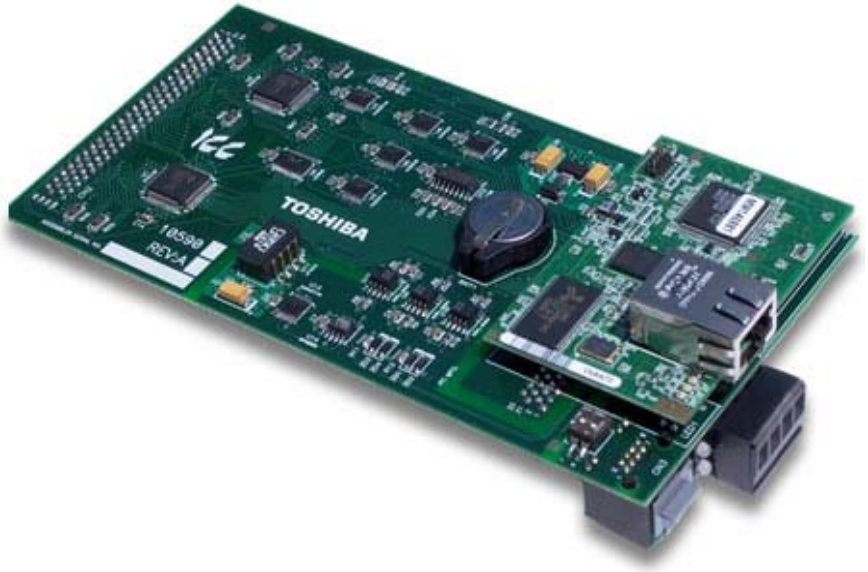
T300MVi

MEDIUM VOLTAGE ADJUSTABLE SPEED MOTOR DRIVE



MULTIPROTOCOL ETHERNET AND MODBUS RTU INTERFACE USER'S MANUAL

February 2006
ICC #10605-1.100-000

Important Notice

The Multiprotocol Ethernet and Modbus RTU Interface is a component of the drive system. Refer to the drive instruction manual for further information and precautions.

The instructions contained in this manual are not intended to cover all details or variations in equipment types, nor may it provide for every possible contingency concerning the installation, operation, or maintenance of this equipment. Should additional information be required contact your Toshiba representative.

The contents of this manual shall not become a part of or modify any prior or existing agreement, commitment, or relationship. The sales contract contains the entire obligation of Toshiba International Corporation. The warranty contained in the contract between the parties is the sole warranty of Toshiba International Corporation and any statements contained herein do not create new warranties or modify the existing warranty.

Any electrical or mechanical modifications to this equipment without prior written consent of Toshiba International Corporation will void all warranties and may void the UL/CUL listing or other safety certifications. Unauthorized modifications may also result in a safety hazard or equipment damage.

Misuse of this equipment could result in injury and equipment damage. In no event will Toshiba Corporation be responsible or liable for either indirect or consequential damage or injury that may result from the misuse of this equipment.

Manual's Purpose and Scope

This manual provides information on how to install, configure and communicate with the Multiprotocol Ethernet and Modbus RTU Interface. Refer to the drive instruction manual and MVI-EOI instruction manual for further information and precautions. This manual includes a section of general safety instructions that describes the warning labels and symbols that are used throughout the manual. Read the manual completely before installing, operating, or performing maintenance on this equipment.

This manual and the accompanying drawings should be considered a permanent part of the equipment and should be readily available for reference and review. Dimensions shown in the manual are in metric and/or the English equivalent.

Toshiba International Corporation reserves the right, without prior notice, to update information, make product changes, or to discontinue any product or service identified in this publication.

TOSHIBA is a registered trademark of the Toshiba Corporation. All other product or trade references appearing in this manual are registered trademarks of their respective owners.

Toshiba International Corporation (TIC) shall not be liable for direct, indirect, special, or consequential damages resulting from the use of the information contained within this manual.

Contacting the Customer Support Center

Toshiba's Customer Support Center can be contacted to obtain help in resolving any Adjustable Speed Drive system problem that you may experience or to provide application information.

The center is open from 8 a.m. to 5 p.m. (CST), Monday through Friday. The Support Center's toll free numbers are:

US.....(800) 231-1412 / Fax (713) 466-8773
Canada .....(800) 527-1204

You may also contact Toshiba by writing to:

Toshiba International Corporation
13131 West Little York Road
Houston, Texas 77041-9990
Attn: ASD Product Manager

For further information on Toshiba's products and services, please visit our website at www.tic.toshiba.com.

General Safety Instructions

DO NOT attempt to install, operate, maintain or dispose of this equipment until you have read and understood all of the product safety information and directions that are contained in this manual.

Safety Alert Symbol

The Safety Alert Symbol indicates that a potential personal injury hazard exists. The symbol is comprised of an equilateral triangle enclosing an exclamation mark.

Signal Words

Listed below are the signal words that are used throughout this manual followed by their descriptions and associated symbols. When the words **DANGER**, **WARNING** and **CAUTION** are used in this manual they will be followed by important safety information that must be adhered to.

The word **DANGER** preceded by the safety alert symbol indicates that an imminently hazardous situation exists that, if not avoided, will result in death or serious injury to personnel.


DANGER

The word **WARNING** preceded by the safety alert symbol indicates that a potentially hazardous situation exists that, if not avoided, could result in death or serious injury to personnel.


WARNING

The word **CAUTION** preceded by the safety alert symbol indicates that a potentially hazardous situation exists which, if not avoided, may result in minor or moderate injury.


CAUTION

The word **CAUTION** without the safety alert symbol indicates a potentially hazardous situation exists which, if not avoided, may result in equipment and property damage.

CAUTION

Special Symbols

To identify special hazards, other symbols may appear in conjunction with the **DANGER**, **WARNING** and **CAUTION** signal words. These symbols indicate areas that require special and/or strict adherence to the procedures to prevent serious injury to personnel or death.

Electrical Hazard Symbol

A symbol which indicates a hazard of injury from electrical shock or burn. It is comprised of an equilateral triangle enclosing a lightning bolt.

Explosion Hazard Symbol

A symbol which indicates a hazard of injury from exploding parts. It is comprised of an equilateral triangle enclosing an explosion image.

Equipment Warning Labels

DO NOT attempt to install, operate, perform maintenance, or dispose of this equipment until you have read and understood all of the product labels and user directions that are contained in this manual.

Labels attached to the equipment are there to provide useful information or to indicate an imminently hazardous situation that may result in serious injury, severe property and equipment damage, or death if the instructions are not followed.

Qualified Personnel

Installation, operation, and maintenance shall be performed by **Qualified Personnel Only**. A **Qualified Person** is one that has the skills and knowledge relating to the construction, installation, operation, and maintenance of the electrical equipment and has received safety training on the hazards involved (Refer to the latest edition of NFPA 70E for additional safety requirements).

Qualified Personnel shall:

- Have read the entire operation manual, as well as all other manuals supplied with this product.
- Be familiar with the construction and function of the ASD, the equipment being driven, and the hazards involved.
- Able to recognize and properly address hazards associated with the application of motor-driven equipment.
- Be trained and authorized to safely energize, de-energize, ground, lockout/tagout circuits and equipment, and clear faults in accordance with established safety practices.
- Be trained in the proper care and use of protective equipment such as safety shoes, rubber gloves, hard hats, safety glasses, face shields, flash clothing, etc., in accordance with established safety practices.
- Be trained in rendering first aid.

For further information on workplace safety visit www.osha.gov.

Disposal

Never dispose of electrical components via incineration. Contact your state environmental agency for details on disposal of electrical components and packaging in your area.

System Integration Precautions

The following precautions are provided as general guidelines for the setup of the ASD within the system.

- The Toshiba ASD is a general-purpose product. It is a system component only and the system design should take this into consideration. Please contact Toshiba for application-specific information and for training support.
- The Toshiba ASD is part of a larger system and the safe operation of the device will depend on observing certain precautions and performing proper system integration.
- A detailed system analysis and job safety analysis should be performed by the systems designer and/or systems integrator before the installation of the ASD component. Contact Toshiba for options availability and for application-specific system integration information if required.

Personnel Protection

- Installation, operation, and maintenance shall be performed by **Qualified Personnel Only**.
- A thorough understanding of the ASD will be required before the installation, operation, or maintenance of the ASD.

- Rotating machinery and live conductors can be hazardous and shall not come into contact with humans. Personnel should be protected from all rotating machinery and electrical hazards at all times.
- Insulators, machine guards, and electrical safeguards may fail or be defeated by the purposeful or inadvertent actions of workers. Insulators, machine guards, and electrical safeguards are to be inspected (and tested where possible) at installation and periodically after installation for potential hazardous conditions.
- Do not allow personnel near rotating machinery. Warning signs to this effect shall be posted at or near the machinery.
- Do not allow personnel near electrical conductors. Human contact with electrical conductors can be fatal. Warning signs to this effect shall be posted at or near the hazard.
- Personal protection equipment shall be provided and used to protect employees from any hazards inherent to system operation.

System Setup Requirements

⚠ WARNING

- The parameter settings affect how the drive operates. Only Qualified Personnel should set or change parameters.
- When using the ASD as an integral part of a larger system, it is the responsibility of the ASD installer or maintenance personnel to ensure that there is a fail-safe in place, i.e., an arrangement designed to switch the system to a safe condition if there is a fault or failure.
- System safety features should be employed and designed into the integrated system in a manner such that system operation, even in the event of system failure, will not cause harm or result in personnel injury or system damage (i.e., E-Off, Auto-Restart settings, System Interlocks, etc.).
- The programming setup and system configuration of the ASD may allow it to start the motor unexpectedly. A familiarity with the Auto-restart settings is a requirement to use this product.
- Improperly designed or improperly installed system interlocks may render the motor unable to start or stop on command.
- The failure of external or ancillary components may cause intermittent system operation, i.e.; the system may start the motor without warning.
- There may be thermal or physical properties, or ancillary devices integrated into the overall system that may allow for the ASD to start the motor without warning. Signs at the equipment installation must be posted to this effect.
- If a secondary magnetic contactor (MC) is used between the ASD and the load, it should be interlocked to halt the ASD before the secondary contact opens. If the output contactor is used for bypass operation, it must be interlocked such that commercial power is never applied to the ASD output terminals (U, V, and W).
- Power factor improvement capacitors or surge absorbers must not be installed on the output of the ASD.
- Use of the built-in system protective features is highly recommended (i.e., E-Off, Overload Protection, etc.).
- The operating controls and system status indicators should be clearly readable and positioned where the operator can see them without obstruction.
- Additional warnings and notifications shall be posted at the equipment installation location as deemed required by **Qualified Personnel**.

Operational and Maintenance Precautions

- Turn off, lockout, and tagout the main power, the control power, and instrumentation connections before inspecting or servicing the drive, or opening the door of the enclosure.
- Turn off, lockout, and tagout the main power, the control power, and instrumentation connections before proceeding to disconnect or connect the power wiring to the equipment.
- The capacitors of the ASD maintain a residual charge for a period of time after turning the ASD off. The required time for each ASD typeform is indicated with a cabinet label and a **Charge LED**. Wait for at least the minimum time indicated on the label and ensure that the **Charge LED** has gone out before opening the door of the ASD once the ASD power has been turned off.
- **Do Not** attempt to disassemble, modify, or repair the ASD. Call your Toshiba sales representative for repair information.
- Do not place any objects inside of the ASD.
- Turn the power on only after attaching (or closing) the front cover and **Do Not** remove the front cover of the ASD when the power is on.
- If the ASD should emit smoke or an unusual odor or sound, turn the power off immediately.
- The heat sink and other components may become extremely hot to the touch. Allow the unit to cool before coming in contact with these items.
- Remove power from the ASD during extended periods of non-use.
- The system should be inspected periodically for damaged or improperly functioning parts, cleanliness, and to ensure that the connectors are tightened securely.
- Ensure that the **Run** functions (**F**, **R**, **Preset Speed**, etc.) of the ASD are off before performing a **Reset**. The post-reset settings may allow the ASD to start unexpectedly.
- In the event of a power failure, the motor may restart after power is restored.
- **Retry** or **Reset** settings may allow the motor to start unexpectedly. Warnings to this effect should be clearly posted near the ASD and motor.

DO NOT install, operate, perform maintenance, set up, adjust, or dispose of this equipment until you have read and understood all of the product warnings and user directions. Failure to do so may result in equipment damage, operator injury, or loss of life.

TABLE OF CONTENTS

1. Introduction

The TOSVERT-300MVi Multiprotocol Ethernet and Modbus RTU Interface allows information to be transferred seamlessly between the drive and various fieldbus networks with minimal configuration requirements. In addition to the connection to the ASD, the unit provides a 10/100BaseT Ethernet port, one RS485 port, and one RS232 port. These various communication ports operate independently, and are configurable along with the unit's internal point database via a standard web browser.

The unit currently provides support for the following popular protocols:

- Modbus RTU (RS485 master & slave)
- Modbus RTU (RS232 master & slave)
- Modbus TCP/IP (slave)
- Ethernet/IP (server)

Before using the Multiprotocol Ethernet and Modbus RTU Interface, please familiarize yourself with the product and be sure to thoroughly read the instructions and precautions contained in this manual. In addition, please make sure that this instruction manual is delivered to the end user of the interface, and keep this instruction manual in a safe place for future reference or unit inspection.

The TOSVERT-300MVi Multiprotocol Ethernet and Modbus RTU Interface provides simultaneous support for many different communication protocols, allowing complex interchanges of data between otherwise incompatible networks. At the heart of the interface is an element called the "point database". The point database is entirely user-configurable, and provides the mapping information that allows requests from the various supported networks to be interpreted and stored in a common format. This allows data to be routed from any supported network to any other supported network.

Although the interface is hosted by and always in communication with the TOSVERT-300MVi drive into which it is installed, from a programming perspective the drive is just another "network" with which the interface board can communicate, and its configuration is therefore treated as such. Although this may appear unusual at first glance, maintaining this paradigm provides the benefit of uniform overall configuration and therefore comprehension of the entire network architecture. This advantage will especially become apparent when more than one network is simultaneously connected to the interface.

In addition to the point database's mapping capabilities, it also provides the added benefit of "data mirroring", whereby current copies of point values (populated by a "source port" designation) are maintained locally within the interface itself. This greatly reduces the request-to-response latency times on the various networks, as requests (read or write) can be entirely serviced

locally, thereby eliminating the time required to execute a secondary transaction on a different network.

When properly configured, the interface will become essentially “transparent” on the networks to which it is connected, and the various network devices can engage in seamless dialogs with each other.

2. Feature Summary

Ethernet Port

IEEE 802.3 10/100BaseT Ethernet compliant. Shielded RJ45 connector accepts standard CAT5-type 8-conductor unshielded twisted-pair (UTP) patch cables. Supports multiple simultaneous protocols.

RS485 Port

One optically-isolated half-duplex 2-wire RS485 port (A / B / Signal Ground / Shield). This port allows a selection of various master and slave protocols.

RS232 Port

One RS232 port that can be used to configure the unit, update the internal firmware, upload/download configuration files or act as a control protocol port.

Text-Based Console Configuration

Basic unit configuration is performed via a text-based console interface, available locally over the RS232 port via a standard PC terminal program such as Microsoft Windows HyperTerminal®, or remotely over Ethernet via a Telnet session. The unit also provides initial configuration access via ICMP ("ping") configuration.

Macromedia® Flash-Enabled Embedded Web Server

Advanced unit configuration and point monitoring/control are also provided via an embedded web server using the HTTP protocol. The unit's web server feature provides direct data access and control via standard web browsers such as Microsoft Internet Explorer and Netscape Navigator. The latest version of Macromedia Flash Player browser plug-in is required.

Configuration File Upload/Download

The interface's configuration can be uploaded from / downloaded to a PC, which provides the capability for PC-based file backup and easy configuration copying to multiple units.

Network Timeout Action

A per-port and per-point two-level configurable network timeout action can be programmed that allows each internal point to have its own unique "fail-safe" condition in the event of a network interruption.

Indicators

- 1 green "LNK" LED that is on whenever a valid Ethernet connection is detected.
- 1 green "SPD" LED that is on whenever a 100BaseT Ethernet connection is established.

- 1 amber “ACT” LED that flashes whenever data is transferred across the Ethernet network.
- 1 bicolor red/green “MS” LED that indicates module status information.
- 1 bicolor red/green “NS” LED that indicates network status information.
- 1 green “TX” and 1 “RX” LED on the RS232 port, which indicates RS485 port activity.

Refer to section 8 for more detailed information about the LED indicators and their meanings.

Field-Upgradeable

As new firmware becomes available, the unit can be upgraded in the field by the end-user. Refer to section 16 for more information.

3. Installation

Before opening the drive, please observe all safety precautions as outlined on the unit's front cover and in the operation manual. Installation of the interface should only be performed by a qualified technician familiar with the maintenance and operation of the drive.

1.  **CAUTION!** Verify that all input power sources to the drive have been turned OFF and are locked and tagged out.

2.  **DANGER!**  Wait at least 5 minutes for the drive's electrolytic capacitors to discharge before proceeding to the next step. **Do not touch any internal parts with power applied to the drive, or for at least 5 minutes after power to the drive has been removed. A hazard exists temporarily for electrical shock even if the source power has been removed.**

3. Open the drive's cabinet door (refer to the drive manual for instructions how to do this).

4. Press the interface board firmly onto the connectors marked CN4 and CN5 on the drive's control board.

5. Connect the various network cables to their respective plugs/terminal blocks. Ensure that any terminal blocks are fully seated into their respective headers, and route the network cables such that they are located well away from any electrical noise sources, such as ASD input power or motor wiring. Also take care to route all cables away from any sharp edges or positions where they may be pinched.

6. Take a moment to verify that the interface board is seated properly, and that all network cables have sufficient clearance from electrical noise sources.

7. Close the drive's cabinet door.

8. Turn the power source to the drive ON, and verify that the drive functions properly. If the drive does not appear to power up, or does not function properly, immediately turn power OFF. **Repeat steps 1 and 2 to remove all power from the drive.** Then, verify all connections. Contact Toshiba for assistance if the problem persists.

4. ASD Parameter Configuration

Note that whenever any of the parameters documented in this section are changed, they must be written to the EEPROM and the control board must be initialized (power cycled OFF and back ON again) before the changes will take effect.

4.1 General Configuration

`Program … Communication … Comm configuration … COMM_TYPE` must be set to `0400h`.

There are three possible conditions that can be created upon loss of communication or an internal board failure. The drive can be made to coast to a stop, ramp to a stop, or take no action. These different actions can be selected by changing the masking in the drive as follows:

- **Coast to stop:** `Program … Protection … Protection masking … MSK_READY1` should have its bits #14 and #15 set to unmask the TL_F1 and TL_F2 conditions. This is equivalent to adding `C000h` to whatever value the mask is currently set to.

- **Ramp to stop:** `Program … Protection … Protection masking … MSK_UVA4` should have its bits #12 and #13 set to unmask the TL_F1 and TL_F2 conditions. This is equivalent to adding `3000h` to whatever value the mask is currently set to.

- **Take no action:** Leave the above faults masked off. This option should generally be used only if the interface is being used solely for drive monitoring.

4.2 Receive (Command) Data Configuration

`Program … Communication … Comm addressing … Comm read addressing … SCAN_R_ADRS` must be set to `0`.

`Program … Communication … Comm addressing … Comm read addressing … SCAN_R_SIZE` must be set to the number of command items the drive is to receive. For example, if only two command words are to be sent to the drive, then this value can be set to 2. This will enable the first two `SCAN_RCVxx_AS` parameters, which are numerically indexed via the interface as parameters #1 and #2 (refer to section 15.3). Note that there is no penalty in setting this parameter to its maximum value (10): any “excess” parameters that are not written via the network will have no effect on the drive’s operation.

Program … Communication … Comm addressing … Comm read addressing … SCAN_RCV01_AS – SCAN_RCV10_AS should be set as needed to reference the desired command words. Any unused addresses should be programmed as DUST. These parameters correspond to parameter numbers 1 - 10 when configured in the interface's point database (refer to section 15.3). Note that although all 10 of these parameters (#1 - #10) can be written via the interface at any time, only SCAN_R_SIZE number of parameters will be recognized by the drive.

4.3 Write (Status) Data Configuration

Program … Communication … Comm addressing … Comm write addressing … SCAN_W_ADRS can be set to any value between 10 and 1010. A value of 10 is recommended.

Program … Communication … Comm addressing … Comm write addressing … SCAN_W_SIZE must be set to the number of status items the drive is to transmit. For example, if only four status words are to be received from the drive, then this value can be set to 4. This will enable the first four SCAN_WRxx_AS parameters, which are numerically indexed via the interface as parameters #11 through #14 (refer to section 15.3). Note that there is no penalty in setting this parameter to its maximum value (25). Also note that any parameter indexes larger than SCAN_W_SIZE that are accessed via the interface will always return value of 0. For example, if SCAN_W_SIZE is set to a value of 5 and ASD parameter #17 (corresponding to SCAN_WR07_AS) is accessed via the network, then the value returned will always be 0.

Program … Communication … Comm addressing … Comm write addressing … SCAN_WR01_AS – SCAN_WR25_AS should be set as needed to reference the desired status words. Any unused addresses should be programmed as DUST. These parameters correspond to parameter numbers 11 - 35 when configured in the interface's point database (refer to section 15.3). Note that although all 25 of these parameters (#11 - #35) can be read via the interface at any time, only SCAN_W_SIZE number of parameters will contain actual data.

5. RS485 Port Electrical Interface

In order to ensure appropriate network conditions (signal voltage levels, etc.) when using the interface's RS485 port, some knowledge of the network interface circuitry is required. Refer to Figure 1 for a simplified network schematic of the RS485 interface circuitry. Note that the "Shield" terminal has no internal connection: its purpose is simply to provide a cable shield chaining location between devices. The shield is then typically connected to ground at one location only.

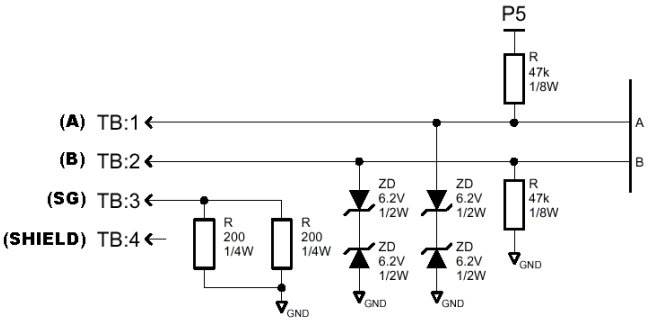


Figure 1: RS485 Interface Circuitry Schematic

Figure 2 details the specific network connections to the RS485 terminal block (TB1).

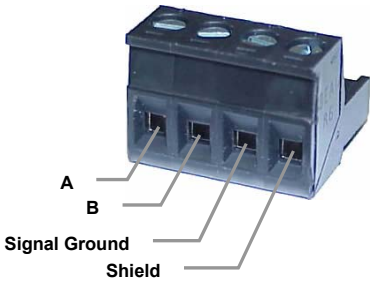


Figure 2: RS485 Terminal Block (TB1) Connections

6. Maintenance and Inspection

Preventive maintenance and inspection is required to maintain the interface in its optimal condition, and to ensure a long operational lifetime. Depending on usage and operating conditions, perform a periodic inspection once every three to six months. Before starting inspections, disconnect all power from the drive.

Inspection Points

- Check that the network cable(s) are properly terminated in the terminal block(s), and ensure that pluggable terminal blocks are fully seated in their headers. Reseat if necessary.
- Check that there are no defects in any attached wire terminal crimp points. Visually check that the crimp points are not damaged or loose.
- Visually check all wiring and cables for damage. Replace as necessary.
- Clean off any accumulated dust and dirt.
- Do not perform hi-pot tests on the interface, as they may damage the unit.

Please pay close attention to all periodic inspection points and maintain a good operating environment.

7. Storage and Warranty

7.1 Storage

Observe the following points when the interface is not used immediately after purchase or when it is not used for an extended period of time.

- Avoid storing the unit in places that are hot or humid, or that contain large quantities of dust or metallic dust. Store the unit in a well-ventilated location.
- When not using the unit for an extended period of time, apply power at least once every two years and confirm that it still functions properly.

7.2 Warranty

The TOSVERT-300MVi Multiprotocol Ethernet and Modbus RTU Interface is covered under warranty by Toshiba for a period of 12 months from the date of installation, but not to exceed 18 months from the date of shipment from the factory. For further warranty or service information, please contact Toshiba support.

8. LED Indicators

The interface contains several different LED indicators, each of which conveys important information about the status of the unit and connected networks. These LEDs and their functions are summarized here.

8.1 Ethernet Port Indicators

The Ethernet Port RJ45 connector has three LEDs positioned immediately below it.

SPD..... SPeeD: solid green whenever a 100BaseT Ethernet connection is established.
LNK..... LiNK: solid green whenever a valid Ethernet connection is detected.
ACT..... ACTivity: flashes amber whenever network activity is detected.

8.2 RS485 Port Indicators

The RS485 port has two green LEDs that indicate TX data and RX data activity. Note that although these LEDs are indeed associated with the RS485 port, they are physically integrated within the RS232 port's RJ45 connector. Refer to Figure 3 for the meanings and positions of these LEDs.

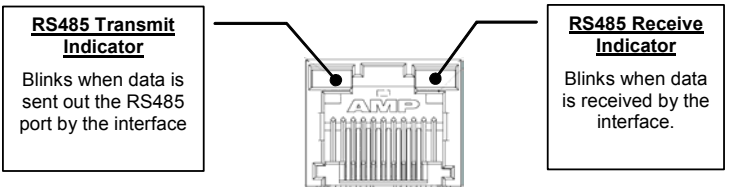


Figure 3: RS232 Port Indicators for RS485 Activity

NOTE that the RS485 receive indicator LED lights whenever the interface receives data on the port. This does NOT indicate the validity of the data with respect to any particular protocol or even whether or not the data is targeting this specific node. It simply shows that that data exists and is being detected. Also note that because the RS485 network is 2-wire (half-duplex), the interface will also indicate data reception whenever it transmits data.

8.3 Ethernet/IP Status Indicators

The back side of the interface board contains two bicolor red/green status LEDs. The lower LED (situated closest to the interface PCB) indicates the Module Status (MS), and the upper LED indicates the Network Status (NS). Refer to Figure 4. These LEDs conform to the prescribed behavior as dictated in the Ethernet/IP specification, Volume 2, Chapter 9.

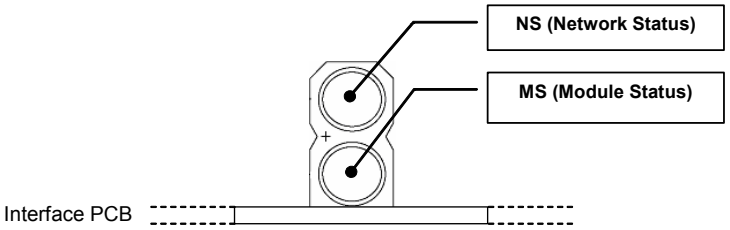


Figure 4: Ethernet/IP Status Indicators

9. Configuration Switches

There are two configuration DIP switches (marked “DS1”) located on the lower right-hand portion of the interface board, below the Ethernet port.

Switch #1..... Firmware update switch. Place in “OFF” position for normal operation, and in the “ON” position only when new application firmware is to be downloaded to the unit. Refer to section 16 for more information.

Switch #2..... RS232 port selection switch. When “OFF” at unit startup, the RS232 port will act as the serial console, regardless of the port’s configuration as indicated on the web interface (refer to section 13.1 for more information on the serial console). When “ON” at unit startup, the RS232 port carries whatever control protocol was assigned to it via the web interface. Note that the state of this switch is only detected when the interface boots up (from drive power-up or as the result of a soft reset, such as after a web page “submit” is performed).

10. Internal Battery

The interface has an internal coin-cell type battery that is currently only used to support the real-time clock when the unit is unpowered. This battery is designed to last the lifetime of the product under normal use. However, if the interface is left unpowered for several years, the battery may become exhausted. If the battery becomes discharged, it can be replaced by removing all power sources from the connected drive according the required safety procedures, and then carefully popping out the discharged battery and replacing it with a Panasonic BR1632 or equivalent component.

11. Unit Configuration Concepts

11.1 Port and Protocol Configuration

Each of the communication ports (or, in the case of the Ethernet port, the protocols) can be individually configured or enabled/disabled. It is important to note that the ports (and Ethernet protocols) function independent of one another, and can operate simultaneously. For example, a Modbus TCP/IP request, Modbus RTU slave request on the RS485 port, and an ASD request can simultaneously access the same internal point.

Although each communication port can be configured via the web interface, their configuration selections vary slightly. The ASD port has no configuration, and is always enabled. The RS232 and RS485 ports can be disabled, or can have one of a selection of control protocols assigned to them. The Ethernet port can by definition carry multiple control protocols simultaneously, and therefore each protocol it supports can be individually enabled or disabled.

Along with the protocol selection for the RS232/RS485 ports, each of these ports also has a corresponding baudrate, parity, address assignment and timeout time assignment. Note that not all assignable protocols support the same range of configuration options: therefore be sure to assign a valid entry in all cases (for example, a Modbus RTU slave's "address" assignment must be in the range 1-247 to comply with the Modbus specification).

Similarly, each of the Ethernet protocols has its own unique configuration attributes, such as Ethernet/IP's assembly object member lists and Modbus TCP/IP's timeout assignments.

11.2 Timeout Configuration

The interface's points can be configured to perform a specific set of actions when communications are lost on one or more of its various networks. This allows each point to have its own unique "fail-safe" condition in the event of a network interruption. There are three separate elements (four in the case of Modbus TCP/IP) that define the network timeout behavior:

- A port's network timeout time
- A point's "Timeout Enable" selection
- A point's "Timeout Value" setting
- For Modbus TCP/IP, a "Master IP" address designation

The ***timeout time*** adjustment range depends on the port. For the RS485 and RS232 ports, the time is adjustable in 1s increments from 0 to 500s. For the Modbus TCP/IP protocol, the time is adjustable in 1ms increments from 500ms-30000ms (0.5s-30.0s).

The default timeout time for the RS232 and RS485 ports is 0, which disables network timeout handling. When nonzero, timeout processing does not begin until after a valid network packet has been received by the unit on that port. In the case of Modbus TCP/IP, a "timeout" event will only be deemed to have occurred when a communication lapse or abnormal socket error takes place with the specific client device designated by the "Master IP" address: a communication lapse or abnormal socket error with any other client will not result in a timeout event.

When the timeout time is nonzero and a communication interruption is detected, the ***timeout enable*** selections for each point are inspected. Those points that are found to have their timeout enable selections set to "enabled" will then have their configured ***timeout values*** automatically written to their assigned "source port" objects. This mechanism provides for a flexible set of device failsafe conditions to be established on a point-by-point basis.

11.3 Point Configuration

As mentioned in section 1, the TOSVERT-300MVi Multiprotocol Ethernet and Modbus RTU Interface concept revolves around a central "point database", containing the value and access characteristics for each network. With respect to the interface, a "point" is simply an object that defines some sort of network access, mapping and configuration data, as well as a single "value" attribute that can be read from or written to by various communication ports or protocols.

The only restriction placed on this "central clearinghouse" concept is that only one port can autonomously update the point's value, "mirroring" its designated object for other protocols to access. What this means is that although any protocol can read from or write to a point's internal value, most of the time that point's value will simply be mirroring a remote data object that resides on one of the interface's subnets (or on the drive into which it is installed). The selection of what a specific point is to mirror is performed via its "source port" selection.

For example, a point may be configured to contain Toshiba ASD parameter mapping and Modbus master ID and holding register mapping information. However, because both of these protocols act as "master" protocols, only one of them can be allowed to continuously update the point's value. If both master protocols were allowed to simultaneously update the point's internal value, it would erratically alternate back and forth between the values designated by the Toshiba parameter and Modbus holding register objects. Any "slave" protocol (Modbus RTU slave, Ethernet/IP etc.) can read from or write to a point at any time, but only the protocol designated by the point's "source port" assignment will autonomously update the point's value independent of any other protocol traffic.

The "source port" designation also determines where a new point value will be written to when a "slave" protocol writes a new value to the point. For example,

if an Ethernet/IP connection consumes new data that changes the value of a point, how do we know where this new value will exit the interface to arrive at its final destination? The answer is that any new point values written by “slave” protocols will generate “write” transactions only on the “source port”.

This concept may best be further explained by way of a representative scenario. For example, let’s assume that the interface’s RS485 port has been designated to be a Modbus Master. Let’s further assume that the “Modbus Master” portion of point #5 indicates a “Source ID” value of 8 and “Register” value of 14, and that point #5’s “Source Port” selection is set to “RS485”. What this means is that independent of any other interface traffic, point #5 will continuously attempt to update its internal value by making requests to the RS485 port. And, because the RS485 port has been designated as a Modbus Master, then the “Modbus Master” portion of point #5’s configuration will be referenced by the update task, and point #5’s value will therefore always be mirroring the value of holding register #14 of remote Modbus station address #8 connected to the Modbus subnet attached to the interface’s RS485 port. Perhaps holding register #14 of Modbus station address #8 is a monitor item, indicating the pressure in compressor tank. Whenever the tank’s pressure changes, therefore, the value of point #5 will automatically update to reflect the new value read from the remote device. Once the tank’s pressure reading has been brought into the interface, it can then be retrieved by any protocol (or ALL the protocols) currently assigned to the interface’s other communication ports.

As a modification to the previous example, let’s assume this time that holding register #14 of Modbus remote station address #8 is the speed command of a conveyor belt. In this case, point #5 of the interface will be mirroring the current speed command of the conveyor, in a similar fashion to how it previously mirrored the compressor tank’s pressure. This time, however, the speed command represents something that can also be written to. Therefore, let’s assume that point #5 has been included in the output assembly member list of the Ethernet/IP protocol, and that a new data value is consumed by an Ethernet/IP connection object that causes the value of point #5 to be changed. In this case, this new point value will automatically cause a “write holding register” transaction to occur on the RS485 Modbus master port, updating the value of holding register #14 on remote Modbus station #8, causing the conveyor to accelerate (or decelerate) to the new speed.

Note that it is also perfectly acceptable to have a point’s “source port” assigned to “no source”. All this means that this point will not be autonomously updated (i.e. that it will not automatically mirror anything.) In a sense, it will simply be “scratchpad memory” that the various ports and protocols can use to exchange information among themselves. For example, a Modbus TCP/IP write transaction could update the value of such a point, which then can be inserted into the produced assembly data of an Ethernet/IP connection, causing the interface to act as a Modbus TCP/IP –to- Ethernet/IP router, while simultaneously performing its other network functions.

Although the various configuration possibilities may seem overwhelming at first, it is clear that the interface can perform powerful and flexible routing algorithms.

Through configuration experience, the “in” and “out” data flows will become more clear.

11.4 General Configuration Procedure

Now that we have had a brief tutorial on port and point configuration, we can proceed on to how these elements fit into the overall configuration procedure. The general configuration procedure steps can be summarized as follows:

1. Assign the initial Ethernet configuration via either the ARP ping method or console configuration method.
2. Access the embedded web server’s configuration page via a web browser.
3. Assign (or enable/disable) the desired protocols and their characteristics to the specific communication ports.
4. Perform the desired per-protocol mapping and definition assignments for each point, including the name, timeout and “source port” assignments.
5. Submit the changes to the interface, which will update its internal configuration file and reboot the unit.
6. Download a copy of the unit’s configuration file to your PC for backup purposes

Of course, it is possible to simplify or even eliminate some of these steps by starting your configuration from a pre-existing point database file (either downloaded from the internet or previously-created by the user), and then simply modifying those elements necessary to match your application.

12. Initial Ethernet Configuration

The interface typically requires configuration prior to communicating on an Ethernet network. This fundamental configuration is achieved via one of two possible methods: using ICMP ("ping") configuration via the Address Resolution Protocol (ARP), or via a text-based console interface, accessible over the RS232 serial channel and a telnet interface. The following are the factory-set values of the most important Ethernet parameters:

IP Address 192.168.1.100
Subnet Mask..... 255.255.255.0
Default Gateway 192.168.1.2

If these parameters are not compatible with your network settings, they will need to be modified.

12.1 ARP Method

The IP address can be changed remotely by using the Address Resolution Protocol (ARP). This is performed by adding a static entry into a PC's ARP cache table, which stores the associations between a device's IP and physical (MAC) addresses. The unit is then "pinged" from a command prompt (MS DOS™ window) to assign the new IP address to it. Below is an example of the commands used to change the unit's IP address:

```
arp -s <IP address> <MAC address>
ping <IP address>
arp -d <IP address>
```

The initial "arp –s" command adds a static association between the unit's MAC address and the desired IP address to the PC's ARP table. When the ping command is executed with the IP address as an argument, the PC sends this information to the unit indicated by the associated MAC address. The unit then detects that it was addressed with the correct MAC address and adopts the IP address indicated in the ICMP "ping" packet. The optional "arp –d" command then removes the static route from the PC's ARP table.

The unit's MAC address is printed on a long bar-coded label located just below the Ethernet connector, and just above DIP switch DS1. The label contains bar-coded information on its left side and 6 characters on its right side. The 6 characters represent the least-significant 24 bits of the interface's unique 48-bit MAC ID. The most-significant 24 bits are always "0090C2", and are therefore not printed. For example, if the label reads "C0298B", then this unit's complete 48-bit MAC ID is 00-90-C2-C0-29-8B, and an example of setting this unit's IP address to 192.168.16.110 would look like:

```
arp -s 192.168.16.110 00-90-C2-C0-29-8B
ping 192.168.16.110
arp –d 192.168.16.110
```

Forcing the unit to adopt the new IP address completes only half of the ARP configuration process. In addition to the IP address being changed, the unit also automatically configures its subnet mask to a temporary value of 255.255.255.255. This setting essentially allows only the computer that issued the ping command to communicate with the unit. From this computer, then, the user must also access the unit's web page via a web browser, or its console via a telnet session, in order to write the IP address to the filesystem. Until the new IP address is written to the filesystem, the IP address change is only temporary. If the unit loses power or is otherwise reset prior to submitting/setting the new IP address, the previous IP address and subnet mask settings will return.

Note that if the IP address is to be written to the filesystem by performing a "submit" via the unit's web page, that network elements such as HTTP proxy servers may relay the web page request for the configuring computer. The unit, seeing the HTTP request from a computer other than that which performed the initial "ping", will ignore such a request. Therefore, be sure to bypass or disable any proxy servers at least temporarily when using this configuration method.

For security reasons, once the ARP method of configuration has been successfully completed (i.e. the IP address has been written to the filesystem), the ARP method of configuration will be disabled, and all future attempts at using this method will be ignored by the unit. It is possible, however, to re-enable the ARP method via a console command (refer to section 13.3).

12.2 Console Method

The console method of configuration is achieved via a text-based console interface, accessible over the RS232 port and a telnet interface. The RS232 console is accessed by connecting the port to a computer's serial (COM) port, and then running a terminal emulation program, such as Windows® HyperTerminal. If the ARP method of initial configuration is not used, then the RS232 console must be accessed. More information about the console interface and its commands can be found in section 13.

13. Console Access

13.1 RS232

The console is accessible via an RS232 interface for direct connection to a computer's serial (COM) port. This is performed by connecting the unit's RS232 port to the computer's serial port via the #10425 DB9-to-RJ45 serial cable included with the interface kit. Unless the ARP ping configuration method is used, this will typically be the initial configuration channel, as the telnet and web browser interfaces can only be accessed once the network parameters have already been established and the device is communicating on the Ethernet network.

13.1.1 Requirements

All that is needed is a computer with a standard serial (COM) port, some sort of communications software (such as HyperTerminal, included with Microsoft Windows operating systems), and the included #10425 DB9-to-RJ45 serial cable. Any communications software and PC will work, provided they support ASCII communications at 38.4kbaud.

13.1.2 Connection

Connect the RJ45 end of the serial cable to the interface's RS232 port, and connect the DB9 end to the computer's serial port. Make sure that DIP switch DS1 #2 is in the "OFF" (down) position to force the RS232 port to act as the serial console. If the unit is currently using the RS232 port for control protocol communication, then it must be rebooted (drive powered down and then back up again or a "submit" performed from the web interface) with DS1 #2 in the OFF position to enable the serial console on the RS232 port.

13.1.3 Application Configuration

As previously mentioned, any PC communication software and serial port can be used. The software configuration example given here will be for Windows HyperTerminal communicating via COM1.

Figure 5 shows the "Connect To" tab of the properties window for COM1. Figure 6 shows the window that appears when "Configure" is selected in the "Connect To" tab. Figure 7 shows the "Settings" tab of the properties window. Most of these settings are their default values: usually the only change needed is the "Bits per second" setting shown in Figure 6.

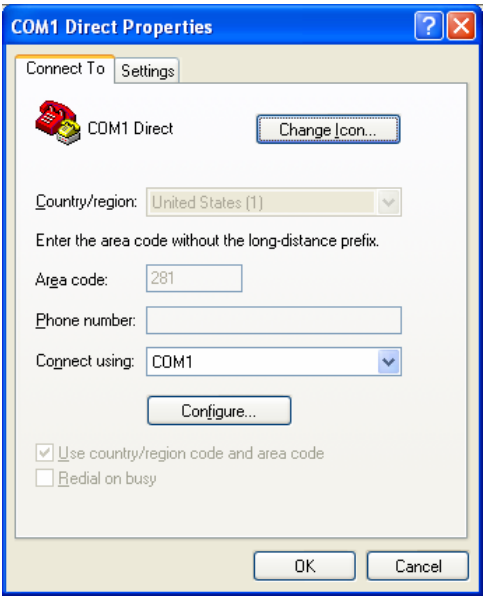


Figure 5: HyperTerminal Properties…Connect To

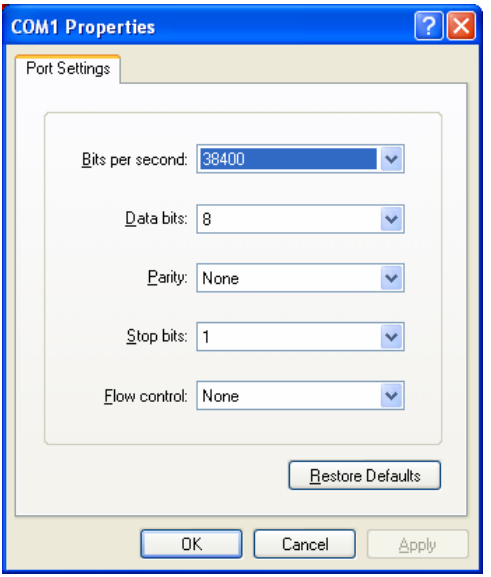


Figure 6: HyperTerminal Properties…Connect To…Configure

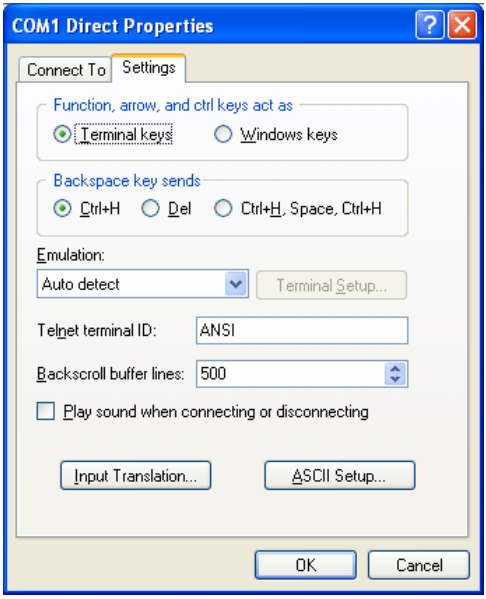


Figure 7: HyperTerminal Properties…Settings

13.2 Telnet

The console is also accessible via a Telnet interface for remote administration over Ethernet once the unit is communicating on the network. The Telnet console uses well-known port 23. Note that although only 1 telnet console session can be active at any given time, the telnet console and RS232 console operate independently and can be used simultaneously.

13.2.1 Requirements

All that is needed is a computer with telnet software that can access the interface over the Ethernet network. Telnet software is typically included as a standard component of Microsoft Windows and other PC operating systems.

13.2.2 Connection

No special connections are required, other than the PC running the Telnet application must be able to access the interface to be configured.

13.2.3 Application Configuration

Although any software vendor's Telnet client application can be used, the configuration example given here will use the Microsoft Windows Telnet application. To start the Telnet application, simply type "telnet" at either a DOS (command) prompt or in the "Start…Run" window. Once the telnet client screen opens, the target device can be accessed simply by typing "open" at the Telnet prompt with the interface's IP address as an argument. Refer to Figure 8.

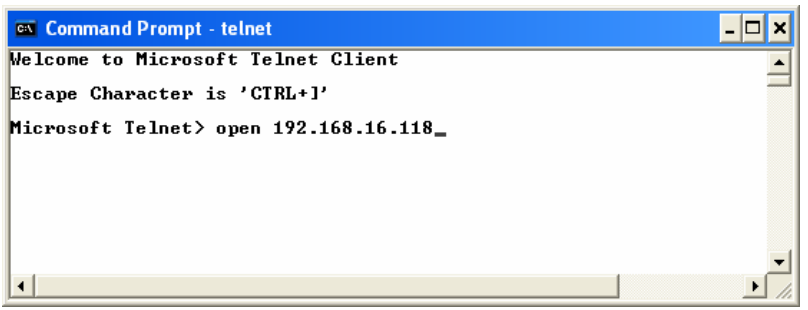


Figure 8: Telnet Menu

13.3 Command Overview

The console provides standard access and configuration methods for the various network parameters and configurations supported by the unit. This section will present an overview of the supported console commands.

It is important to note that unless otherwise indicated, each of these commands will become effective immediately after it has been successfully entered. This may have several repercussions; for example, if you change the IP address of the device via the Telnet console, then you will lose the telnet connection to the device (as it was a connection to the old IP address) and therefore must re-connect to the console if you wish to continue changing parameters. Also note that the console commands are not case-sensitive.

Help: This command shows the console version and an overview of all available commands. As indicated in the returned help information, typing "Help <command>" with a specific command will return help information specific to that command. Refer to Figure 9 for the help command output via Telnet. All further display screens shown in this section will be from Telnet, although they will look identical when accessed via the RS232 port.

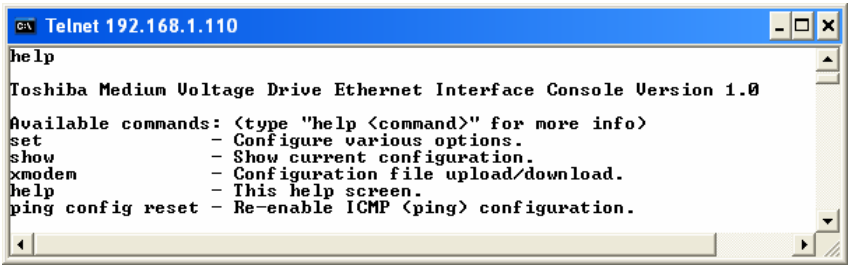


Figure 9: "Help" Command

Set: The "Set" command actually encompasses several subcommands, each of which allows setting a different configuration parameter. To set a parameter, two arguments are required: the parameter's name and the value to set it to. Figure 10 shows an example of changing the IP address of a device to 192.168.16.120. After this command is entered, the device will then reconfigure itself to allow network access via the IP address 192.168.16.120.

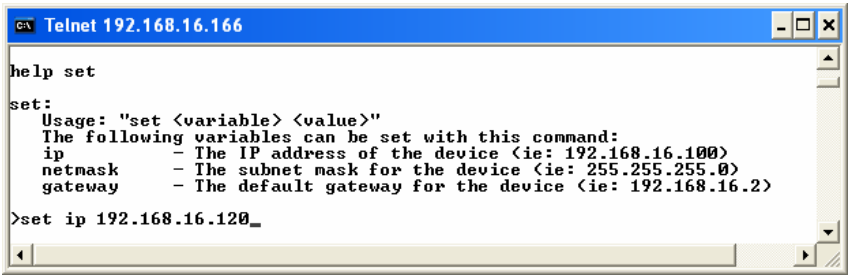


Figure 10: "Set" Command Overview and Implementation

Show: Figure 11 shows an example of this command, which displays current configuration information. Some of this information (IP Address, Netmask and Gateway) is configurable via the "set" command. The "Firmware Version" field indicates the unit's current application firmware version. The "Ping Configuration" field indicates whether or not the ability to remotely configure the unit via the ARP method is currently allowed (refer to section 12.1).

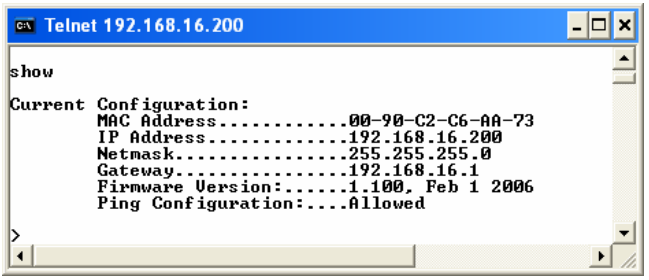


Figure 11: "Show" Command Overview

Xmodem: The "xmodem" command allows unit configuration files to be transferred between the interface and a PC. As Xmodem is a serial protocol, the xmodem command only applies to the serial console (RS232 port).

Whenever unit configuration is completed, it is highly recommended that a backup copy of the configuration file be downloaded from the unit to a PC. One reason for this is in case it becomes necessary to restore the file to the unit's file system later (such as if the unit's internal backup battery becomes exhausted and requires replacement). Another reason is that it may be desirable to load multiple units with the same configuration. Configuration files contain all point and port settings (but not network configuration information, such as IP address). A downloaded configuration file can be uploaded to any TOSVERT-300MVi Multiprotocol Ethernet and Modbus RTU Interface, allowing the user to clone multiple units with the same configuration.

Two different variations of the Xmodem protocol are supported (CRC and Checksum) for those serial communication packages that only support one or the other. However, some programs can automatically adapt to the user's selection, making the specific Xmodem protocol selection arbitrary. The first argument of the xmodem command indicates the mode, and must be set to either "/crc" for Xmodem CRC mode, or "/cs" for Xmodem checksum mode.

As mentioned above, configuration files can be both downloaded and uploaded. The second argument in the xmodem command indicates the action to take, and must be set to either "/d" to download the configuration file from the unit, or "/u" to upload a configuration file to the unit.

Figure 12 shows an example of initiating an Xmodem download in CRC mode. Once the message "The interface is ready to send its configuration file via Xmodem…Download the file now" appears, the user has 30 seconds to start the Xmodem download. This can be performed in HyperTerminal by clicking the "receive" button () on the tool bar. Figure 13 shows the dialog box that will appear after clicking the "receive" button. Specify the folder in which to place the received file, select Xmodem as the receiving protocol, and click "Receive". One last dialog box will prompt the user to name the received file, and then the transfer will begin. This will only take several seconds to complete, and at the conclusion the console will indicate the status of the transfer and return to the entry menu.

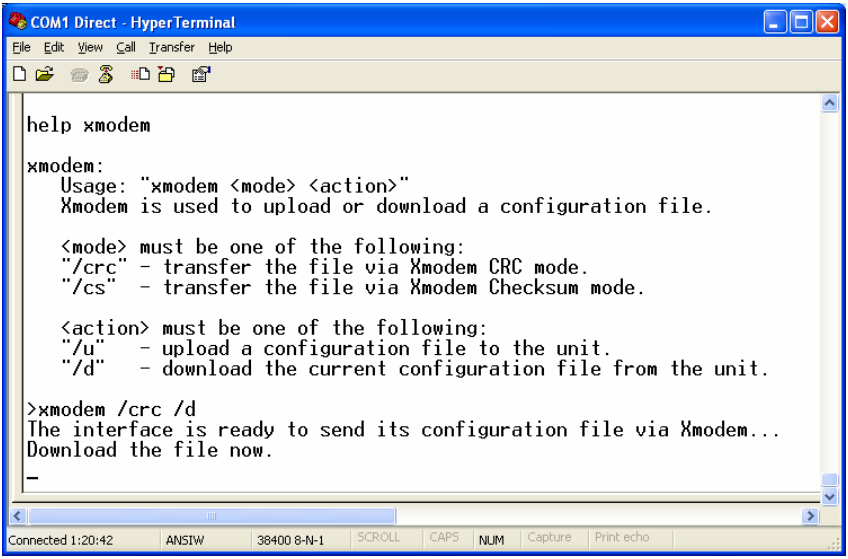


Figure 12: "Xmodem" Command Overview and Implementation

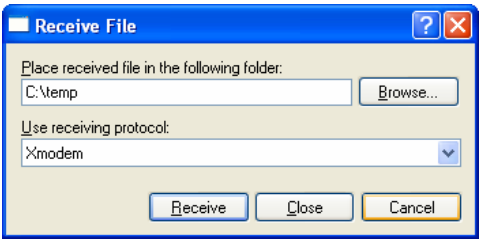


Figure 13: HyperTerminal receive file dialog box

When uploading a file, the procedure is similar to downloading. Enter "/u" instead of "/d" for the action parameter of the xmodem command. Once the xmodem upload command is entered, the user will have 30 seconds to click the "send" button ( ) on the tool bar in HyperTerminal and initiate the Xmodem upload transaction. Upon successful completion of the Xmodem upload, the unit will reset, and the uploaded file will become the unit's active configuration. The previous configuration cannot be recovered (unless a corresponding configuration file exists, of course). Note that uploading a file will also cause the unit to become "configured" (refer to section 14.2).

Ping config reset: This command re-enables the ability to configure the unit's IP address via the ARP method (refer to section 12.1). For security reasons, whenever the ARP method of configuration is successfully completed, the unit disables this method, and subsequent attempts at ARP configuration will be ignored. By entering the "ping config reset" console command, however, the unit will once again allow the ARP method of configuration. Refer to Figure 14. Recall that the current ARP method configuration status can always be obtained via the "show" command.

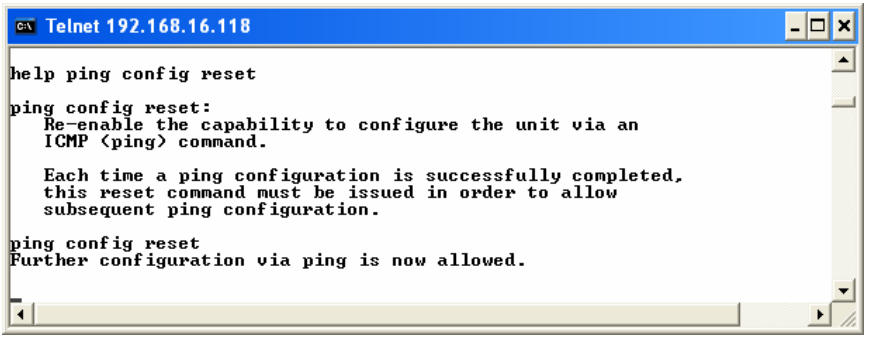


Figure 14: "Ping Config Reset" Overview and Implementation

14. Embedded Web Server

The interface contains an embedded web server (also known as an HTTP server), which allows users to access the unit's internal data in a graphical manner with web browsers such as Microsoft Internet Explorer or Netscape Navigator. In this way, the unit and connected devices can be monitored, configured and controlled from across the room or from across the globe.

The TOSVERT-300MVi Multiprotocol Ethernet and Modbus RTU Interface's web pages are best viewed with either Internet Explorer version 5.x and later, or Netscape Navigator version 6.x and later. The free Macromedia Flash player plug-in is also required, and can be obtained at http://www.macromedia.com/go/getflash. Always ensure that you have the latest version of the Flash player installed: if some aspect of the web pages appears to be displayed unusually, installing the latest Flash player update usually resolves the problem.

To access the unit's embedded web server, just enter its configured IP address into the address (URL) field of your web browser. Accessing the TOSVERT-300MVi Multiprotocol Ethernet and Modbus RTU Interface's web page is the same as surfing the Internet's world-wide web. Refer to Figure 15 for an example.

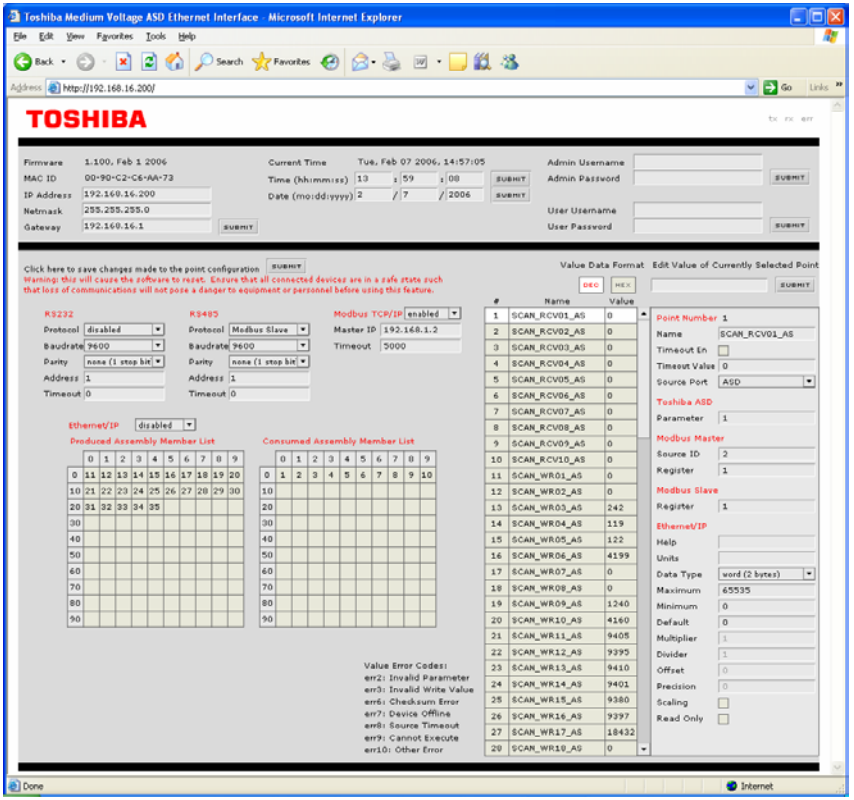


Figure 15: Embedded Web Server Interface

14.1 Authentication

For security, the interface requires valid user authentication when the web page is accessed or the point information is modified. The authentication request will appear as a browser popup box that will request entry of a user name and password. The unit contains two different security realms: an administrator realm and a user realm. Each of these realms has a different username and password, and applies to different activities. This division of authentication realms allows a device administrator to retain control of critical items (such as changing a unit's IP address or modifying point values and point definitions) while allowing a device user with appropriate authorization to monitor point values (i.e. observe the status of the attached network devices).

Refer to Figure 16 for a screen shot of the administrator realm authentication dialog box, and Table 1 for initial factory-set authentication values. Note that the username and password are case-sensitive, and that once authenticated,

the authentication will remain in effect from that point until all browser windows are closed.

Figure 16: Administrator Authentication

Table 1: Initial factory-set authentication values

Realm	Username	Password	Realm Applies To
USER	user	Blank (i.e. do not enter a password)	Monitoring capabilities
ADMIN	admin	Blank (i.e. do not enter a password)	All change actions

14.2 Unit Configuration

Before the interface is allowed to activate any of its communication protocols, it must be configured. This is to ensure that the user has initially confirmed that the current configuration is what they desire. When the interface requires configuration, the pop-up window shown in Figure 17 appears whenever the web server page loads into the web browser. The warning will no longer appear once a configuration data set has been sent to the interface.

- If the interface is not configured, all RS232, RS485 and Ethernet-based control protocols are disabled. The web (HTTP) interface, however, can still be used to read/write information from/to the drive.
- Even if the unit's factory-default point configuration is to be used, the "submit" button (refer to section 14.10) must still be clicked to confirm this configuration to the interface and activate the Ethernet and serial control protocols.
- If the RS232 serial console is selected (refer to section 13.1.2), the console will operate regardless of the interface's configuration status.

- Uploading a configuration file via Xmodem to the interface (refer to section 13.3) will also cause the unit to become “configured”.

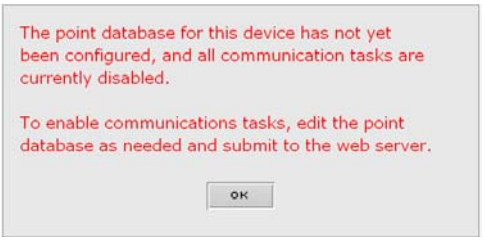


Figure 17: “Configuration Required” Notification

14.3 Communication Status Indicators

Figure 18 shows the communication status indicators. These will blink periodically to show the status of data communication between the web browser and the unit.

Figure 18: Communication Status Indicators

14.4 Unit Status

Figure 19 shows the non-modifiable unit status information. This includes the 48-bit Ethernet MAC address, and the application firmware version information.

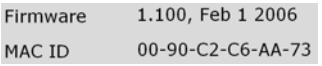


Figure 19: Unit Status

14.5 Set Date and Time

Figure 20 shows the submission boxes in which new date and time information can be entered. Note that the hours are entered in military time format (0-23 = 12AM – 11PM).

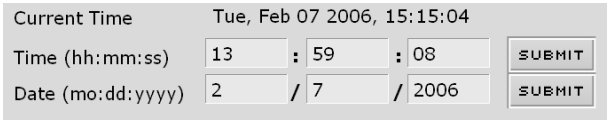


Figure 20: Set Date and Time

14.6 Network Configuration

Figure 21 shows the submission boxes in which network configuration information can be entered. Note that changing the subnet mask or default gateway will immediately result in a momentary loss of communications: just wait for a moment, or use the "refresh" button on your browser to re-establish communications. Changing the unit's IP address, however, will result in a complete loss of communications, as the unit's IP address will immediately be changed from that of the page you are viewing to the new value. To reconnect, therefore, requires transitioning to the new IP address via the browser's "Address" (URL) field.

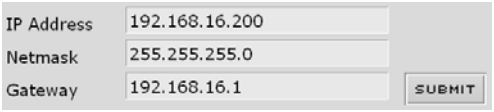


Figure 21: Network Configuration

14.7 Authentication Configuration

Figure 22 shows the submission boxes used to change the user-level and administrator-level usernames and passwords.

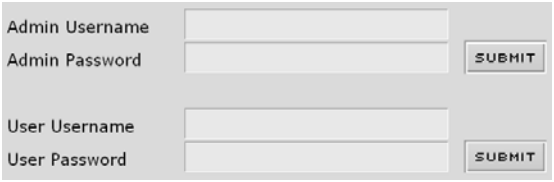


Figure 22: Authentication Configuration

To change, enter your desired username and password (max 11 characters each), then click "Submit". Contact Toshiba if you have forgotten your username or password for instructions on how to reset them.

14.8 Port Configuration

The TOSVERT-300MVi Multiprotocol Ethernet and Modbus RTU Interface has four ports (the Ethernet port actually acts like two independent “ports”, as the control protocols it supports can be used simultaneously). There is one RS485 connection, one RS232 connection, one Modbus TCP/IP connection, and one Ethernet/IP connection. These various connections are configured using the interface shown in Figure 23.

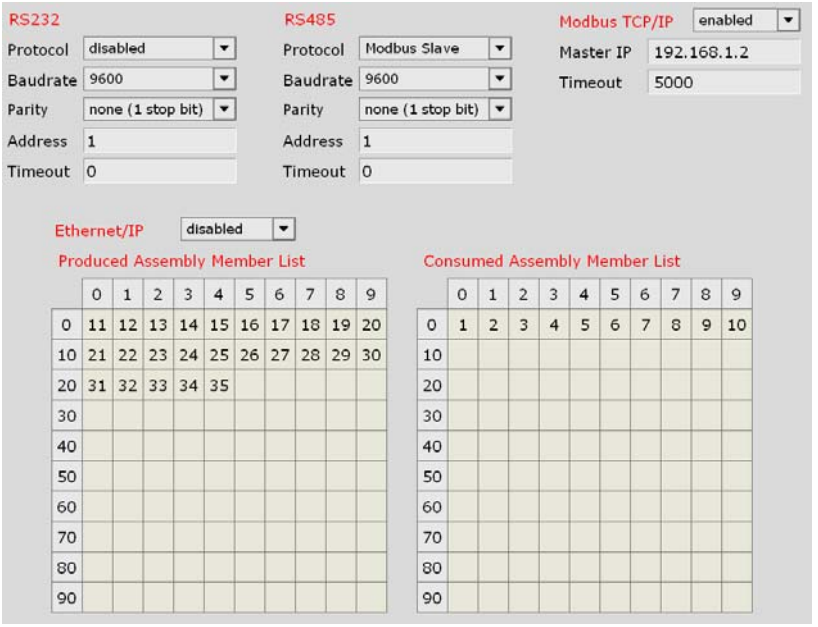


Figure 23: Port Configuration Interface

14.8.1 RS232 and RS485 Port Configuration

The RS232 and RS485 ports have the following configuration parameters:

- Protocol: Use the drop-down box to select the desired protocol to be attached to this port.
- Baudrate: Use the drop-down box to select the desired network baudrate (note that some protocols have a fixed baudrate and therefore ignore this selection).
- Parity: Use the drop-down box to select the desired network parity (note that some protocols have a fixed parity and therefore ignore this selection).
- Address: This assigns a network address to this port for the selected protocol.
- Timeout: Defines a timeout time (in seconds) that the port uses to identify a network timeout. 0 = timeout disabled.

14.8.2 Modbus TCP/IP Configuration

The Modbus TCP/IP protocol has the following configuration parameters:

- Enable/Disable: Enables or disables this protocol.
- Master IP: Defines the IP address that the Modbus TCP/IP driver will consider as its “master” for timeout purposes.
- Timeout: Defines a timeout time (in milliseconds). This network timeout only applies to network traffic originating from the configured “master IP” address. Valid timeout times are 500ms-30000ms (0.5s-30.0s).

Because the socket timeout determination is performed on a per-socket basis, note that a certain degree of caution must be exercised when using the network timeout feature to avoid “nuisance” timeouts from occurring. Specifically, do not perform inadvisable behavior such as sending a request from the master device to the interface, and then closing the socket prior to successfully receiving the unit’s response. The reason for this is because the interface will then experience an error when attempting to respond via the now-closed socket, which will immediately trigger the timeout action. Always be sure to manage socket life cycles “gracefully”, and do not abandon outstanding requests.

Modbus TCP/IP sockets initiated from devices other than the “master” device use a fixed 30s timeout time, and do not perform timeout processing. This allows devices other than the designated “master” to access the unit for monitoring or other non-critical access purposes.

14.8.3 Ethernet/IP Port Configuration

The Ethernet/IP port has the following configuration parameters:

- Enable/Disable: Enables or disables this protocol.
- Produced/Consumed Assembly Member Lists: These arrays allow the creation of custom-built assembly instances. Each box in the array is capable of containing a point number. Because the "value" attributes of each point are 16-bit data elements, each box represents two bytes of consumed or produced data.

  Up to 100 points can be assigned to each member list (for a total of 200 bytes of produced and/or consumed data). The array locations are numbered 0-99, and traverse from left to right across each row, and then increment to the left-most position on the next row. Clicking on a box in an array toggles the point that will be referenced when class 1 connected data is produced or consumed at that corresponding location. A blank array entry indicates that no point is referenced at that location, which will cause corresponding consumed data to be ignored and produced data to be a default value of 0.

  As an example, looking at the member list definitions shown in Figure 23, we can see that the *Produced Assembly Member List* contains 25 defined points, and the *Consumed Assembly Member List* contains 10 defined points. Therefore, up to 20 "meaningful" bytes of data can be consumed and up to 50 "meaningful" bytes of data can be produced via class 1 connected messages (the qualifier "meaningful" is used here because a client may configure a class 1 connection that indicates larger produced and/or consumed data sizes, but all unreferenced consumed data (data after byte #20) will be ignored, and all unreferenced produced data (data after byte #50) will be dummy "0" values). The first word (two bytes) of consumed data will be written to the "value" attribute of point #1, the next two bytes to point #2 and so on. If points #1 and #2 etc. have a "Source Port" selection defined (such as the ASD), then this command data will subsequently also propagate to that port and down to the point's configured remote device.

  This example works similarly when describing the behavior of the produced member list in Figure 23. In this case, the first 2 bytes of the produced data will be the value of point #11, the next two bytes will be the value of point #12 and so on.

14.9 Point Configuration

The TOSVERT-300MVi Multiprotocol Ethernet and Modbus RTU Interface supports 100 total points. The configuration of these points determines what data is available from attached network devices. Points are configured using the interface shown in Figure 24.

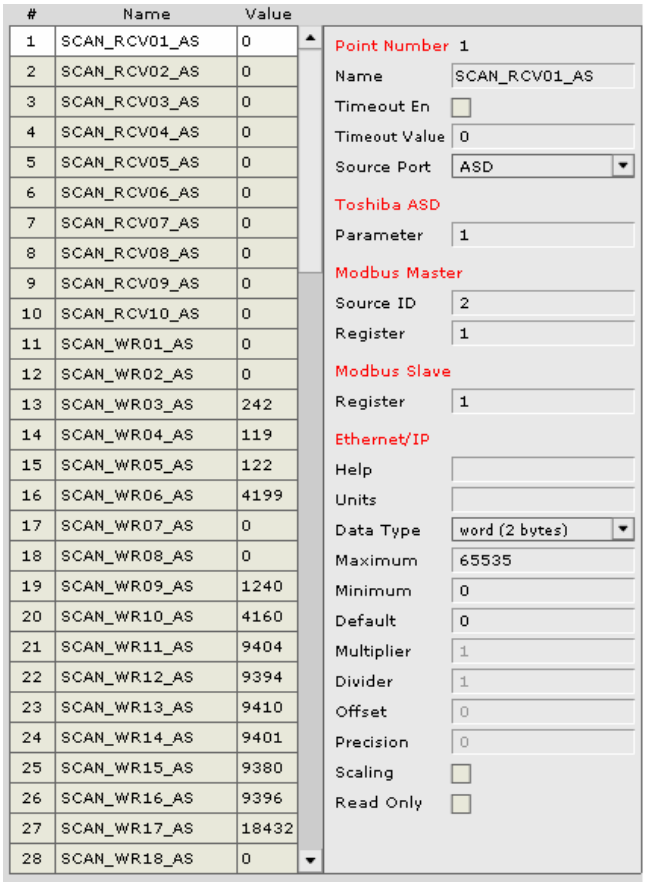


Figure 24: Point Configuration Interface

The list on the left displays the point number, name and current value for each available point. Clicking on one of these locations will load that point's current configuration into the interface on the right, where the configuration may be edited.

Each point contains the following configuration attributes:

- Name: This is a user description of the point, up to 16 characters.

- Timeout En: Checking this box will allow the point to participate in timeout processing when a port network timeout event is detected.
- Timeout Value: This determines the value this point will default to upon the occurrence of a network timeout. If a "Source Port" has been designated (see below), then this value will also propagate to the configured remote device connected to the designated port.
- Source Port: This determines the interface port that this point will obtain its value from and write values to.
- Toshiba ASD:
    - Parameter: The Toshiba ASD parameter (in decimal, 1 - 35) that this point refers to.
- Modbus Master:
    - Source ID: The ID (station address) of the Modbus slave that this point refers to.
    - Register: The holding register or input register within that slave that this point refers to. The default register type is "holding register", but an "input register" will be accessed if the register value entered here is 30001..39999.
- Modbus Slave:
    - Register: The holding register number assigned to this point.
- Ethernet/IP: Note that these entry fields are only necessary for support of the custom Electronic Data Sheet (EDS) download function, which will be supported on a future firmware release. They will then allow explicit messaging access to points as CIP parameter objects.
    - Help: User defined help text, up to 24 chars.
    - Units: User defined engineering units text, up to 5 chars.
    - Data Type: The data type of this point.
    - Maximum: The max value of this point.
    - Minimum: The min value of this point.
    - Default: The default value of this point.
    - Multiplier: The multiplier of this point.
    - Divider: The divider of this point.
    - Offset: The offset of this point.
    - Precision: The precision, in decimal places, of this point.
    - Scaling: Checking this box tells this point to use (value x multiplier)/divider + offset to determine its actual value.
    - Read only: Defines this point as read only when checked.

14.10 Upload Port and Point Configuration

Once all desired changes have been made to the port and point configurations, this data must be uploaded to the interface. This is performed by clicking the "SUBMIT" button shown in Figure 25.

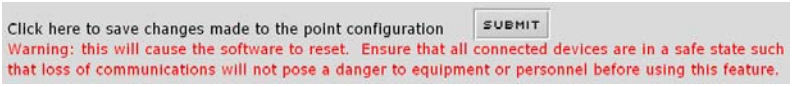


Figure 25: Port and Point Configuration Upload

Submitting the port and point configuration may require up to 1 minute to complete, during which time a "please wait" graphic will be displayed. Once the upload completes, the interface will return to its normal screen. However, clicking your browser's refresh button may be required to reestablish communications with the interface.

This process will also result in the loss of communications with all devices connected to the interface. It is important to ensure that all connected devices are in a safe state such that loss of communications will not pose a danger to equipment or personnel before using this feature.

14.11 Radix Selection

Figure 26 shows the radix selection buttons. These selection buttons allow changing the point value data display and entry radix between decimal and hexadecimal formats.

Figure 26: Radix Selection

14.12 Editing Point Values

The value of the currently selected point can be modified using the interface shown in Figure 27. The radix of the value entered here is determined by the radix selection described in section 14.11. Editing the point value in this interface and selecting "SUBMIT" immediately updates the point's value in the unit, which will result in a write to the point's configured "Source Port" if one is assigned.

Figure 27: Edit Point Value Interface

14.13 Error Code Reference

Figure 28 shows the error code reference table. These error codes may appear in certain situations in the point "Value" fields.

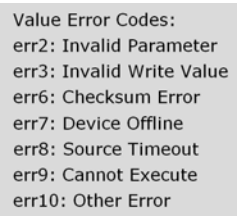


Figure 28: Error Code Reference

15. Protocol-Specific Information

This section will discuss topics that are specific to each of the available network selections.

15.1 Modbus

The interface supports Modbus slave functionality via both Modbus RTU and Modbus TCP/IP, and Modbus master functionality via Modbus RTU. The slave implementations share common access methods, which is to say they support the same functions and reference the internal points via a common "Modbus Slave" holding register assignment. Other notes of interest are:

- Points are addressed by their assigned holding register (4X reference) via Modbus slave protocols.
- Points can access both holding register (4X references) and input registers (3X references) via Modbus master protocols.
- Supported Modbus slave functions are indicated in Table 2.

Table 2: Supported Modbus Slave Functions

Function Code	Function	Modbus TCP/IP Class
1	Read coils	1
3	Read multiple registers	0
5	Write coil	1
6	Write single register	1
15	Force multiple coils	2
16	Write multiple registers	0

- Register number entry radix is decimal (e.g. 10 = 10_{10})
- Configuration tip: Improved network utilization may be obtained by appropriately grouping points into blocks having contiguous holding register assignments. In this way, the "read multiple registers" and "write multiple registers" functions can be used to perform transfers of larger blocks of registers using fewer Modbus transactions compared to a situation where the read/write registers were arranged in an alternating or scattered fashion.

- Because the transaction is handled locally within the interface, write data checking is not available. For example, if a write is performed to a register with a data value that is out-of-range of the corresponding "source port" object, no Modbus exception will be immediately returned. However, the point will always reflect the "source port" status and object value. In other words, if such an out-of-range write attempt is performed, the unsuccessful "source port" network write can be observed by reading the current (unchanged) value of the point during a subsequent Modbus transaction.

15.1.1 Coil Mappings

The Modbus slave implementations provide read/write support for coils (0X references). Accessing coils does not reference any new physical data: coils are simply indexes into various bits of Modbus holding registers. What this means is that when a coil is accessed, that coil is resolved by the interface into a specific holding register, and a specific bit within that holding register. The pattern of coil-to-register/bit relationships can be described as follows:

Coils 1...16 map to holding register #1, bit0...bit15 (bit0=LSB, bit15=MSB)
Coils 17...32 map to holding register #2, bit0...bit15, and so on.

Arithmetically, the coil-to-register/bit relationship can be described as follows: For any given coil, the holding register in which that coil resides can be determined by:

$$holding\ register = \left\lfloor \frac{coil + 15}{16} \right\rfloor \qquad \textit{...Equation 1}$$

Where the bracket symbols "⌊ ⌋" indicate the "floor" function, which means that any fractional result (or "remainder") is to be discarded, with only the integer value being retained.

Also, for any given coil, the targeted bit in the holding register in which that coil resides can be determined by:

$$bit = (coil - 1)\ \%\ 16 \qquad \textit{...Equation 2}$$

Where "coil" ∈[1…65535], "bit" ∈[0…15], and "%" is the modulus operator, which means that any fractional result (or "remainder") is to be retained, with the integer value being discarded (i.e. it is the opposite of the "floor" function).

From these equations, it can be seen that the largest holding register number that can be accessed via this coil-to-register mapping method is 4096 (which contains coil 65535).

For clarity, let's use Equation 1 and Equation 2 in a calculation example. Say, for instance, that we are going to read coil #34. Using Equation 1, we can determine that coil #34 resides in holding register #3, as ⌊3.0625⌋ = ⌊3 r1⌋ = 3.

Then, using Equation 2, we can determine that the bit within holding register #3 that coil #34 targets is (34-1)%16 = 1, as 33%16 = mod(3 r1) = 1. Therefore, reading coil #34 will return the value of holding register #3, bit #1.

Note that this coil-to-register/bit relationship holds true regardless of whether or not holding register #3 is assigned to a point. If holding register #3 is not assigned to a point, then a Modbus exception will be returned. Either way, coil #34 will always access holding register #3, bit #1.

15.1.2 Modbus RTU Slave

- Broadcast (for functions 5, 6, 15 and 16) is supported.

- Network characteristics selections
  - Baud rate: 2400 / 4800 / 9600 / 19200 / 38400 bps
  - Parity: odd / even / none (1 stop bit) / none (2 stop bits)

15.1.3 Modbus RTU Master

- Supported Modbus master functions are indicated in Table 3. These functions are automatically invoked by the interface in response to point read or write requests.

Table 3: Supported Modbus Master Functions

Function Code	Function
3	Read multiple registers
4	Read input registers
16	Write multiple registers

- The slave response timeout (in seconds) is assigned via the designated port's "Timeout" selection. If "0" is chosen (an invalid timeout time), the interface will use a 2s timeout by default.

- Network characteristics selections
  - Baud rate: 2400 / 4800 / 9600 / 19200 / 38400 bps
  - Parity: odd / even / none (1 stop bit) / none (2 stop bits)

- The default register types that the Modbus master driver attempts to access (read and write) are "holding" (4X) registers. However, "input" (3X) registers will be accessed whenever a point's assigned "register" index is in the range of 30001..39999. Refer to Figure 29 for a graphical explanation of which type of register is accessed (i.e. which function code is used) based on the Modbus master "register" index assigned to a point. Simply put, if the assigned "register" index is in the range of 30001..39999, a

corresponding input register in the range of 1..9999 will be accessed. Otherwise, a holding register of the same index as the assigned "register" index will be accessed.

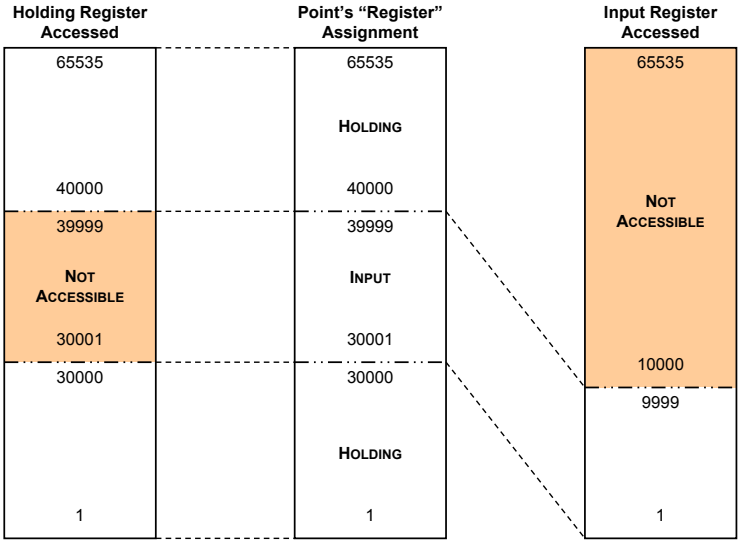


Figure 29: "Register" Assignment and Resulting Register Type Accessed

- Input (3X) registers are read-only. Attempts to write to a point associated with an input register will result in an exception.

15.1.4 Modbus TCP/IP Slave

The interface supports Schneider Electric's Modbus TCP/IP protocol, release 1.0. The unit is conformance class 0 and partial class 1 and class 2 compliant, and allows up to 4 simultaneous Modbus TCP/IP client connections (sockets).

- The "unit identifier" (UI) field of the request packets is ignored.
- Standard socket timeouts are set to 30s, which means that if a particular open socket experiences no activity for more than 30s, then the interface assumes that the client or network has experienced some sort of unexpected problem, and the interface will close that socket.
- A "master" IP address and timeout time can be assigned to the unit. Each point defined in the point database has the capability to be assigned an optional failsafe timeout value. When an unexpected socket failure from

the “master” client occurs, all points with timeout processing enabled will be written with their failsafe values. This provides an additional level of process security in the event of a network or master device disturbance.

15.2 Ethernet/IP

The interface supports the Ethernet/IP protocol (release 1.0), administered by the Open DeviceNet Vendor Association (ODVA).

- This product has been self-tested by ICC, Inc. and found to comply with ODVA Ethernet/IP Conformance Test Software Version A3.7.3.
- Supports unconnected messages (UCMM), and up to 16 simultaneous class 1 or class 3 connections.
- Supports CIP point-to-point transport types in the originator-to-target direction, and both point-to-point and multicast transport types in the target-to-originator direction.
- Supports only CIP “cyclic” transport triggers.
- Connection sizes are adjustable between 0 and 200 bytes (100 points @ 2 bytes per point = 200 bytes). Because point “value” attributes are 16-bit elements, however, connection sizes cannot be odd (i.e. 1, 3, 5 etc.)
- When data is consumed via a class 1 connection, if the actual consumed data size is less than or equal to the connection’s configured consumed connection size, then all received data will be consumed. If the actual consumed data size is larger than the connection’s configured consumed connection size, however, the consumed data will be ignored.
- If a parameter entry in the consumed assembly member list is empty (i.e. no parameter has been assigned to that location), then any consumed data that corresponds to that location will be ignored. Conversely, if a parameter entry in the produced assembly member list is empty, then any produced data that corresponds to that location will be a default value of 0. Refer to section 14.8.3 for further information on the assembly object member lists.
- The 32-bit run/idle header is required in the originator-to-target direction. When using an originator that does not support the run/idle header, then just send dummy data as the 1st two words, as the interface ignores the contents of the run/idle header. The interface does not send a run/idle header in the target-to-originator direction.
- Point-to-point class 1 connected messages will be produced targeting the IP address of the device that instantiated the connection, port 0x08AE (port 2222).
- If a class 1 connection’s consuming half (O=>T) times out, then the producing half (T=>O) will also time-out and will stop producing.

- Once instantiated, class 1 connections act independently of the encapsulation protocol sessions over which they were established. The client may therefore terminate the encapsulated session at any time with no ill affects on the class 1 transport mechanism.

15.3 Toshiba ASD

- The interface acts as a TOSVERT-300MVi master simply by virtue of being installed into a drive.

- No configuration other than that indicated in section 4 is necessary, as the interface automatically adapts to the ASD's configured characteristics.

- 35 ASD items are accessible. These items are referenced by ASD parameters SCAN_WR01_AS..SCAN_WR25_AS and SCAN_RCV01_AS..SCAN_RCV10_AS. For the purposes of point database numerical configuration, these ASD parameters have been assigned the "parameter numbers" indicated in Table 4. For example, if ASD parameter SCAN_WR05_AS is assigned "VDC_F_DSP", then accessing a point in the interface's point database whose "Source Port" is set to "ASD" and whose "Toshiba ASD Parameter" value is 15 will return the drive's DC voltage (in %). For further information on the SCAN_xxxx_AS parameters and their settings, please refer to the relevant ASD configuration manual and section 4 in this manual.

Table 4: Toshiba ASD Parameter Assignments

Parameter Number	Item Reference	Input to ASD / Output from ASD	Read Only / Read/Write
1	SCAN_RCV01_AS	Input	Read/Write
2	SCAN_RCV02_AS	Input	Read/Write
3	SCAN_RCV03_AS	Input	Read/Write
4	SCAN_RCV04_AS	Input	Read/Write
5	SCAN_RCV05_AS	Input	Read/Write
6	SCAN_RCV06_AS	Input	Read/Write
7	SCAN_RCV07_AS	Input	Read/Write
8	SCAN_RCV08_AS	Input	Read/Write
9	SCAN_RCV09_AS	Input	Read/Write
10	SCAN_RCV10_AS	Input	Read/Write
11	SCAN_WR01_AS	Output	Read Only
12	SCAN_WR02_AS	Output	Read Only
13	SCAN_WR03_AS	Output	Read Only
14	SCAN_WR04_AS	Output	Read Only
15	SCAN_WR05_AS	Output	Read Only
16	SCAN_WR06_AS	Output	Read Only
17	SCAN_WR07_AS	Output	Read Only
18	SCAN_WR08_AS	Output	Read Only
19	SCAN_WR09_AS	Output	Read Only
20	SCAN_WR10_AS	Output	Read Only
21	SCAN_WR11_AS	Output	Read Only
22	SCAN_WR12_AS	Output	Read Only
23	SCAN_WR13_AS	Output	Read Only
24	SCAN_WR14_AS	Output	Read Only
25	SCAN_WR15_AS	Output	Read Only
26	SCAN_WR16_AS	Output	Read Only
27	SCAN_WR17_AS	Output	Read Only
28	SCAN_WR18_AS	Output	Read Only
29	SCAN_WR19_AS	Output	Read Only
30	SCAN_WR20_AS	Output	Read Only
31	SCAN_WR21_AS	Output	Read Only
32	SCAN_WR22_AS	Output	Read Only
33	SCAN_WR23_AS	Output	Read Only
34	SCAN_WR24_AS	Output	Read Only
35	SCAN_WR25_AS	Output	Read Only

- Point parameter number entry radix is decimal (e.g. 10 = 10_{10}).

- Note that although every one of the parameters listed in Table 4 is always accessible via the network, writing to parameters 1 - 10 may not have an actual effect on the drive's operation (depending on the values of SCAN_R_SIZE and SCAN_RCV01_AS ... SCAN_RCV10_AS), and reading from parameters 11 – 35 may not return actual drive status data (depending on the values of SCAN_W_SIZE and SCAN_WR01_AS ... SCAN_WR25_AS). Refer to section 4 for more information.

16. Firmware Updates

The interface's embedded firmware resides in flash memory that can be updated in the field. Firmware updates may be released for a variety of reasons, such as custom firmware implementations, firmware improvements and added functionality as a result of user requests.

Toshiba is continually striving to enhance the functionality and flexibility of our products, and we therefore periodically release new embedded firmware to achieve these goals and meet customer requests. Flash firmware files and all related documentation (such as updated user manuals) can be downloaded as complete board support packages (referred to as BSPs) from http://www.iccdesigns.com. It is suggested that users check this Internet site prior to installation, and then periodically afterwards to determine if new support packages have been released and are available to upgrade their units.

16.1 Requirements

Besides the new firmware file, firmware updates require a PC with a Windows operating system (Windows 95 or newer) and a serial port, the RFU PC application (refer to section 16.3), and the RS232 cable included with the interface kit (ICC part number 10425) to connect the RS232 port of the unit to the PC.

Please be sure to read the firmware release notes and updated user's manual (included with the BSP) for any important notices, behavior precautions or configuration requirements prior to updating your firmware. For example, upgrading to a new firmware version may affect user-defined configuration files: prior to starting an update procedure always back up your configuration file to a PC for later recovery if necessary.

16.2 Connection

IMPORTANT: Note that the interface will not be operating its system control and communication tasks while its internal firmware is being updated. Therefore, be sure to shut down the system to a known safe state prior to initiating the firmware update procedure.

Connect the #10425 serial port cable between the RS232 port of the interface and the computer's serial port. Move DIP switch #1 to the "ON" (up) position: this will place the interface into the "firmware download" mode. Whenever DIP switch #1 is "ON", the interface can only download firmware to its flash memory: all other application functions (such as communications, console access etc.) will be disabled.

16.3 Using the RFU Utility

Support for downloading new application firmware to the interface is provided by the free Rabbit Field Utility (RFU), which is a 32-bit application that runs on Microsoft Windows platforms. The RFU utility can be downloaded from ICC's home page at http://www.iccdesigns.com. When downloading a new interface application BSP, always confirm that you also have the latest version of RFU, as new .BIN firmware files contained in BSPs may require functionality found only in the most recent RFU versions for successful downloading.

The remainder of this section will detail the RFU utility configuration and firmware download procedures.

16.3.1 Required Files

When first downloaded, the RFU utility files are compressed into one self-extracting .EXE distribution file. Create a folder (such as c:\RFU), place the distribution file in this folder, and then execute it. This will extract the compressed files into that same folder. The distribution file is then unneeded and can be deleted if desired. To run the RFU utility, double-click on the RFU.EXE file icon.

16.3.2 First-Time Configuration

The first time the RFU utility is run on a computer, several configuration items need to be confirmed. These configuration items are retained in the computer's registry from that point on, so reconfiguration is not required unless certain parameters (such as which serial port to use on the computer) are changed.

The two configuration items that need to be confirmed are the communications and bootstrap loaders path. First, select the "Setup…Communications" menu item (refer to Figure 30).

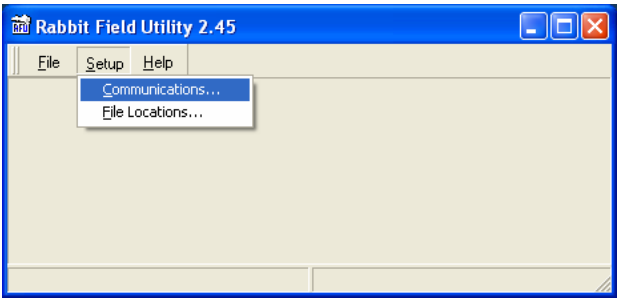


Figure 30: RFU Main Screen

The Communications Options window shown in Figure 31 then appears. Confirm that the settings are as shown, with the possible exception of the "Comm Port" settings, which depends on the COM port you are using. Click "OK" when complete.

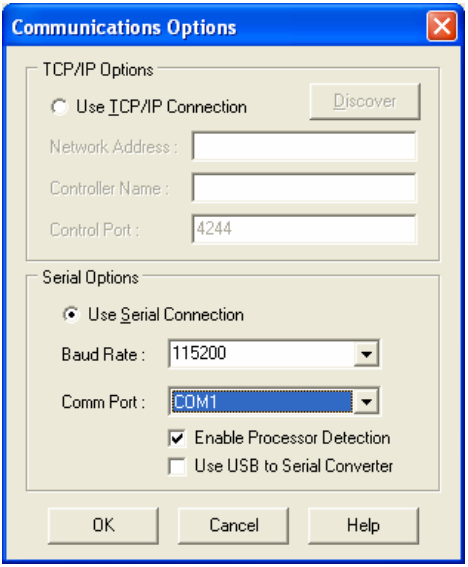


Figure 31: Communications Options Window

Next, select the "Setup…File Locations" menu item from the main screen. The "Choose File Locations" window shown in Figure 32 then appears. Confirm that the correct paths to the referenced files are entered. Enter the correct paths if necessary.

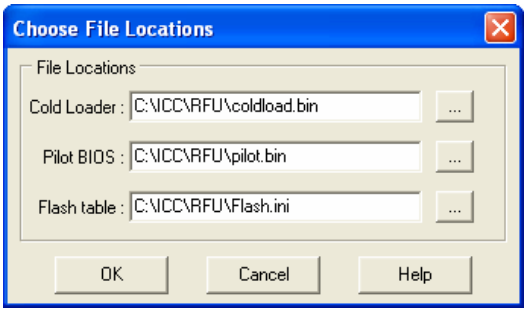


Figure 32: Choose File Locations Window

16.3.3 Transmitting Firmware Files

When a board support package (BSP) has been downloaded and unzipped, the flash firmware file will be the one with ".BIN" as its file name extension.

Once the RFU utility has been configured, the flash firmware files can be downloaded to the interface by two different methods. The simplest way is to drag the application firmware .BIN file's icon and drop it onto the RFU utility's main screen. This will automatically initiate the download process.

Alternatively, select the "File…Load Flash Image" menu item (refer to Figure 33).

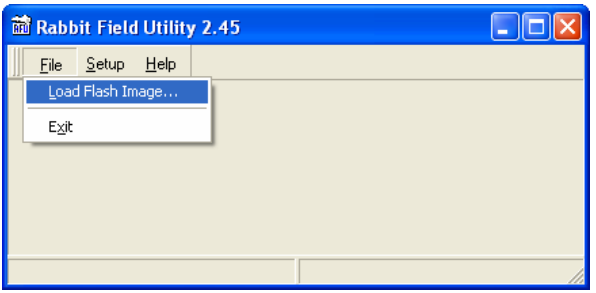


Figure 33: Load Flash Image Menu Selection

The flash image (.BIN file) selection window will then appear (refer to Figure 34). Browse to the location of the flash image file and select it. Clicking "OK" will then initiate the download process.

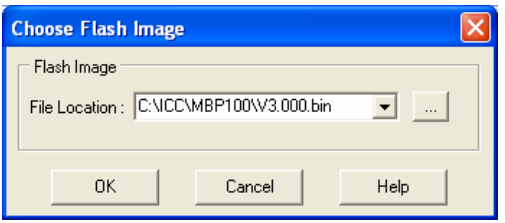


Figure 34: Flash File Selection Window

While downloading, the RFU utility will indicate the download status. Once complete, summary information will be displayed in the bottom status bar (see Figure 35).

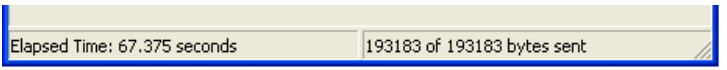


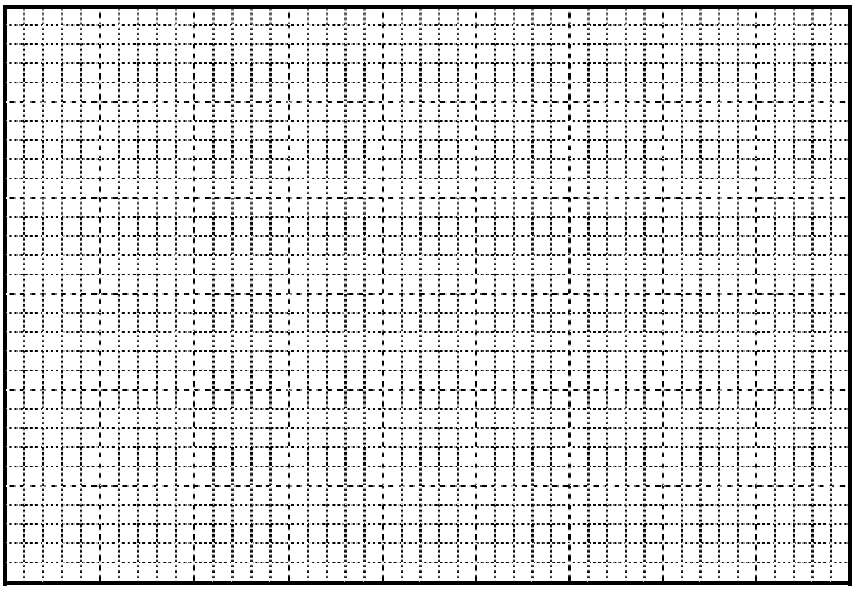
Figure 35: Summary Information

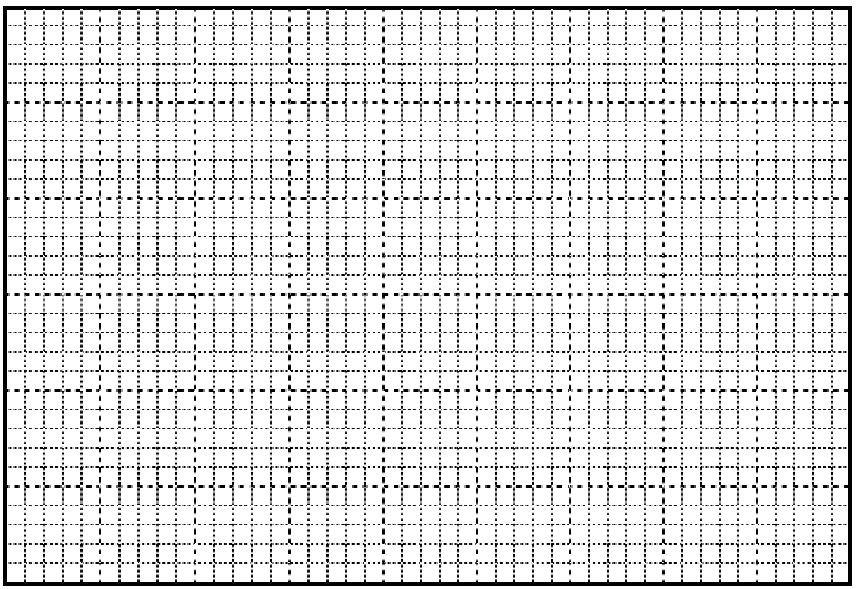
16.4 Wrap-Up

Once downloading is complete, close the RFU utility, move DIP switch #1 back to the “OFF” (down) position to exit “firmware download” mode, and cycle power momentarily to the drive to reset the interface.

When the unit powers up again, it will be running the new application firmware. If the new firmware version release notes indicated that the configuration file might need to be reloaded, then do so at this point.

17. Notes





TOSHIBA

13131 West Little York Road
Houston, TX USA 77041
Tel: [800] 231-1412 Fax: [713] 466-8773
World Wide Web http://www.tic.toshiba.com

Printed in U.S.A