



# Terafence MBsecure

## Installation and Configuration Manual

PN: PartNumber-TBD-001

Terafence Ltd.

Tel +972 4 850 0101 > Fax +972 4 855 1491 > [www.terafence.com](http://www.terafence.com)

Nahum Het 5, Haifa, Israel 3508504

## Contents

<b>Introduction .....</b>	<b>1</b>
Background.....	1
Definitions and Acronyms .....	2
About this Manual.....	3
<b>Safety First.....</b>	<b>3</b>
Warnings and Precautions.....	3
Labels and Symbols .....	3
<b>TF_MBsecure solution diagram: .....</b>	<b>4</b>
Solution Highlights:.....	4
<b>MBsecure Panels.....</b>	<b>5</b>
Front Panel .....	5
Rear Panel.....	5
<b>MBsecure Installation .....</b>	<b>6</b>
What's in the box .....	6
Installing MBsecure .....	6
Configuring MBsecure .....	8
<b>Technical Specifications .....</b>	<b>10</b>
Hardware.....	10
Environmental Conditions.....	10
<b>Limited Warranty.....</b>	<b>10</b>
Warranty Card .....	10
<b>Appendix A: MBSecure Configuration Sheet .....</b>	<b>11</b>

## Introduction

### Background

**MODBUS** is a serial communications protocol originally published in 1979 by Schneider Electric (formerly known as Modicon) for use with its programmable logic controllers (PLC). MODBUS has become a *de facto* standard communication protocol and is now a commonly available means of connecting industrial electronic devices. The main reasons for the use of MODBUS in the industrial environment are:

- developed with industrial applications in mind
- openly published and royalty-free
- easy to deploy and maintain
- moves raw bits or words without placing many restrictions on vendors

MODBUS enables communication among many devices connected to the same network, for example, a system that measures temperature and humidity and communicates the results to a computer. MODBUS is often used to connect a supervisory computer with a remote terminal unit (RTU) in supervisory control and data acquisition (SCADA) systems. Many of the data types are named from industry usage of Ladder logic and its use in driving relays: a single-bit physical output is called a *coil*, and a single-bit physical input is called a *discrete input* or a *contact*.

Supervisory Controls and Data Acquisition (SCADA) protocols are communications protocols designed for the exchange of control messages on industrial networks. Over the past three decades, several hundred of these protocols have been developed for serial, LAN, and WAN-based communications in a wide variety of industries including petrochemical, automotive, transportation, and electrical generation/distribution.

SCADA MODBUS is the most widely used SCADA Protocol.

There are many variants of MODBUS protocols:

MODBUS RTU	Used in serial communication and makes use of a compact, binary representation of the data for protocol communication. The RTU format follows the commands/data with a cyclic redundancy check checksum as an error check mechanism to ensure the reliability of data. MODBUS RTU is the most common implementation available for MODBUS. A MODBUS RTU message must be transmitted continuously without inter-character hesitations. MODBUS messages are framed (separated) by idle (silent) periods.
MODBUS ASCII	Used in serial communication and makes use of ASCII characters for protocol communication. The ASCII format uses a longitudinal redundancy check checksum. MODBUS ASCII messages are framed by leading colon (":") and trailing newline (CR/LF).
<b>MODBUS TCP/IP or MODBUS TCP</b>	Used for communications over TCP/IP networks, connecting over port 502. It does not require a checksum calculation, as lower layers already provide checksum protection.

MODBUS over TCP/IP or MODBUS over TCP or MODBUS RTU/IP	Differs from MODBUS TCP in that a checksum is included in the payload as with MODBUS RTU.
MODBUS over UDP	Some have experimented with using MODBUS over UDP on IP networks, which removes the overheads required for TCP.
MODBUS Plus (MODBUS+, MB+ or MBP)	Proprietary to Schneider Electric and unlike the other variants, it supports peer-to-peer communications between multiple masters. It requires a dedicated co-processor to handle fast HDLC-like token rotation. It uses twisted pair at 1Mbit/s and includes transformer isolation at each node, which makes it transition/edge-triggered instead of voltage/level-triggered. Special hardware is required to connect MODBUS Plus to a computer, typically a card made for the ISA, PCI or PCMCIA bus.
Pemex MODBUS	Extension of standard MODBUS with support for historical and flow data. It was designed for the Pemex oil and gas company for use in process control and never gained widespread adoption.
Enron MODBUS	Extension of standard MODBUS developed by Enron Corporation with support for 32-bit integer and floating-point variables and historical and flow data. Data types are mapped using standard addresses. The historical data serves to meet an American Petroleum Institute (API) industry standard for how data should be stored.

Terafence MBsecure (currently supporting only **RTU over MODBUS TCP/IP or MODBUS TCP**) allows network architects to interconnect network segments of unequal security classification without exposing the secure network to hacking attacks. The secure network (or segment) is physically isolated (at OSI Layer 1) from the less secure segment.

Data is transmitted downstream untouched.

Terafence MBsecure unit acquires MODBUS data from sensors and PLCs over TCP/IP and responds to the HMI with the acquired data. At no time physical access to the PLC is available to any device on the HMI network side.

## Definitions and Acronyms



Acronym/Term	Definition
ASCII	American Standard Code for Information Interchange
HMI	Human-Machine Interface
IP	Internet Protocol
Module A	MBsecure Module connected to Programmable Logic Controller.
Module B	MBsecure Module connected to HMI
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
TCP	Transmission Control Protocol

Acronym/Term	Definition
SCADA	Supervisory Controls and Data Acquisition
UDP	User Datagram Protocol




## About this Manual

This document provides instructions for pre-installation site survey, operation, troubleshooting, and maintenance of MBsecure system.


This document uses various types of messages. An explanation of each type, in the appropriate format, is given below.

	<p><b>NOTE</b></p> <p>A note provides important information, emphasizing or supplementing the main text. The information does not relate directly to issues that might cause injury to patients or users, or damage to the system.</p>
	<p><b>CAUTION!</b></p> <p>A caution provides information relating to issues that might cause injury to patients or users, or damage to the system.</p>


## Safety First




	<p><b>CAUTION!</b></p> <p>Unpack and use the device in a dry environment.</p>
	<p><b>CAUTION!</b></p> <p>Read this document carefully before using the device.</p>
	<p><b>CAUTION!</b></p> <p>The device has no user-serviceable parts. Do not open the covers!</p>

## Warnings and Precautions

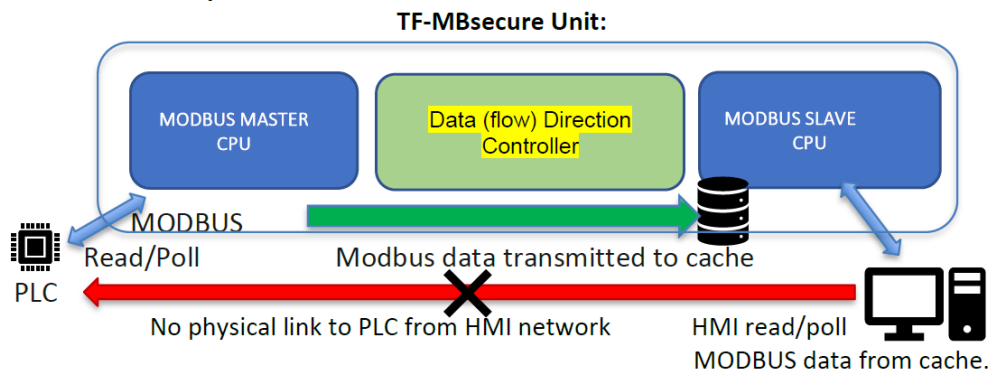
	<p><b>CAUTION!</b></p> <p>Be sure to follow the Power Supply polarity labels on the rear panel. Switching the poles may cause damage to the device.</p>
---	---

## Labels and Symbols

Symbol	Description
	Keep dry

Symbol	Description
	Fragile, handle with care
	This side up
	Electrical and electronic equipment marked with this symbol are covered by the European Directive 2012/19/EU (WEEE). The symbol denotes that the equipment must not be disposed of in the municipal waste system.

### TF\_MBsecure solution diagram:



### Solution Highlights:

- PLC is secure from attacks at OSI Layer-1, physical link.
- MODBUS data is collected from PLC and made available for HMI.
- PLC read/poll command interval is configurable for maximum accuracy.
- Near Zero (30µs on average) latency through the unit.
- HMI restriction, only configured HMI units may request data.
- Unit is a network device / bridge, not a service or an application server.
- Unit configuration is available only via the PLC side (WEB GUI).
- No access to the unit from the HMI SIDE due to security hazards.

## MBsecure Panels

### Front Panel

The front panel includes:

- 6 LEDs in one row:
  - The left-most and right most LEDs indicate (blink) when there is MODBUS traffic through the device.
  - The 4 LEDs between the traffic indicators show the data flow direction through the device, regardless of actual traffic.
- Hard Reset switch for restoring factory settings. (Press and hold for 10 seconds)

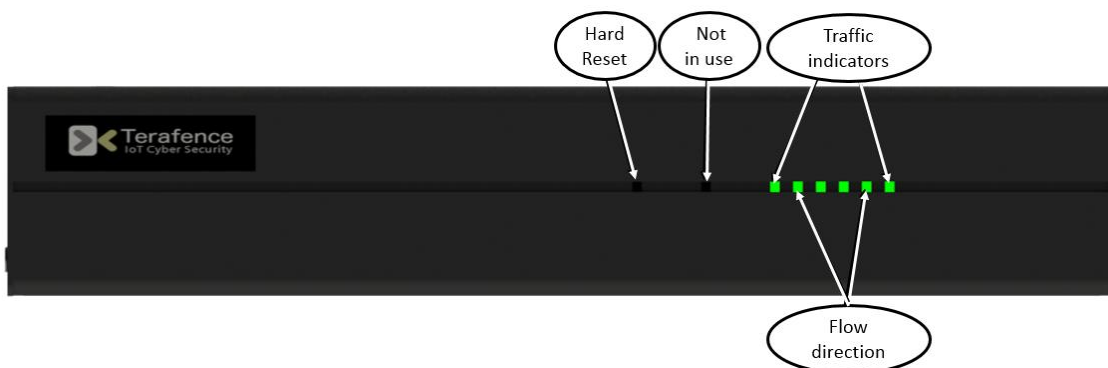


Figure 1: MBsecure Front Panel

### Rear Panel

The rear panel includes:

- Module A (PLC Side) and Module B (HMI Side) RJ-45 Ethernet ports
- DC power ports (3x2)

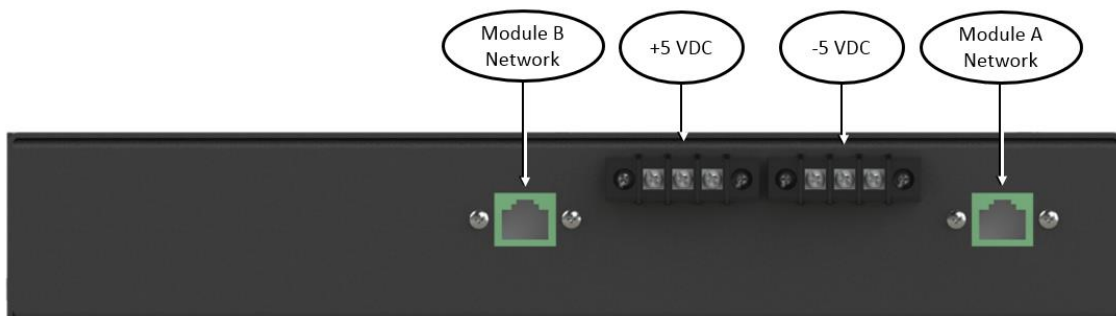


Figure 2: MBsecure Rear Panel

## MBsecure Installation

### What's in the box

Item	Quantity
MBsecure device	1
5 VDC Power Supply	3
Installation and Operation manual	1
Warranty Card	1

### Installing MBsecure

1. Unpack the device and verify that the box content is as listed in [What's in the box](#) section.
2. Connect both Module A and Module B to the same network switch using RJ45 Ethernet cables (not provided with the device).
3. Connect a computer to the same network switch.
4. Configure the computer Ethernet port settings to:
  - a. IP address: 192.168.1.3
  - b. Subnet MASK: 255.255.255.0
5. Connect the power supplies to the device. Wait for the device to boot.



#### CAUTION!

Be sure to follow the Power Supply polarity labels on the rear panel. Switching the poles may cause damage to the device.

6. Open your Internet Browser and access the unit at IP address 192.168.1.1. the Login screen will be displayed.

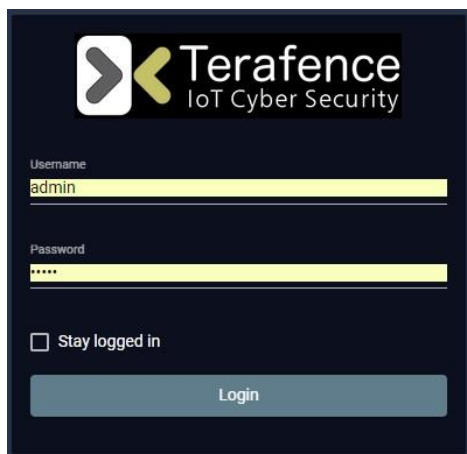


Figure 3: MBsecure Login menu





#### NOTE

There is no user interface for Module B at IP address 192.168.1.2 but you can ping Module B to verify connectivity.

7. Log in using the following credentials:

- User Name: Admin
- Password: admin

8. Once logged in, you will see MBsecure configuration screen:

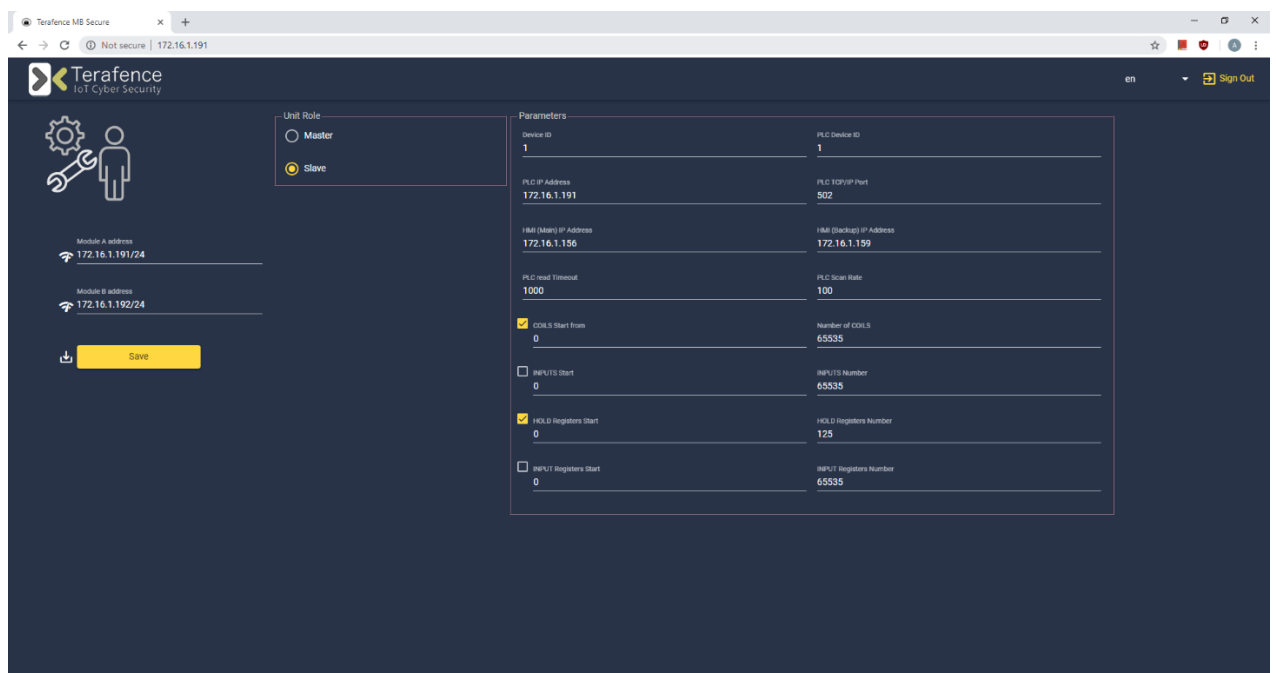


Figure 4: MBsecure Configuration Menu

## Configuring MBsecure

1. Select the Unit role:

- MASTER – The unit will function as an HMI application requesting data from the PLC at given intervals (PLC Scan Rate), according to the configured function (MODBUS function).
- SLAVE – The unit will behave as a PLC waiting for information to be pushed from the configured PLC. The data pushed is propagated to Module “B” where it is made available to the HMI for retrieval.

If the Role is set to MASTER, select the “Modbus Function” from the drop-down list.


2. Configure the relevant MODBUS parameters according to Table 1.


Table 1: Configuration Parameters Explained

Parameter	Configuration of	Description
Module B Address	MBsecure Module B LAN Port	Module B IP Address to communicate with HMI
Module A Address	MBsecure Module A LAN Port	Module A IP Address to communicate with PLC
Device ID	MBsecure Module B	MBsecure MODBUS device ID as configured in the HMI application
PLC Device ID	PLC	MODBUS ID designating the PLC
PLC IP Address	PLC	TCP/IP Address to access the PLC over Ethernet.
PLC TCP/IP Port	PLC	PLC TCP Port to access for data.
HMI IP Address (Main)	HMI Main computer	Only HMI from this address will be served. All other requests will be dropped.
HMI IP Address (Backup)	HMI Backup computer	Only HMI from this address will be served. All other requests will be dropped.
HMI side TCP Port	MBsecure Module B	Must match the configuration in the HMI unit (if other than default)
PLC Read Timeout	MBsecure Module A	Number of milliseconds before timeout is declared and error is generated.
PLC Scan Rate	MBsecure Module A	Number of milliseconds between each data request from the PLC.
COILS start from	Read Coils	Set the first COIL number to read


Parameter	Configuration of	Description
Number of COILS	Read Coils	COILS range. Number of COILS in total to read
INPUTS Start	Discrete Inputs	Set the first INPUTS number to read
INPUTS Number	Discrete Inputs	INPUTS range Number on consecutive INPUTS to read
HOLD Registers Start	Read Holding Registers	Set the first HOLD Register number to read
HOLD Register Number	Read Holding Registers	HOLD Registers range Number on consecutive HOLD Registers to read
INPUT Register Start	Read Input Registers	First INPUT Register to read
INPUT Registers Number	Read Input Registers	Number on consecutive INPUT Registers to read
MODBUS Function	MBsecure Module A	Select the desired data option

3. Select the PLC parameter to read by ticking the check-box. More than one can be selected. Selecting none will deactivate the unit.
4. Configure the unit Module “A” and Module “B” IP address as required on-site.

	<p><b>NOTE</b></p> <p>It is recommended to capture a screen shot at this point to document the configuration.</p>
---	---

	<p><b>CAUTION!</b></p> <p>MBsecure default configuration Module IP addresses is set as 192.168.1.1 for Module “A” and 192.168.1.2 for Module “B”.</p> <p>Once configured, please remember to revert your PC addresses to match the new IP addresses as configured. After pressing “SAVE” the new addresses would take affect within a few seconds.</p>
---	--

5. Verify that all parameters are configured correctly.
6. Click **Save** to save the configuration and deploy setting to Module “A” and Module “B”. Wait a few seconds to allow the unit to reboot.
7. Configure the computer to match the same IP network as configured in MBsecure and access the unit once again to verify the saved configuration.
8. If all works well, connect the unit into the operational network. Side “A” to the PLC side, Side “B” to the HMI side.
9. Test the HMI application.

	<p><b>NOTE</b></p> <p>If the connection cannot be established, <b>restore factory settings</b> by pressing the hard-reset button on the front panel and re-configure the device. (Press and hold for 10 seconds)</p>
---	--

## Technical Specifications

### Hardware

<b>Size</b>	W 290 mm, H50 mm, D230 mm
<b>Mounting</b>	Desktop or 19" Rack Shelf; DIN Rail
<b>Power supplies</b>	3x 5VDC 2.5Amp directly connected with no redundancy. <b>Optional:</b> 2 x 5.5VDC 7.5Amp with redundancy
<b>Power consumption</b>	270W
<b>Indicators</b>	Front Panel indication LEDs
<b>Controls</b>	Hard reset on the front panel
<b>Data transfer speed</b>	1 Gbps
<b>Network connections</b>	2x1 Gbps LAN ports
<b>Weight</b>	450gr

### Environmental Conditions

For proper functioning of the system, ensure that MBsecure is used under regular office environment conditions.

### Limited Warranty

WE GUARANTEE THAT ALL OUR PRODUCTS WILL BE FREE FROM DEFECTS IN MATERIALS AND WORKMANSHIP WHEN PURCHASED BY END-USERS. WE ALSO PROVIDE, WITH RESPECT TO OUR PRODUCTS' HARDWARE COMPONENTS ONLY, A 12-MONTH LIMITED GUARANTEE PERIOD, COMMENCING ON THE DATE OF INITIAL PURCHASE, PROVIDED THAT THE PRODUCTS WAS UNDER NORMAL USE AND PROPER HANDLING.

PURCHASERS WILL BE ENTITLED TO REPAIR OR REPLACEMENT OF DEFECTIVE UNITS. TO OBTAIN WARRANTY SERVICE, PURCHASERS SHALL RETURN THE DEFECTIVE PRODUCT, IN ITS ORIGINAL PACKAGE, AND THE PROOF OF PURCHASE TO THE ORIGINAL PLACE OF PURCHASE. TERAENCE RESERVES THE RIGHT TO REPAIR OR REPLACE THE PRODUCT AT ITS SOLE DISCRETION.

IN THE EVENT THE ORIGINAL PLACE OF PURCHASE IS NOT REACHABLE, PURCHASERS SHALL CONTACT TERAENCE IN ORDER TO OBTAIN A RETURN MATERIAL AUTHORIZATION (RMA) AND RETURN THE DEFECTIVE PRODUCT TOGETHER WITH PROOF OF PURCHASE TO THE LOCATION SPECIFIED BY TERAENCE UNDER THE RMA.

TO THE EXTENT THAT A PRODUCT IS REPLACED, THE PURCHASER WILL OWN THE REPLACING PRODUCT AND THE PRODUCT BEING REPLACED WILL BE THE PROPERTY OF TERAENCE.

### Warranty Card

Upon receipt of the device, fill in the provided Warranty Card and send it to the address indicated on the front page of this manual.

## Appendix A: MBSecure Configuration Sheet

For your convenience, below is the MBSecure Configuration Sheet. Use the provided table to record the Device settings for future use.

Parameter	Configuration of	Description	Value
Module B Address	MBsecure Module B	Module B IP Address to communicate with HMI	
Module A Address	MBsecure Module A	Module A IP Address to communicate with PLC	
Device ID	MBsecure Module B	MBsecure MODBUS device ID as configured in the HMI application	
PLC Device ID	PLC	MODBUS ID designating the PLC	
PLC IP Address	PLC	TCP/IP Address to access the PLC over Ethernet.	
PLC TCP/IP Port	PLC	PLC TCP Port to access for data.	
HMI IP Address (Main)	HMI Main computer	Only HMI from this address will be served. All other requests will be dropped.	
HMI IP Address (Backup)	HMI Backup computer	Only HMI from this address will be served. All other requests will be dropped.	
HMI side TCP Port	MBsecure Module B	Must match the configuration in the HMI unit	
PLC Read Timeout	MBsecure Module A	Number of milliseconds before timeout is declared and error is generated.	
PLC Scan Rate	MBsecure Module A	Number of milliseconds between each data request from the PLC.	
COILS start from	Read Coils	Set the first COIL number to read	
Number of COILS	Read Coils	COILS range. Number of COILS in total to read	
INPUTS Start	Discrete Inputs	Set the first INPUTS number to read	

<b>Parameter</b>	<b>Configuration of</b>	<b>Description</b>	<b>Value</b>
INPUTS Number	Discrete Inputs	INPUTS range Number on consecutive INPUTS to read	
HOLD Registers Start	Read Holding Registers	Set the first HOLD Register number to read	
HOLD Register Number	Read Holding Registers	HOLD Registers range Number on consecutive HOLD Registers to read	
INPUT Register Start	Read Input Registers	First INPUT Register to read	
INPUT Registers Number	Read Input Registers	Number on consecutive INPUT Registers to read	