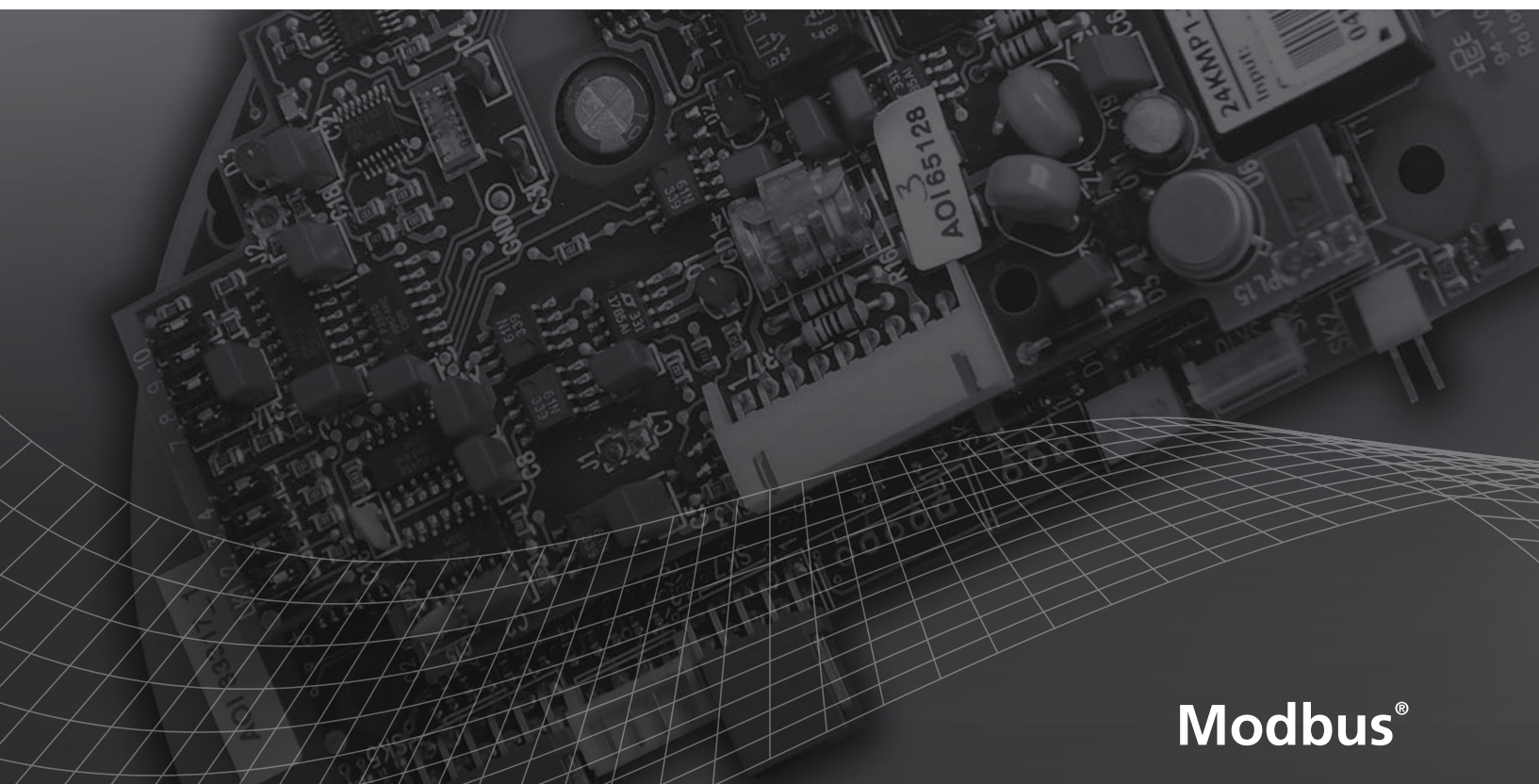# rotork ®

**Keeping the World Flowing
for Future Generations**

Modbus **TCP**
Start Up Guide

Modbus ®

**Ethernet communication and control
of Rotork actuators**

Contents

1. Introduction

Industrial Ethernet is becoming an increasingly popular choice for connecting industrial equipment together. It is also being used more frequently to connect field devices back to the control room.

Rotork has developed a solution that allows a Modbus TCP connection to its IQ and CK range of actuators.

Modbus TCP is an open standard that allows Modbus messages to be sent over a TCP/IP network. The Modbus TCP solution also incorporates a built in web server that allows individual actuators to have their own local webpage complete with status and diagnostic data.

Worldwide coverage

Our extensive international network enables us to think globally and act locally when it comes to supporting our customers. Rotork provides an efficient sales service, after sales commissioning and maintenance support throughout the life of our products.

Global manufacturing

Product reliability and integrity are priorities for Rotork product development. Our quality control teams source components from suppliers throughout the world to ensure our customers always receive first class automation solutions.

Customer support

Rotork provide service support solutions to maximise your productivity and reduce your operational risk.

Information about this manual

The information and instructions included in this manual are applicable for Modbus TCP equipped Rotork devices. For information or instructions on other Rotork products please visit www.rotork.com

1.   Introduction

Modbus TCP equipped Rotork actuators use a gateway to convert messages into Modbus RTU. Refer to the Rotork Modbus RTU manual (PUB091-004) to interpret information and commission the connected device. Modbus publications are available for download here:

https://www.rotork.com/products-and-services/control-networks/modbus/modbus-literature

The Netbiter AB7702 Gateway is the device that converts Modbus TCP messages into Modbus RTU messages. This gateway is usually integrated as part of the actuation solution. A manual providing further details about the operating conditions and settings for the Netbiter AB7702 module can be found here:

https://www.anybus.com/support/file-doc-downloads/gateway-specific/?ordercode=AB7702

⚠ **It is important that the person commissioning the actuator has an understanding of Ethernet/Modbus TCP and they know which IP address and Subnet are to be used. The gateway should only be connected into an existing network once all settings have been checked and confirmed as correct, otherwise communication issues may occur.**

2. Modbus TCP Gateway Configuration

2.1 Modbus TCP Installation

The Modbus TCP to Modbus RTU converter is installed within the actuator terminal cover. The Netbiter AB7702 and power supply module are fixed to a DIN rail. The AB7702 is wired onto the terminal bung of the actuator. An Ethernet cable should be passed through a cable entry on the terminal cover and used to connect the AB7702 module onto your network. The Ethernet connection for the AB7702 is found on the lower side of the module as labelled.

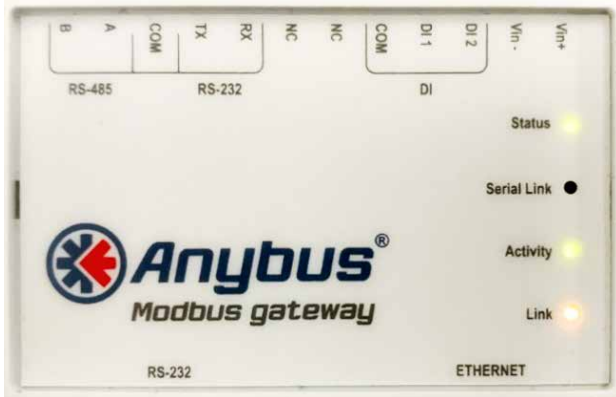There are four LEDs on the Netbiter AB7702 as depicted below:

Figure 1. Netbiter LED view

The LEDs should be in the following state when connected to the network in a normal operating state:

LED	Colour
Module Status	Solid Green
Serial link Status	Green or Orange
Activity/Collision	Flashing Green
Link	Solid Green or Solid Orange

Please refer to the Netbiter manual for full details of LED status.

2.2 Modbus TCP IP Configuration

IPconfig software should be used to detect any Netbiter gateway devices connected to the same subnet as the computer. IPconfig enables configuration of the Netbiter IP address and subnet. Default settings are:

IP address: 10.200.1.1
Subnet: 255.255.255.0

IPconfig can be downloaded from:
https://www.anybus.com/support/file-doc-downloads/gateway-specific/?ordercode=AB7702

All modules detected will be shown in the window. Click Scan to refresh the list.

Double clicking a module from the list will open up a window to edit the IP settings for the unit. Configure the correct settings and close the window.

Enter the Username and Password to edit settings. Default Username/Password is **admin**.
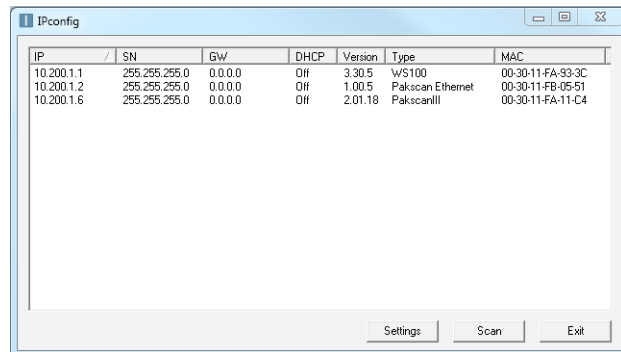

Figure 2. IPconfig window

The Modbus address of the actuator and the Netbiter IP address need to be known to communicate with the actuator via the AB7702.

The IP address is visible in IPconfig as detailed above.

All Rotork Modbus equipped actuators have a default Modbus address of 247. Always check the Modbus address of the device using the supplied tools and supporting manuals.

Once the IP and Modbus node address are known, the network can be tested.

Communication to the Netbiter AB7702 is only possible if the Ethernet configuration of the laptop/PC is set to communicate on the same subnet and IP address range.
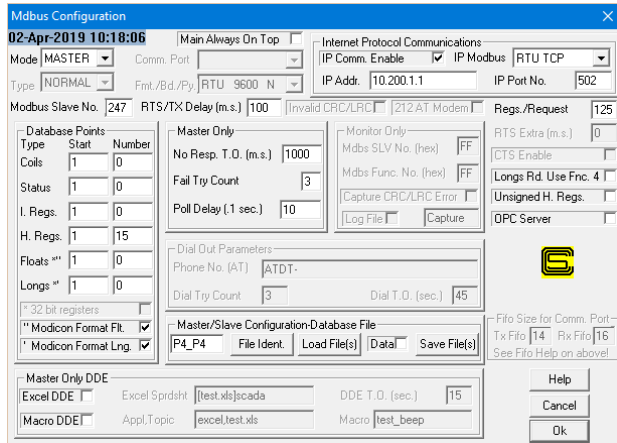
3. Example Network Test

Figure 3. Mdbus Configuration

This example shows a network test using a Modbus TCP master simulator tool (Mdbus). Other test tools are available.

Configure the Mdbus settings to match the Modbus TCP actuator.

As shown above, Mdbus has been configured to communicate with the AB7702 (10.200.1.1) and Modbus address 247.

Database Points need to be selected for cyclic communications. In the above example, 15 Holding Registers (H. Regs.) have been selected, starting at the first holding register. This refers to registers 0 to 14. *Refer to PUB091-004 for more information about each register.*

Select **Ok** when all the necessary configuration settings are populated to open the main Mdbus window.
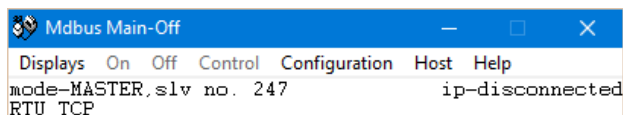

Figure 4. Mdbus Main window

Select **On** to start communications with the Rotork actuator. If a communication failure occurs, check the configuration settings are correct and cable connections from the PC to AB7702 and AB7702 to the actuator are correct and secure.

⚠ **NOTE: It may be necessary to add an offset of +1 to any data locations (coils or registers) listed in PUB091-004. This is because communication programs may begin address count at 1 instead of address count 0 within the actuator.**

4. Netbiter Webpages

4.1 Web Page Login

Use IPconfig to identify the IP address for the AB7702.

Open up a web browser and type the IP address into the address bar as shown below.
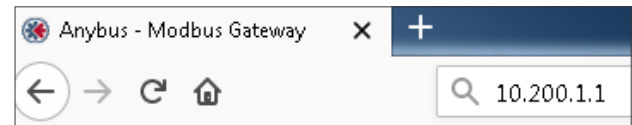

Figure 5. IP Address in web browser

The Netbiter login page will appear. Input the username and password for the device. Default access is listed below:

Username = **admin**
Password = **admin**

4.2 Start

Once valid user credentials are entered, the welcome page will appear.

Figure 6. AB7702 Welcome page

4.3 Network

Adjust the network settings of the connected AB7702 device.

Figure 7. Change IP Settings

⚠ **Note: Any change to the IP address settings of the AB7702 will require reconnection through a web browser and possibly further changes to the Laptop/PC Ethernet settings.**

4.4 Modbus

The Modbus RTU network settings should already be set to match the actuator. Any changes made to these settings will need to be mirrored in the actuator configuration.

Figure 8. Modbus RTU Settings

4.5 Status

Modbus connection status information.

Figure 9. View Modbus TCP Statistics

4.6 Admin

Change the password for the AB7702 device.

Figure 10. Change Password

4.7 About

View information about the AB7702 module.

Figure 11. AB7702 Information

5.   Ethernet Security

Always consider security of the Netbiter AB7702 Gateway when connecting it to an Ethernet network.

The user should ensure the Ethernet infrastructure is able to protect the Netbiter AB7702 Gateway from unauthorised access.

It is important to involve the local plant or site IT department in conversations about security of control system networks. The local IT department should be involved with securing access between the business network and the control system network. IT professionals will already be utilising cyber security measures to protect the business networks.

Coordination between IT and the control system team is important to ensure cyber security is managed properly and functions for all networks on site. Security policies may require modification if the exact same policy is not appropriate for the control system and business network.

For example, IT departments can use remote access to periodically maintain and update devices on the business network, these routine updates could disrupt the control system network. Control system updates to software and configuration must be strictly controlled and remote connection like this could introduce security risks to the control system.

The traditional priority for an IT department managing a business network is confidentiality, integrity and availability of data in the system. The same priority list is reversed for a control system network as availability of the data is the most important. The security of the system should not adversely affect the availability of data to users that need it. Confidentiality is less important as most of the control system data means nothing outside of the system.

The security guidance in this document is intended to help the user implement and maintain reasonable security of the Netbiter AB7702 Gateway, however, no security implementation can guarantee to protect against all existing, new or previously unknown threats. Rotork does not guarantee that adherence to these and any other security recommendations will protect the Netbiter AB7702 Gateway from security breaches and any subsequent impact on process in which the Netbiter AB7702 Gateway and associated ancillary components are involved with.

Examples of security policies that can be employed on site:

- All control systems must be segmented from the business network using a firewall and a DMZ network.

  Recommendation: All control systems must be segmented from the business network using a firewall/ UTM (Unified Threat Management) device which has built-in Intrusion Prevention, Intrusion Detection System and a two-tier DMZ network.

- All users should be trained on the site security procedures and policies.

- Different job and responsibility level users should have different user names and passwords, preferably per individual.

  Recommendation: Each user should have an individual user account with a strong password (minimum of 8 characters using a mix of upper case and lower case alphanumeric characters).

- Default passwords for user accounts must be changed during system installation or site acceptance tests.

  Recommendation: The end-user should always change the default password to a suitable strong password.

- Security events should be logged in a security audit file, these include invalid logins and changes to user accounts.

5.1   Security Environment Expected for the Netbiter AB7702 Gateway

The Netbiter AB7702 Gateway should be installed in an environment with suitable IT security protection to safeguard against internet attacks. Protection should include (but not limited to) DMZs and firewalls between the Netbiter AB7702 Gateway control system network and the plant network. A DMZ is an effective method of protection by separating networks. Direct connection between the Netbiter AB7702 Gateway and control system host is expected. Therefore, a DMZ and firewall is not required between these devices.

5.2   Defence in Depth

A defence in depth strategy utilises multiple layers of security so that a threat has to overcome more than one security mechanism. Defence in depth has 3 fundamental types of security safe guards:

1) Physical controls – the physical access of a device and the protection of the device. Normally achieved through protective measures such as site perimeter fences, locked control rooms and cabinets plus deterrence measures such as CCTV.

2) Technical controls – content access restriction of the system or device.

3) Administrative controls – policies and procedures of the organisation.

rotork®

www.**rotork**.com

A full listing of our worldwide sales and
service network is available on our website.