database which has data from both the Fusesavers and the RCU itself. The SCADA system can access this data with the SCADA protocol. Details of the SCADA protocol and the RCU protocol database are provided in the relevant RCU protocol manual.

RCU Probe is a PC utility that allows a user to directly connect to the RCU via Ethernet cable to view the current state of the protocol database. RCU Probe allows the user to override the value or qualifiers of all points in the protocol database in order to verify their change of state at the utility SCADA control room. The user may also send controls, times and view some general logging information.

The intended users of RCU Probe are the utility SCADA technical staff for the purpose of verifying the correct operation of the SCADA system, communications system and RCU itself.

NOTICE

RCU Probe is not to be used on an RCU in service since it has the capability to override the protocol database and mislead operations staff.

Installation and configuration instructions

RCU Probe is a PC application that allows a user to communicate with an RCU using a Cat 5 cable connected directly between the host PC Ethernet jack and the RCU Ethernet jack.

If uninterrupted connection to the Internet/ corporate network via Ethernet is required while using RCU Probe, then a PC with two Ethernet adapters will be required – one for the corporate network and one for connection to the RCU.

NOTICE

Connecting the PC to the RCU Ethernet port will expose the RCU or PC to damaging voltages if they are on different ground systems or ground systems exposed to voltage surges.

Consequently RCU Probe is not suitable for field installations and its intended use only in well-grounded workshop or laboratory environments.

Requirements

The following are the minimum requirements to run RCU Probe on your PC or laptop:

- Windows® 7, Windows® Vista or Windows® XP – service pack 3 or higher
- Functioning Ethernet jack (RJ45) and permissions to connect to non-networked device
- Cat 5 Ethernet cable
- PC administrator rights - install software, modify the IP properties and add programs to the Windows® firewall exceptions.

Older PC network adapters may not have an auto-sensing MDI/MDIX switch. In this case, a Cat 5 crossover cable or a network switch with two ports and an additional Cat 5 cable will also be needed.

The steps in order to use RCU Probe are:

1. Install the RCU Probe application.
2. Configure the RCU to allow RCU Probe connection.
3. Configure the host PC to allow communication to the RCU (i.e., firewall and Ethernet port settings).

RCU Probe installation

RCU Probe is supplied as a setup file which will self-install on the PC running the following Windows® operating systems:

- Windows 7
- Windows Vista
- Windows XP – service pack 3 or higher.

RCUProbe.zip file contents:

File	Description
dotNetFx40_Client_x86_x64.exe	An executable file for the installation on a PC
RCUProbeSetup.exe	An executable file for the installation on a PC
RCU Probe instructions.pdf	A separate manual with these installation instructions

Table 1: RCU Probe zip file contents

Install .NET

The .NET framework is normally already installed on Windows 7 operating systems. For Windows XP and Windows Vista, it may be necessary to carry out an installation. Launch the installation by clicking on the executable file (dotNetFx40_Client_x86_x64.exe) and following the Windows® installation instructions.

Install RCU Probe application:

- Unzip the install folder to a suitable place on your PC, such as your desktop, and open the RCU Probe folder which has been created.
- Run the RCUProbeSetup.exe self-extracting installation program (double-click it).
- If you have a previous version of RCU Probe installed, you do not have to uninstall it before installing the new version.
- The installation process offers to install RCU Probe to a standard location. Accept this default location unless you have a good reason not to.
- Accept the license agreement.

RCU Probe has now been installed. An icon has been placed on the desktop and in the program menu.

RCU configuration

In service, it is normal to have the RCU Probe connection disabled to prevent inadvertent or malicious changes to the protocol database. Consequently, the RCU configuration must be changed to allow RCU Probe operation.

RCU Connect is used to reconfigure the RCU to enable RCU Probe. See RCU operating instructions (IC1000-F320-A198-X-XXXX) for details on how to change the configuration.

The steps are as follows:

1. Turn on the RCU to be probed.
2. Start RCU Connect software.
3. Click the “Configure RCU” button on the main menu.
4. Select the RCU.
5. Set “RCU Probe Enable.”
6. Send the configuration to the RCU. This will restart the RCU and RCU Probe will be able to connect to the RCU.

If the RCU Probe Enable setting is not visible or is read only in RCU Connect, please contact +1 (800) 347-6659 or +1 (919) 365-2200 outside the U.S. who will provide a version of the RCU configuration template where this setting is available.

PC configuration

To connect to a RCU via RCU Probe, the PC must be configured correctly to enable the Ethernet connection to the RCU. This requires:

- The Ethernet network adapter must be configured to be on the same subnet mask as the RCU Ethernet port.
- The Windows® firewall must be configured to allow RCU Probe access to the network.

You will need to have PC administrator rights in order to complete the PC configuration.

Windows® 7

To configure the PC Ethernet adapter to work with the RCU, the following procedure may be used on a Windows 7 machine:

1. Go to Windows Control Panel and select "Network and Sharing Center."
2. Click on "Change adapter settings."
3. On the screen in Figure 1, right click and select properties of the Ethernet adapter, which is connected to the RCU. If you are not sure which Ethernet adapter is connected to the RCU, plug the Ethernet cable out and back in again while the RCU is on. The "Network Cable Unplugged" message will appear on the adapter you have just disconnected.

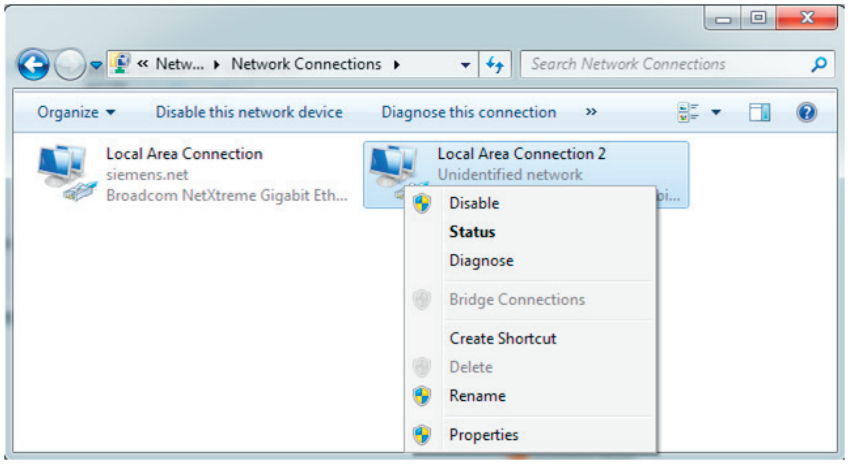


Figure 1

4. Highlight "Internet Protocol Version 4 (TCP/IPv4)" and press the "Properties" button (refer to Figure 2).

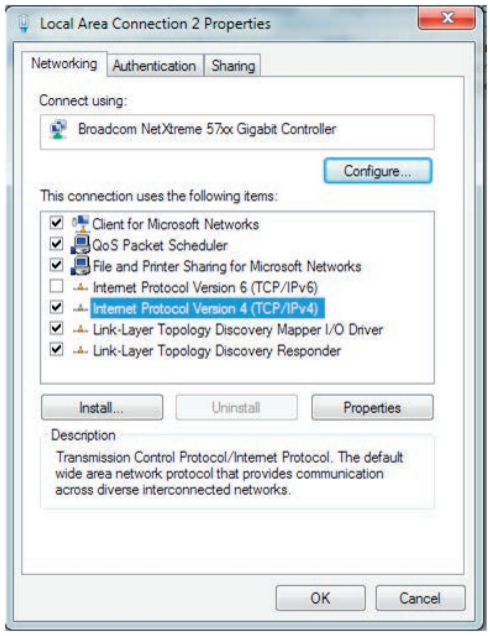


Figure 2

5. Set up the IPv4 settings as shown in the image in Figure 3. The IP address can be anything within the range of the subnet mask assigned to the RCU. The default IP address for an RCU with RCU Probe enabled is 192.168.100.36.

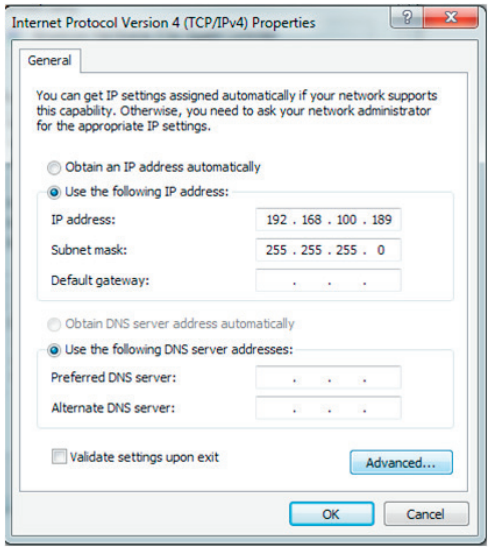


Figure 3

6. Click “OK” to save the settings.
7. Run the RCU Probe application. On first run of the application, the following security alert may be displayed shown in Figure 4. Tick the check boxes to allow RCU Probe to communicate on all networks and click the “Allow access” button.

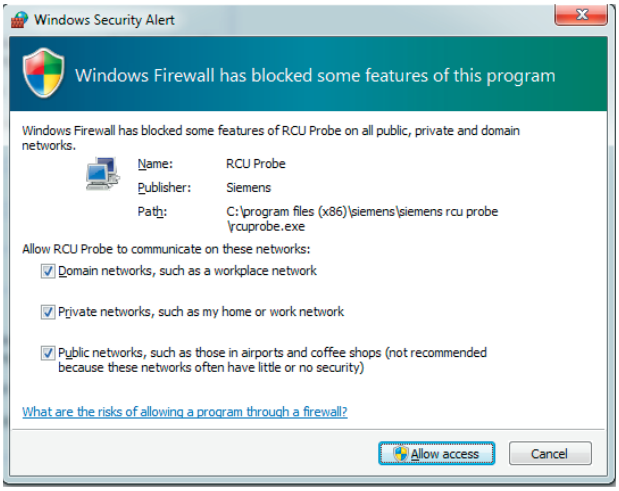


Figure 4

Windows® XP

To make the same changes as above on a Windows XP machine:

1. Go to Control Panel.
2. Click “Performance and Maintenance” and then click on “System.”
3. On the Hardware tab, click on “Device Manager.”
4. Double-click “Network Adapters.”
5. Complete the setup as for Windows® 7 starting at instruction 3.

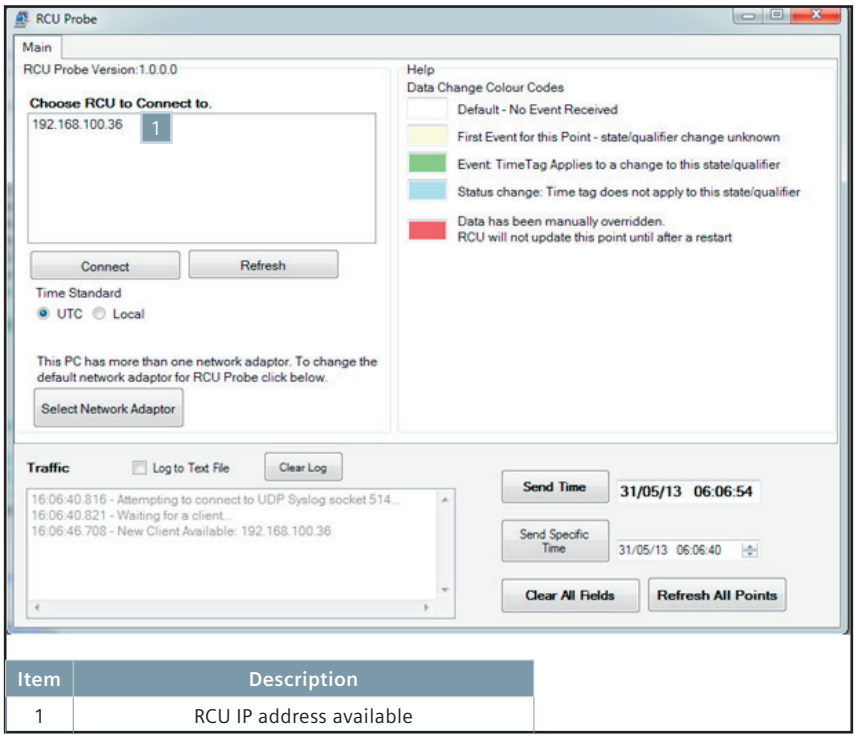
Windows XP does not give an option to modify “Internet Protocol Version 4 (TCP/IPv4).” Instead select “Internet Protocol (TCP/IP).”

Windows® Vista

To make these changes on a Windows Vista machine:

1. Open the Start Menu and right click on “Network” and select “Properties.”
2. On the following window, click “Manage Networks.” (Where is this graphic?)
3. Complete the setup as for Windows 7 starting at instruction 3.

Starting RCU Probe



Item	Description
1	RCU IP address available

Figure 5

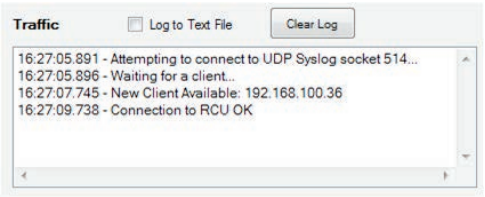


Figure 6

The following instructions are a step-by-step guide to setup and initiate a connection to a RCU via RCU Probe:

1. Turn on RCU power if not already on.
2. Install RCU Probe and configure your PC and RCU following the instruction in Installation and configuration instructions starting on page 4.
3. Connect a Cat 5 Ethernet cable between the RCU Ethernet port and your PC Ethernet port. Crossover cable or network switch may be needed on older PCs that do not have auto-sensing MDIX.
4. Start the RCU Probe application.
5. If the PC has more than one Ethernet port, you will be asked to select the network adapter. Select the Ethernet adapter that is connected to the RCU. The adapter IP address will be the one which configured in step 2. Refer to Selecting network adapter on page 9.
6. The RCU IP address should soon be available in the “Choose RCU to Connect to” list on the RCU Probe main screen. The default RCU IP address in 192.168.100.36.
7. Click on the RCU IP address and then press the “Connect” button.
8. If the RCU responds, the database tabs will be added to RCU connect and “Connection to RCU OK” will appear in the traffic display.
9. The RCU Probe is now connected to the RCU and will be retrieving database status data and events.

If connecting to the RCU has not been successful, please refer to the Troubleshooting on page 18 for your symptoms.

Selecting network adapter

On PCs that have more than one network adapter (e.g., Ethernet and Wi-Fi), it is necessary to select the port for RCU Probe to listen on and to send commands to the RCU.

If the PC only has one network adapter, the option to choose a network adapter will not be given and RCU Probe will default to the only available adapter.

A user will be asked to select the adapter the first time RCU Probe is started and this selection will be saved for every time RCU Probe is started thereafter. However, the user can modify this selection by pressing the "Select Network Adapter" button on the main screen.

When asked to choose a network adapter, the user will be given a choice of two or more network adapter IP addresses. Pick the appropriate adapter IP address and press the "Select" button (refer to Figure 7).

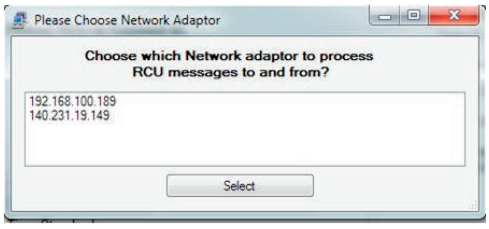


Figure 7

The IP address of the network adapter will be the IP address which was previously configured during the PC configuration for RCU Probe.

Selecting time standard

Typically, an RCU will have its internal clock time in UTC. The "Time Standard" setting can be used to apply the local PC time zone offset to time stamps received by RCU Probe.

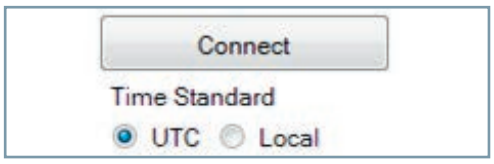


Figure 8

If the "Time Standard" is set to:

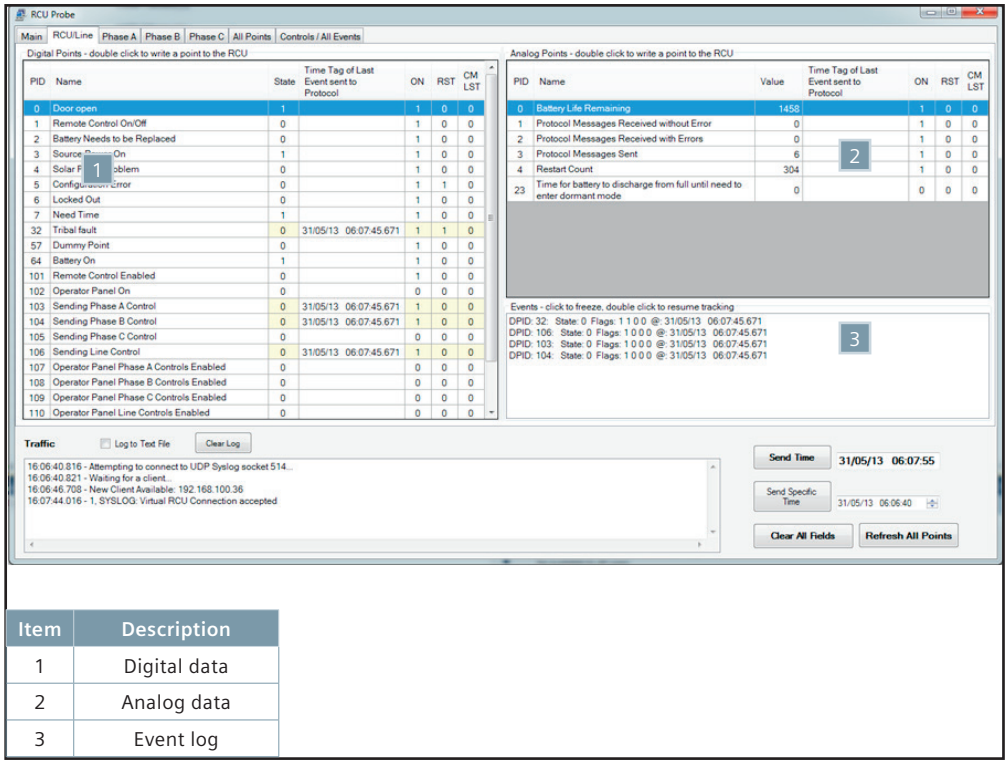
- UTC: the time stamps received by RCU Probe will not be adjusted by RCU Probe and will be shown "as is."
- Local: the time stamps received by RCU Probe are adjusted by the local PC time zone offset before being displayed. This will only be useful if the RCU is using UTC (and that is the normal mode for the RCU).

The RCU Probe clock shows host PC time in the time standard chosen. However, sending current time to the RCU via RCU Probe will always be sent as UTC.

Using RCU Probe to view internal database

RCU Probe gives a user a view into the internal database of an RCU. This allows the user to verify the status data and events that are being received via the SCADA network.

RCU Probe also gives the user the ability to manually override points and send controls and time to the RCU.



Item	Description
1	Digital data
2	Analog data
3	Event log

Figure 9

Database screen

Once connected, RCU Probe will immediately send a message to the RCU to get the current status of all internal database points. This status data will be available to be viewed across a number of tabs which show logical subsets of the database for ease of use.

- RCU/line: Digital and analog data and events that are derived from the RCU itself or where the data refers for the Fusesaver line.
- Phase A/phase B/phase C: Digital and analog data and events that refer to a particular phase Fusesaver.
- All points: Full list of all digital and analog data and events from the RCU internal database.

The database status screens in Figure 10 are split into two windows – one for digital points and one for analog points.

The time tag is only shown for points that have had an event generated. The time tag will be the time tag of the last event received for that point. If no events have been generated for a point, the time tag will be blank.

Each database point will be updated when the point changes or when an event is generated for the point. To ensure the RCU Probe database is correct and up-to-date, the "Refresh All Points" button can be used. The "Refresh All Points" button will update all points in the database.

The "Clear All Fields" button can be used to clear the state/value, time tag and qualifiers of all points on all RCU Probe screens. In this case, the "Refresh All Points" button must be pressed to get the current status again.

Figure 10

PID	Name	State	Time Tag of Last Event sent to Protocol	ON	RST	CM LST
0	Door open	1		1	0	0
1	Remote Control On/Off	0		1	0	0
2	Battery Needs to be Replaced	0		1	0	0
3	Source Power On	1		1	0	0
4	Solar Panel Problem	0		1	0	0
5	Configuration Error	0		1	1	0

The windows show the internal database point ID (PID), the name of the point, the state or value of the point, the time tag of the last event received for the point and the state of the qualifier flags.

The point qualifiers are represented as follows:

- ON: Online
- RST: Restart
- CM LST: Communications lost.

For explanation of the qualifiers, refer to the RCU protocol instruction manual (IC1000-F320-A200-X-XXXX).

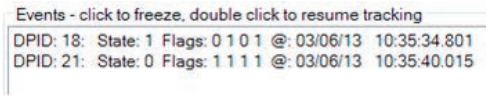
Note that the override qualifier is not shown in the display. Override is indicated by red color display.

Events

Most points in the RCU internal database generate events on change of state/value and always generate events on change of qualifiers. When connected, the RCU will send these events to RCU Probe. The events will contain the new state/value, qualifier flags and the time stamp for the event.

When RCU Probe receives an event, the event will be added to the events list on the "Controls/All Events" screen. The event will also be added to the events list on the screen which contains the points ID as part of the database subset (e.g., Phase A event will appear on the Phase A screen events list. The database status and time tag will also be updated with the new event data) (refer to Figure 11).

Figure 11



The event qualifier flags are represented in the following order:

Online – Restart – Communications Lost – Override

The event time tag will be adjusted to local time standard if local time standard is selected when connection to the RCU is made.

Color codes

Color codes are used to help determine what data has changed when an event is received. Events from the RCU contain the new state and qualifiers of the point. The event does not indicate if the event was due to a change in qualifier, state/value or both.

When RCU Probe receives an event, it compares the event data with the last event data it received for the point. Following this comparison, RCU Probe can determine what actually changed and highlight the data changes that caused the event.

A green highlight on a state/value or qualifier indicates that the last event for this point changed this state/value or qualifier (refer to Figure 12). The time tag for this point relates to changes to the green highlighted value/state or qualifiers. In the example, events were received for communications module A and B – Communications OK Restart flag cleared and state set. The other qualifiers were unchanged.

Figure 12

8	Communications Module A - Communications OK	1	31/05/13 06:07:48.457	1	0	0
9	Communications Module B - Communications OK	1	31/05/13 06:08:07.608	1	0	0
10	Communications Module C - Communications OK	0		0	1	0

Figure 13

4	RCU - Solar Panel Problem	0		1	0	0
5	RCU - Configuration Error	0	31/05/13 06:09:58.137	1	0	0
6	RCU - Locked Out	0		1	0	0

A yellow highlight indicates that this is the first event received for this points and the point change is unknown. As the event is the first event received for the point, RCU Probe has no previous event to compare against so cannot highlight which state/value or qualifiers changed. In the example in Figure 13, this is the first event received for RCU – Configuration Error.

Figure 14

5	Communications Module A - Battery Life Remaining	66	31/05/13 06:09:31.091	1	0	0
6	Communications Module B - Battery Life Remaining	85	31/05/13 06:10:08.689	1	0	0
7	Communications Module C - Battery Life Remaining	0		0	1	0

Sometimes a state/value or qualifier will be highlighted in blue. This indicates that the status of this data has changed but an event was not received. This may happen for points that do not generate events on status change or if the event is delayed (e.g., retrieval from Fusesaver).

A blue highlight indicates that the time stamp does not relate to the current state/value or qualifier that is highlight in blue. In the example above, communications module A – Battery Life Remaining had received an event that cleared the Restart flag. Following this, the status value changed to 66. The status change has been highlight in blue as this value does not correspond to the time tag adjacent (refer to Figure 14). The time tag still corresponds to the Restart Qualifier highlighted in green.

A red highlight (refer to Figure 15) indicates the point has its override flag set. The point data or qualifier has been overridden by the user with RCU Probe.

When a point has been overridden, the RCU will not update the state/value or qualifiers with valid data. The data will only be changed by subsequent override operations by the external tool. To clear the override flags and revert the points back to be updated with valid data, the RCU must be reset. In the example, Permanent Fault Occurred and Cleared Fault Occurred both have their override flags set.

Figure 15

15	Line Current On	0		0	1	0
18	Permanent Fault Occurred	1	03/06/13 10:35:34.801	0	1	0
21	Cleared Fault Occurred	0	03/06/13 10:35:40.015	1	1	1
24	Detected Fault Occurred	0		0	1	0

Strings

RCU Probe will download all RCU strings on connection. The “Get Strings” button can be pressed to update the strings after connection.

Some protocol database strings may get updated while the RCU is running. To view the updated strings in RCU Probe, the “Get Strings” command must be sent as the strings are not updated automatically on change of value.

Controls

RCU Probe gives the user the ability to send controls to the RCU in much the same way as a SCADA system would. Controls can be sent via the “Controls / All Events” screen.

To send a control, the user presses the desired control button. Feedback for the control can be viewed in the traffic box (refer to Figure 16).

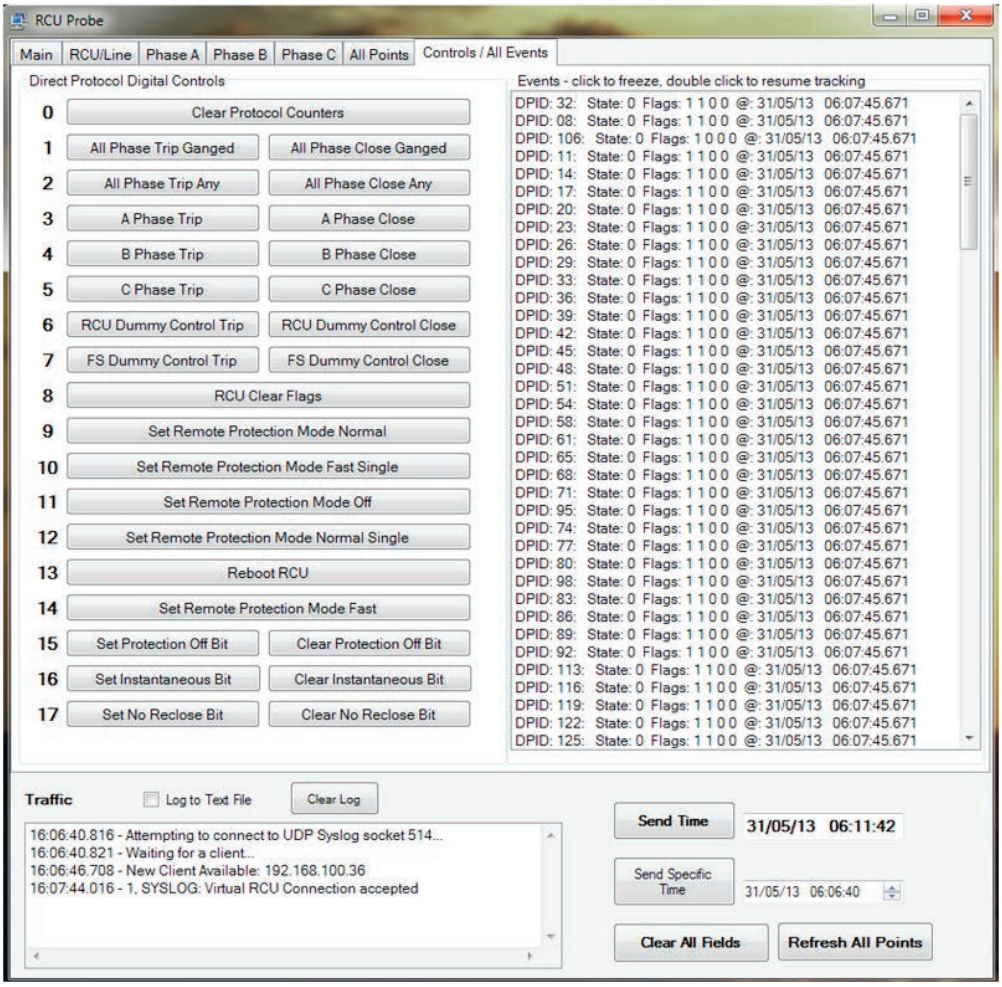


Figure 16

Override point data

RCU Probe gives the user the ability to manually override the state/value and qualifiers of points. To override a point, double click on the point row in the point status window.

A "Write Database point" window will pop up for the point that has been double clicked (refer to Figure 18). The default data to be written to the point will be the current status data. The user can modify the data to be sent and then press the send button to write the new data to the database point.

When a point has been overridden, the RCU will not update the state/value or qualifiers with valid data. The data will only be changed by subsequent override operations by the external tool. To clear the override flags and revert the points back to be updated with valid data, the RCU must be reset.

Sending time

The RCU internal clock is normally updated by the SCADA system. RCU Probe may also update time to the RCU.

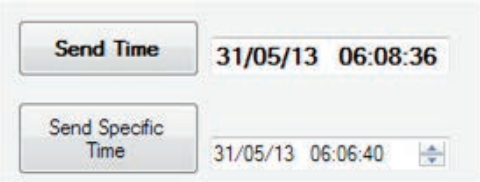


Figure 17

The "Send Time" button (refer to Figure 17) will send the current PC time in UTC standard to the RCU, regardless of the time standard selected on connection to the RCU.

It may be desired to send a specific time to the RCU for test purposes (e.g., to verify the SCADA system is updating time correctly). In this case, a specific time can be manually written to the "Send Specific Time" box and sent to the RCU.

Sending time to an RCU via RCU Probe will set the "Need Time" DPID in the protocol database. If connected to a SCADA system, the RCU time may be automatically changed back to SCADA time when the SCADA system registers that the "Need Time" point is set.

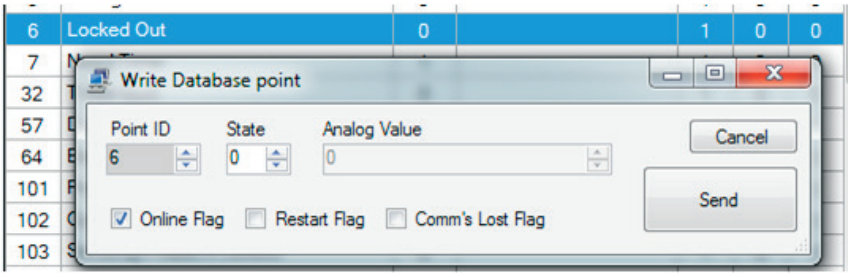


Figure 18

Disconnecting

When finished, RCU Probe can be disconnected from the RCU by pressing the "Disconnect" button on the main screen.

If the communications to the RCU failed while the RCU Probe is already in session (e.g., cable disconnected, RCU turned off), all database fields will darken to indicate that data is not being received anymore. If communications are re-established, the fields will lighten again. RCU Probe will not automatically disconnect if communications to the RCU are lost.

When finished probing an RCU, it is important to ensure that the RCU configuration is reverted to the standard configuration. If the RCU configuration is left with RCU Probe enabled, the RCU Ethernet port will be enabled which will affect power consumption of the RCU in the field.

Hints and tips:

- Clear list box: Right click on an event list or the traffic list and click "Clear Listbox" to clear the contents of the traffic list.
- Clear all fields: The "Clear All Fields" can be used to clear all of the database state/value and qualifier fields. The fields will be update when an event is received for the point or when "Refresh All Points" is pressed.

Diagnostics

RCU Probe - ping IP address

RCU Probe provides a mechanism to ping an IP address directly. Under some circumstances users may have difficulty communicating with an RCU due to corporate firewalls, incorrectly configured IP parameters, etc. The ping utility allows the user to verify that RCU Probe can or cannot communicate with the RCU IP address in question.

To use the ping IP address utility, press on the "Ping IP Address" button on the main screen (refer to Figure 19). Input the IP address of the RCU you are trying to communicate with. The default RCU IP address will be 192.168.100.36 unless manually configured otherwise.

Press the "Send" button to send a ping. The ping result list will output one of the following results:

- Ping reply from xxx.xxx.xxx.xxx in 0 ms: The ping was successful. The response time will normally be 0 ms on a direct Ethernet connection.
- No ping reply: The ping failed – the IP address may be wrong, firewall could be filtering the messages, RCU not powered up, etc.
- This is not a valid IP address. The IP address must be a valid IPv4 IP address.

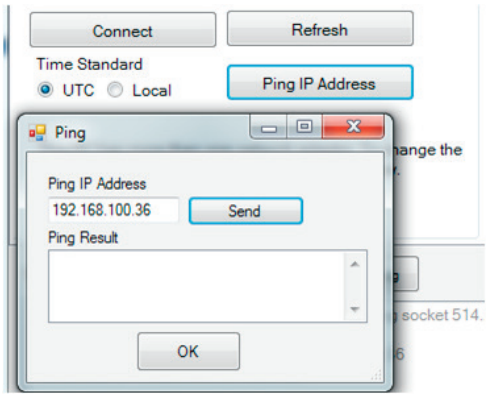


Figure 19

Ping RCU from command prompt

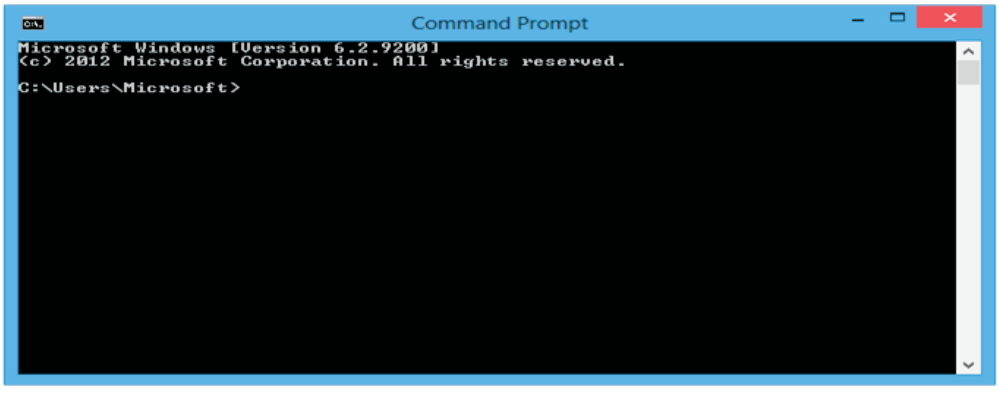
If RCU Probe is having difficulty communicating with an RCU, it is helpful to establish if the issue is with the RCU/PC configuration or with firewall permissions of the RCU Probe application.

By using the ping command from the command prompt, the RCU/PC configuration can be verified as the PC can send and receive messages to the RCU.

To ping an RCU from command prompt:

1. Click on Windows® "Start."
2. Click "Run" or (type run into the search in Windows® 7 or Windows® Vista).
3. Type "cmd" and press "OK."
4. The screen in Figure 20 should appear.

Figure 20



5. Type the following command: “ping 192.168.100.36” (or the IP address of the RCU that you have configured).
6. Press “enter.”

If the ping is successful, you will be presented with an output similar to the following in Figure 21 on the command prompt.

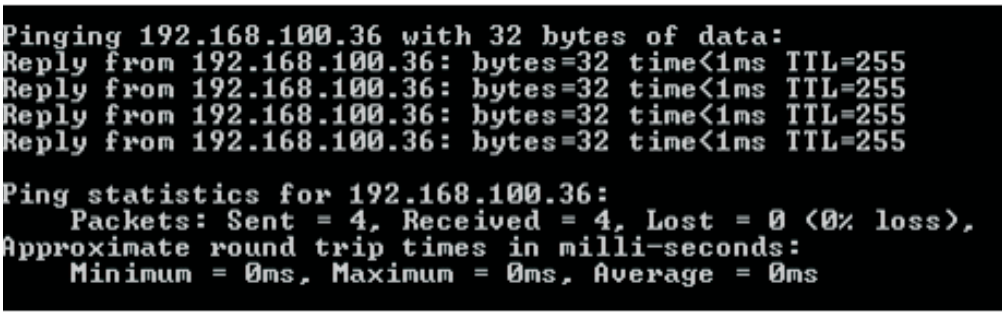


Figure 21

If the ping fails, you will be presented with an output similar to the following on the command prompt in Figure 22.

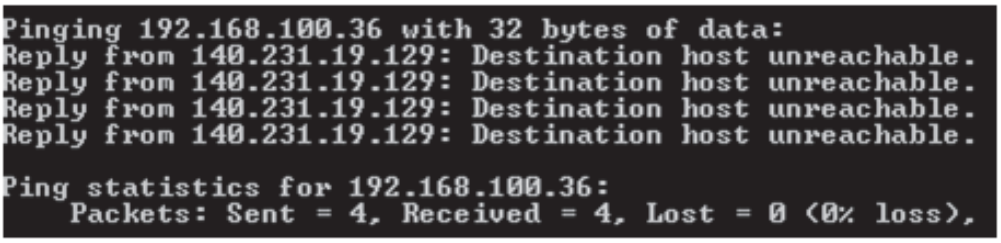


Figure 22

If the ping is successful, then communications between the RCU and the PC are OK, any issues with RCU Probe communications are most likely with the firewall permissions of RCU Probe.

However, if the ping fails, then this means that the PC cannot communicate with the RCU, which could be an RCU configuration, PC configuration, or a PC firewall problem.

Firewall permissions

The following instructions are for a PC using Windows® firewall.

If RCU Probe is not communicating with the RCU, it could be because Windows firewall is filtering out the messages to/from RCU Probe.

To check the firewall setting on your PC:

1. Go to Control Panel
2. Click “Windows firewall”
3. Click on “Allow a program or feature through Window firewall” or the “Exceptions” tab on Windows® XP.
4. Find RCU Probe in the programs list.

If RCU Probe name is not ticked, then it is likely that it is being blocked by Windows firewall. If all of the network groups are not ticked, then the unticked network could be blocking the RCU if it is on that network.

Note: RCU Probe uses communicates using UDP packets on port 514.

Troubleshooting

*For DNP3 protocols. If using another protocol, refer to the protocol manual for your protocol.

RCU IP address does not appear in "Choose RCU" list

There are a number of reasons which could cause this situation. As a first step, take note of any warning messages that pop up or that appear in the traffic log.

Use the following checklist to help diagnose the problem. The possible reasons for the symptoms could be:

1. Ethernet Connected LED on the RCU is not green.

- RCU power is off.
- RCU cable is not connected.
- RCU Probe is not enabled on the RCU.

2. Cannot ping RCU from command prompt. See Ping RCU from command prompt on page 16 from command prompt.

- PC is not on the same subnet mask as the RCU. Refer to page 6 step 5 of the Windows® 7 configuration instructions.
- PC does not have auto-sensing MDIX. In this case, you will need to use a Cat 5 crossover cable or a network switch to interface between the RCU and the PC.
- PC firewall is blocking communication to that IP address.

3. Cannot ping RCU from inside the RCU Probe application.

- PC firewall is blocking the RCU from communicating on with the RCU IP address or on the RCU Probe port (514).

Cannot connect to RCU IP address in choose RCU IP list

If you can see the RCU IP address in the address list but cannot successfully connect using the "Connect" button, the most likely cause is that the PC firewall is blocking some messages to or from the RCU.

Events in RCU Probe do not appear as SCADA events

If events are being received and displayed on RCU Probe events lists but they do not appear as SCADA events this could be:

- The SCADA protocol mapping has been modified to set some points to not generate events. Points that have been mapped to not generate events on the SCADA will still generate events in RCU Probe. Refer to protocol instruction manual IC1000-F320-A200-X-XXXX* and RCU Connect installation instructions in the RCU operating instruction manual IC1000-F320-A198-X-XXXX.

Sending time does not update RCU time.

If the time is not being updated to the time sent by RCU Probe it could be:

- Sending time to the RCU will set the need time point, DPID 7 in the RCU. If a SCADA system is connected to the RCU, it may update the RCU time automatically when it sees this point set. As such it may not be apparent that the time sent by RCU Probe has been accepted by the RCU as it immediately gets set again by the SCADA.
- The RCU Probe "Send Time" button sends UTC time, regardless of what is shown in the RCU Probe clock display, which can be in UTC or in local time.

RDU SCADA protocol testing

General

RCU Probe can alter the state/value and qualifiers of the RCU internal database and send controls to the RCU. RCU Probe should not be used on a site in-service.

When finished with an RCU Probe session, the RCU should be restarted to ensure any overridden protocol database points are reset and control of the point given back to the RCU.

When protocol has been verified, the RCU should be configured to "RCU Probe Disable."

Workshop testing

When integrating RCUs onto the SCADA network, it is recommended to first verify the SCADA system can successfully communicate with a RCU using the SCADA protocol in question.

To verify this SCADA protocol, the following example guidelines are given. The following is a basic example for the DNP3 protocol and will need to be adjusted for your protocol and the SCADA system requirements.

1. Perform integrity poll to read all digital and analog point status data.
2. Use RCU Probe to modify all digital and analog database points that have been mapped to the SCADA protocol. Verify these events are sent to the SCADA system after an event poll or unsolicited if enabled.
3. Read a specify database point verifying the result with RCU Probe for that point. Repeat for a number of points.
4. Send controls to each and every control point. RCU Probe can be used to monitor if the control is been received. It is recommended to have Fusesavers configured to work with the RCU in order to fully verify the controls to Fusesavers.
5. Synchronize time with the RCU. RCU Probe can be used set the time of the RCU an old time/data using the "Send Specific Time" button. Verify the RCU is now using an old time by overriding a point to generate an event with time tag. Update the time in the RCU using the SCADA system and again verify the time is now correct by generating some events with time tags.
6. Get all device attributes (strings). Read all of the RCU strings using the "get all device attributes" command.

Support

Contact regional service centers, sales offices or the factory for details, or telephone Siemens field service at +1 (800) 347-6659 or +1 (919) 365-2200 outside the U.S.

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract.

All product designations may be trademarks or product names of Siemens AG or supplier companies whose use by third parties for their own purposes could violate the rights of the owners.

Siemens Industry, Inc.
7000 Siemens Road
Wendell, NC 27591

For more information, contact:
+1 (800) 347-6659

www.usa.siemens.com/fusesaver

Subject to change without prior notice.
Order No.:
IC1000-F320-A201-X-4A00