Modbus Serial Communication Device Type Manager

User Manual

03/2015

EIO0000000233.05

www.schneider-electric.com

Schneider Electric

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

Table of Contents

Safety Information

Important Information

NOTICE

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

PLEASE NOTE

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

About the Book

At a Glance

Document Scope

This user manual is intended to describe the use of the Communication Device Type Manager (Comm DTM) for Modbus.

Validity Note

This document has been updated with the release of the Modbus Communication Library V2.5.

Product Related Information

⚠ WARNING

LOSS OF CONTROL

- The designer of any control scheme must consider the potential failure modes of control paths and, for certain critical control functions, provide a means to achieve a safe state during and after a path failure. Examples of critical control functions are emergency stop and overtravel stop, power outage and restart.
- Separate or redundant control paths must be provided for critical control functions.
- System control paths may include communication links. Consideration must be given to the implications of unanticipated transmission delays or failures of the link.
- Observe all accident prevention regulations and local safety guidelines.[1]
- Each implementation of this equipment must be individually and thoroughly tested for proper operation before being placed into service.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

[1] For additional information, refer to NEMA ICS 1.1 (latest edition), "Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control" and to NEMA ICS 7.1 (latest edition), "Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems" or their equivalent governing your particular location.

Chapter 1
Hardware and Software Requirements

What Is in This Chapter?

This chapter contains the following topics:

System Requirements

Hardware Requirements

Requirement	Minimum	Recommended
Computer	Pentium 4 or equivalent	Core 2 duo
RAM	1 GB	2 GB
Free hard drive space on system drive	30 MB	
Free hard drive space on installation drive	60 MB	
Swap file	1024 MB	2048 MB
Monitor display	256 color SVGA 800 x 600 resolution	True color XGA 1024 x 768 resolution

Software Requirements

Software operating systems

Operating System	Edition/Service Pack	Special Considerations
Windows 7 32 bit	SP1	You need administrator access rights to install the Modbus SL Comm DTM
Windows 7 64 bit	SP1	
Windows 8.1 Professional	–	

Software installed on the PC

Software	Edition	Special Considerations
Microsoft.NET Framework	V2.0 SP2	–
FDT Frame Application	FDT 1.2 or FDT 1.2.1	The Modbus SL Comm DTM requires an FDT Frame Application compliant to the FDT standard. The FDT Frame Application must support the Microsoft.NET Framework 2.0.
Schneider Modbus serial PC driver	For information about the supported Schneider Modbus serial PC driver editions, refer to the *ReleaseNotes* file of the Schneider Electric Modbus communication library.	–

Compatibility

FDT Compatibility

The Modbus Comm DTM is compliant to the FDT standards FDT 1.2 and FDT 1.2.1. It is based on the FDT Modbus annex 1.0.

Modbus Compatibility

The Modbus Comm DTM supports Modbus services specified in the Modbus application protocol specification V1.1b.

Considerations

Modbus Connections

The maximum number of concurrent Modbus connections is limited to four connections. After installation of the Modbus Driver, one Modbus connection is created by default.

If more connections are required, perform the following steps:

- Open the Windows **Control Panel**.
- Double-click the **Driver Manager** icon.
- Open the **Modbus Serial Driver** tab
- Configure and start all four instances of the Modbus serial PC driver.
- Check if all instances are running (four icons of the Modbus serial driver in the system tray).

NOTE: To perform these steps, administrator access rights are required.

Installing and Removing

Installation

Double-click the file *Schneider Electric Modbus Communication DTM Library.exe* and follow the instructions in the installation wizard.

Removal

To remove the DTM from your computer, choose **Start** → **Settings** → **Control Panel** → **Add/Remove Programs**.

Chapter 2
Connection Types and Communication Models

Introduction

This chapter gives an overview about the different configurations that can be used to establish Modbus communications.

What Is in This Chapter?

This chapter contains the following topics:

Connection Types

Introduction

The Modbus SL Comm DTM can be used to establish Modbus communications based on different connection types.

Serial Connection

The Modbus SL Comm DTM provides the possibility to establish a Modbus communication via a standard PC serial port.

USB/RS232, USB/RS485 Converter Connection

The Modbus SL Comm DTM can be used to establish a Modbus communication via a USB/RS232 or USB/RS485 converters.

NOTE: The Modbus SL Comm DTM only supports USB converters which can be accessed as virtual COM ports.

USB Connection

The Modbus SL Comm DTM can be used to establish a Modbus communication by using the following cables:

- TCS XCN AMUM3P
- UNY XCA USB 033
- BMX XCA USB H018/045

Gateway Connection

The Modbus SL Comm DTM can be used to establish a Modbus communication to Modbus serial devices behind a Modbus TCP/Modbus serial gateway. In this case, the connection is established via the Ethernet network adapter of the PC.

Bluetooth Connection

The Modbus SL Comm DTM provides the possibility to establish a Modbus communication via Bluetooth.

NOTE: The Modbus SL Comm DTM only supports Bluetooth adapters which implement the Bluetooth serial port profile (SPP).

Communication Models

Introduction

This chapter describes the different communication models supported by the Modbus SL Comm DTM.

NOTE: The FDT Technology is not designed for real-time data transfer. Depending on your system and communication model you employ, the data may not reflect the actual, real-time device state.

⚠ WARNING

INVALID DEVICE STATE INFORMATION

Do not use the Modbus Comm DTM for time critical controlling or monitoring tasks because the transferred data may not reflect the actual device state. The FDT Technology is not designed for this purpose.

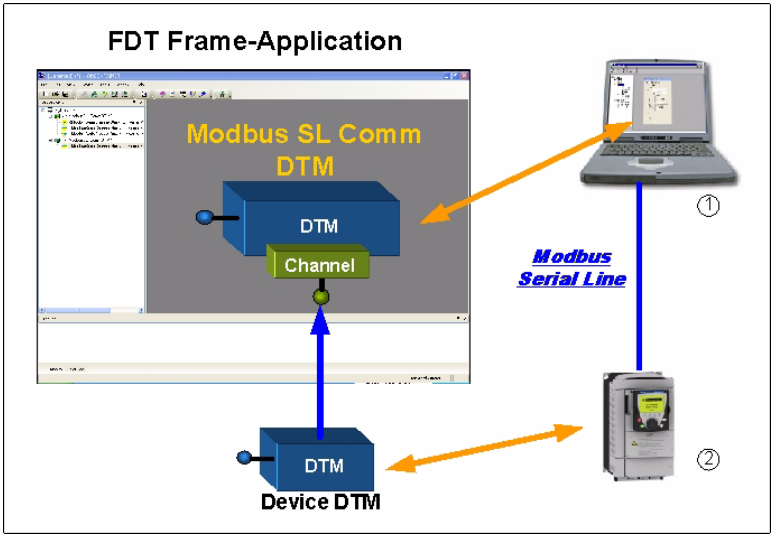
Failure to follow these instructions can result in death, serious injury, or equipment damage.

Direct Connection

The Modbus SL Comm DTM can be used to establish a direct Modbus communication between the PC and the target device.

For the direct connection the following physical connection types are supported:

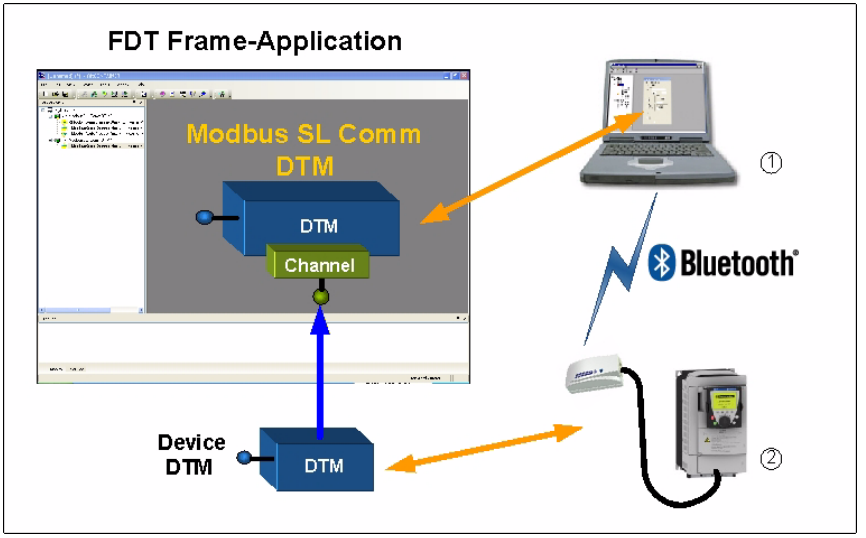
- RS-232
- RS-485 by using an RS232/RS485 converter
- USB by using a USB/Serial line converter
- USB by using a direct USB cable (see your hardware manual for the correct cable reference)



1 PC with Modbus SL Comm DTM
2 target device

Bluetooth Connection

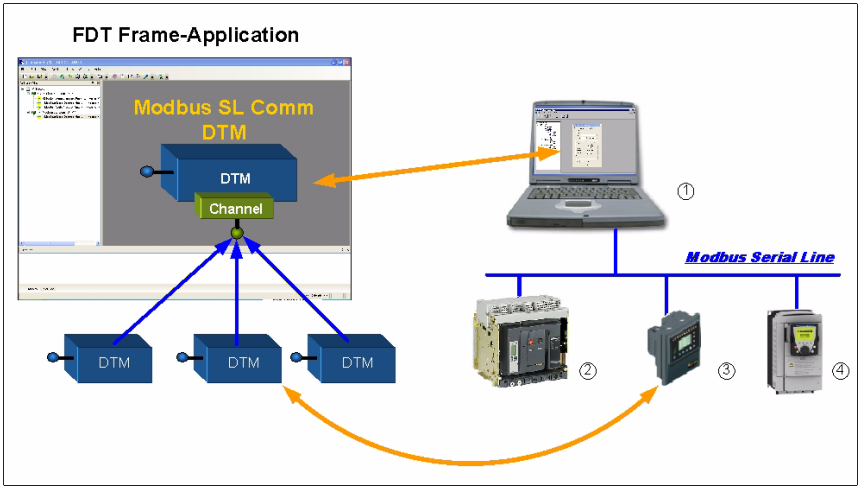
The Modbus SL Comm DTM can be used to establish a direct Modbus communication between the PC and the target device via Bluetooth.



1 PC with Modbus serial comm DTM
2 target device

Bus Connection

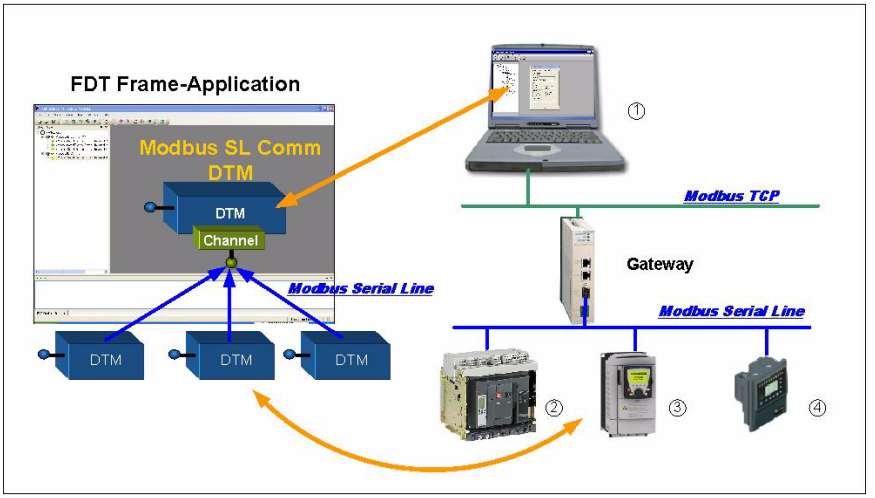
The Modbus SL Comm DTM can be used with a RS232/RS485 converter to establish a Modbus communication to a Modbus serial line bus.



1 PC with Modbus SL Comm DTM
2-4 target devices

Gateway Connection

The Modbus SL Comm DTM can be used to establish a Modbus communication to Modbus serial devices behind a Modbus TCP/Modbus serial gateway.



1 PC with Modbus SL Comm DTM
2-4 target devices

Chapter 3
Graphical User Interface

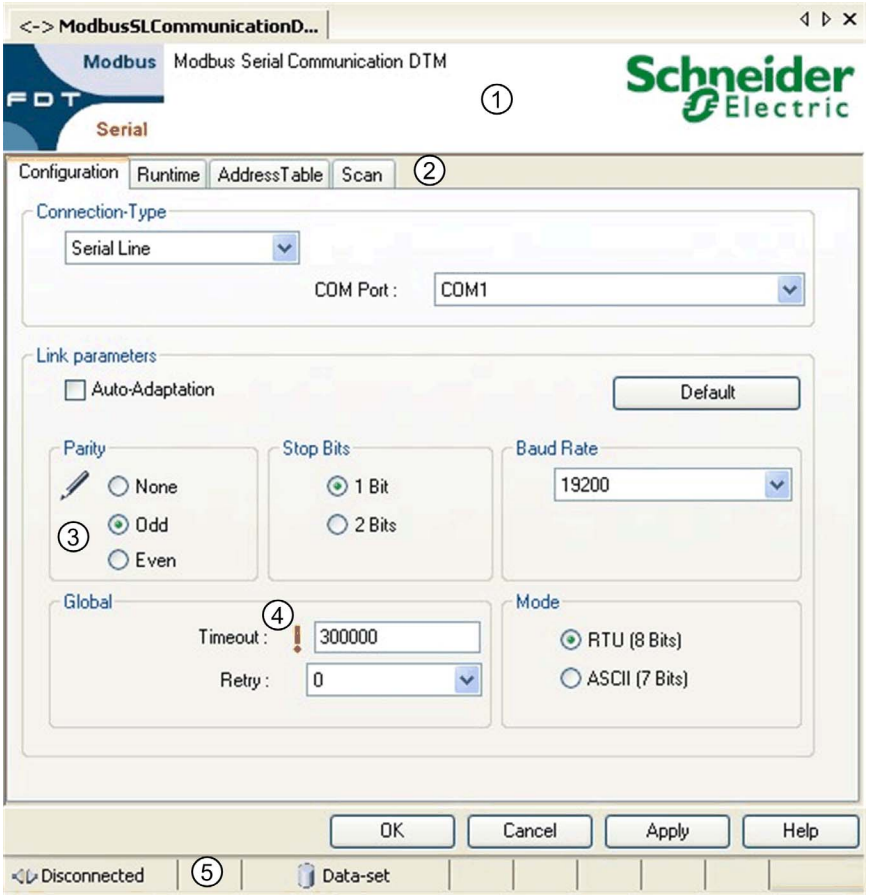
Graphical User Interface

Overview

This chapter describes the graphical user interface (GUI) of the Modbus SL Comm DTM.

Introduction

The following figure shows the GUI (graphical user interface) of the DTM.



1 Identification area
2 Tab menu
3-4 Parameter status icons
5 Status bar

Identification Area

The identification area shows the name and the version of the DTM.

Tab Menu

Use the tab menu to access the different functions provided by the DTM.

Parameter Status Icons

The parameter status icons provide information about the current state of the parameter.

Possible parameter states

Icon	Meaning
	The parameter was modified and has an invalid value.
	The parameter was modified and has a valid value

Status Bar

The status bar provides information about the current status of the DTM.

Possible connection states

Icon	Text	Meaning	DTM State
	Connecting	connecting	going online
	Connected	connected	online
	Disconnecting	disconnecting	going offline
	Interrupted	interrupted	detected communication interruption
	Disconnected	disconnected	all other states

Possible data source states

Icon	Text	Behavior
	Data set	Displayed values are loaded from the instance data set. Changed values are affected on the instance data set only.
	Data set locked	Displayed values are loaded from the instance data set. Data set is locked.

Chapter 4
Configuration

What Is in This Chapter?

This chapter contains the following topics:

Configuration Tab

Introduction

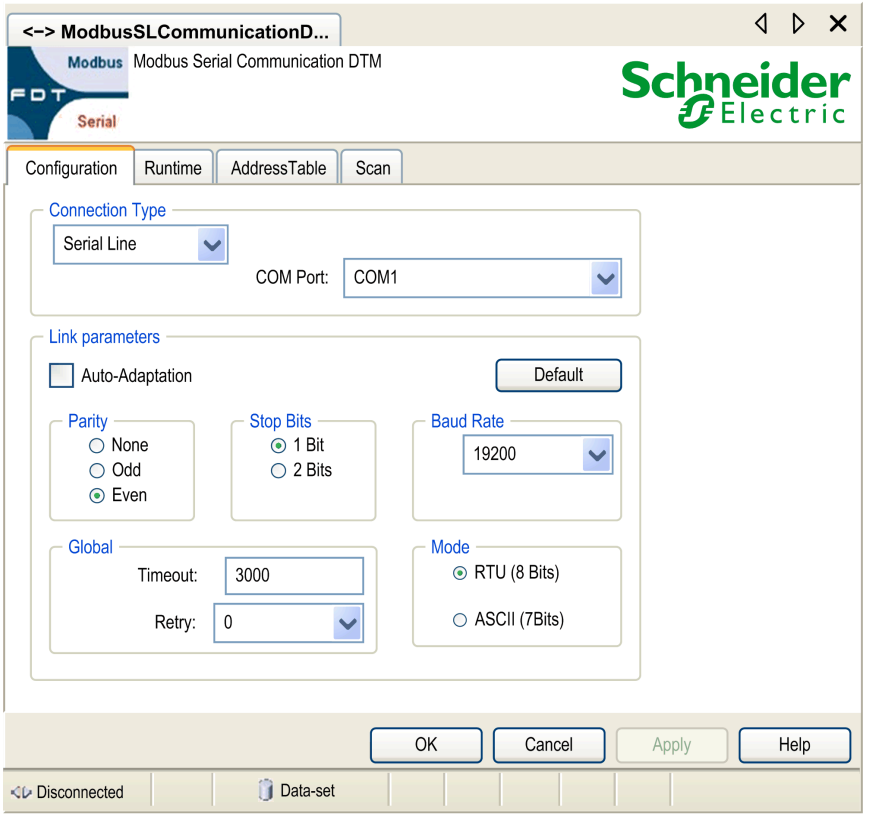
The **Configuration** tab of the Modbus SL Comm DTM contains the communication parameters for the different connection types.

Configuration Tab

You have several possibilities to access the **Configuration** tab of the Modbus Serial Comm DTM:

- In the network view of your FDT Frame Application, double-click the Modbus SL Comm DTM icon.
- In the network view of your FDT Frame Application, right-click the Modbus SL Comm DTM icon and then click **Configuration**.

The following figure shows the **Configuration** tab of the Modbus SL Comm DTM dialog:



Connection Type

In the **Connection Type** list on the **Configuration** tab of the Modbus SL Comm DTM you can select the connection type for the Modbus communication.

The table contains a list of connection types available for selection:

Connection type	Description
Serial line	This connection type shall be selected for the following connections:· ● RS-232 ● RS-485 ● USB to RS-232 converters ● USB to RS-485 converters
Remote gateway	For Modbus communications with serial devices which are located behind a Modbus TCP/Modbus SL gateway select this connection type.
Bluetooth	Select this connection type if the communication to the target device shall be established via Bluetooth.
USB	Select this connection type if you are making a direct USB connection.

Buttons

The table describes the buttons available in the **Configuration** tab

Command	Description
OK	All parameters will be saved and the Modbus SL Comm DTM window will be closed. The new parameter values will be applied at the next connection.
Cancel	All parameter modifications are canceled and the Modbus SL Comm DTM window will be closed. The original values will be applied at the next connection.
Default	Displays the default parameter values.
Apply	Saves the parameters but the Modbus SL Comm DTM window remains open. The new parameter values will be applied at the next connection.

Serial Configuration

Introduction

This chapter describes the parameters for RS232/RS485 connections.

Serial Parameters

The table contains a description of the communication parameters for a serial line connection.

Parameter	Description	Default Value
Auto-Adaptation	Enables/disables the auto-adaptation function, which can be used to detect the communication parameters for Modbus serial line automatically.	Disabled
COM Port	PC COM port	COM1
Baud Rate (Bits/s)	serial line baud rate	19200
Parity	serial line parity	Even
Stop Bits	number of stop bits	1
Timeout	Modbus slave response timeout	3000 ms
Retry	Number of times the Modbus Comm DTM will resend the Modbus request on the serial connection if a communication timeout occurred	0
Mode	Transmission mode: ● RTU (8 Bit) ● ASCII (7 Bit)	RTU

Bluetooth Configuration for Modbus SL Comm DTM

Introduction

This chapter describes the configuration of the Modbus SL Comm DTM for a Bluetooth connection

Bluetooth Configuration

The following table contains a description of the parameters for Bluetooth connections.

Parameter	Description
Bluetooth	This combo box contains a list of found virtual COM Ports provided by the Bluetooth adapters installed on your PC. Select the COM Port on which the Modbus communication shall be established. **NOTE:** If the desired COM Port is not available for selection try to establish the communication with the following configuration: ● set the **Connection Type** to serial line ● select the desired COM Port in the combo box
Global Timeout	Modbus slave response timeout
Retry Number	Number of times the Modbus SL Comm DTM will resend the Modbus request on the Bluetooth connection if a communication timeout occurred.

Remote Gateway Configuration for Modbus SL Comm DTM

Introduction

This chapter describes the configuration of the Modbus SL Comm DTM for the remote gateway connection.

Remote Gateway Configuration

The following table contains a description of the parameters for remote gateway connections.

Parameter	Description
Remote Gateway	IP Address of the Modbus SL Comm DTM gateway behind which the target devices are located
Global Timeout	Modbus slave response timeout
Retry Number	Number of times the Modbus SL Comm DTM will resend the Modbus request if a communication timeout occurred

USB Connection Configuration for Modbus SL Comm DTM

Introduction

This chapter describes the configuration of the Modbus SL Comm DTM for a direct USB connection.

USB Connection Configuration

The following table contains a description of the parameters for an USB connection.

Parameter	Description
Global Timeout	Modbus slave response timeout
Retry Number	Number of times the Modbus SL Comm DTM will resend the Modbus request if a communication timeout occurred.

Runtime Tab

Introduction

The Modbus SL Comm DTM provides different types of runtime information. This chapter describes the information provided by the Modbus SL Comm DTM and the configuration of the log function.

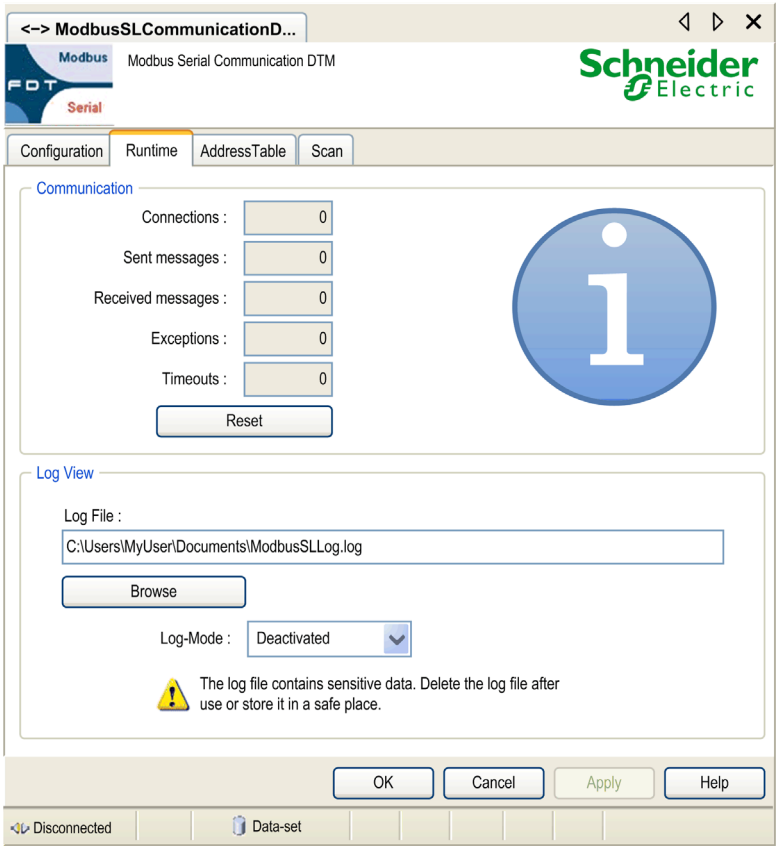
Runtime Tab

The Modbus SL Comm DTM provides different types of runtime information, which can be used to monitor the established communications.

The runtime information is available on the **Runtime** tab of the Modbus SL Comm DTM, which can be accessed in the following manner:

- In the network view of your FDT Frame Application, double-click the Modbus SL Comm DTM icon. Now select the **Runtime** tab.
- In the network view of your FDT Frame Application, right-click the Modbus SL Comm DTM icon and then click **Configuration**. Now select the **Runtime** tab.

The following figure shows the **Runtime** tab of the Modbus SL Comm DTM dialog:



Configuration Commands

The table contains a description of the configuration commands available in the **Runtime** tab.

Command	Description
OK	The parameters will be saved and the Modbus SL Comm DTM window will be closed. The new parameter values will be applied at the next connection.
Cancel	The parameter modifications are canceled and the Modbus SL Comm DTM window will be closed. The original values will be applied at the next connection.
Browse	Opens a file browser to specify the log file path
Reset	Resets all runtime parameters to zero
Apply	Stores the parameters but the Modbus SL Comm DTM window remains open. The new parameter values will be applied at the next connection.

Runtime Parameters

The table contains a description of the runtime parameters available on the **Runtime** tab of the Modbus SL Comm DTM:

Command	Description
Connections	Number of active connections to the Modbus SL Comm DTM.
Sent messages	Number of messages sent by the Modbus SL Comm DTM.
Received messages	Number of messages received by the Modbus SL Comm DTM.
Exceptions	Number of Modbus Exception messages received by the Modbus SL Comm DTM.
Timeouts	Number of detected timeout errors on reception.

Log File

The Modbus SL Comm DTM provides the possibility to create a log file. In the **Log File** box, you have to specify the path in which the log file shall be stored.

The table describes the information which will be written to the log file depending on the selected **Log Mode**:

Log Mode	Description
Deactivated	Disables the log file feature.
Error-Logging	Only information about detected timeout errors and received Modbus exceptions will be written to the log file.
All-Logging	In addition, to the information about detected timeout errors and received Modbus exceptions, information about the sent Modbus requests and received Modbus responses, and the requests received from the device DTM, is written to the log file.

Recommendation for Improved Cyber Security

The log file contains usually sensitive data such as
- Device addresses
- Device names
- Details of the network topology
- Details of the network configuration

It is stored on the hard disk of your PC. Delete the log file as soon as it is no longer needed or store it in a safe place, where unauthorized access is not possible.

Address Table

Introduction

The Modbus Comm DTM provides an address table which lists the connected device DTMs and their target addresses. This chapter describes the information provided in the address table and the configuration of the target addresses of the devices.

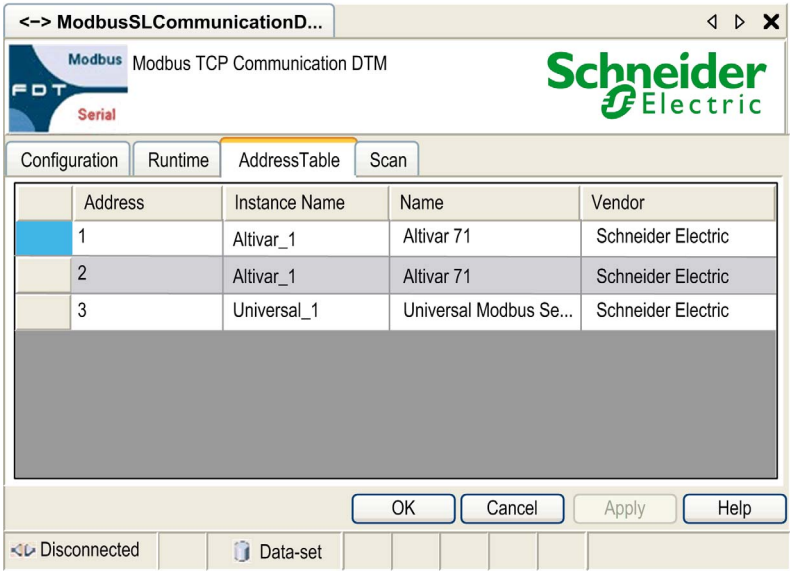
Address Table

The Modbus SL Comm DTM provides an address table which lists the connected device DTMs and their target addresses. In this address table, you can specify the target addresses of the connected device DTMs.

The **Address Table** tab can be accessed in the following manner:

- In the network view of your FDT Frame Application, double-click the Modbus SL Comm DTM icon. Now select the **Address Table** tab.
- In the **Network View** of your FDT Frame Application, right-click the Modbus SL Comm DTM icon and then click **Configuration**. Now select the **Address Table** tab.

The following figure shows the **Address Table** tab of the Modbus SL Comm DTM dialog:



Configuration Commands

The table contains a description of the configuration commands available in the **Address Table** tab

Command	Description
Ok	The modifications will be saved and the Modbus SL Comm DTM window will be closed. The new values will be applied at the next connection.
Cancel	The modifications are canceled and the Modbus SL Comm DTM window will be closed. The original values will be applied at the next connection.
Apply	Stores the modifications but the Modbus SL Comm DTM window remains open. The new values will be applied at the next connection.

Address Information

The table contains a description of the address information available on the **Address Table** tab of the Modbus SL Comm DTM:

Parameter	Description
Address	Target address of the hardware device, which shall be configured with the connected DTM
Instance Name	Instance name of the DTM
Name	DTM-specific name
Vendor	DTM vendor name

Address Assignment

The address table of the Modbus SL Comm DTM can be used to specify the target address of the hardware device, which shall be configured with a specific DTM. To specify the target address, you have to enter the new address in the corresponding **Address** field of this DTM and to validate this modification by clicking either the **Apply** button or by clicking the **Ok** button.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION FOR MODBUS SL

Do not communicate to a device with an address of 248 on a bus with multiple Modbus devices connected.

Only establish connections to a device using an address of 248 point-to-point; that is, directly between the PC and the device.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Scan Configuration

Introduction

The Modbus Comm DTM provides the possibility to specify the range of the scanned addresses for the FDT scan. This chapter describes the configuration of the scan parameters for the FDT scan.

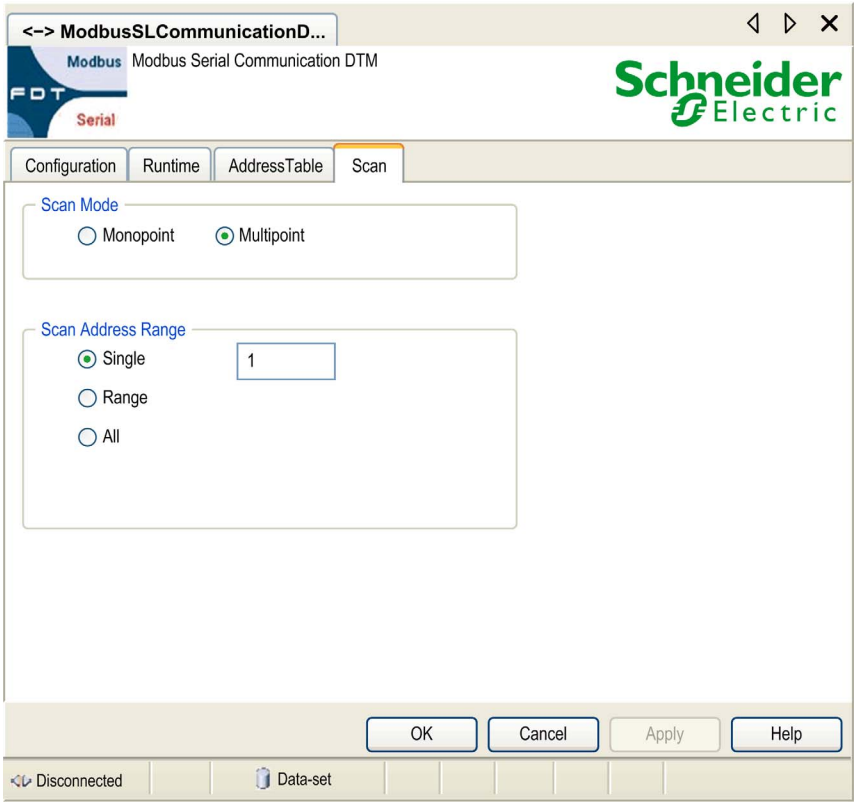
Scan Tab

The Modbus SL Comm DTM supports the scan function as it is defined the FDT specification V1.2.1. The scan can be used to build the network topology of the underlying communication network automatically. The Modbus SL Comm DTM provides the possibility to specify the range of the scanned addresses.

The scan parameters are available on the **Scan** tab of the Modbus SL Comm DTM, which can be accessed in the following manner:

- In the **Network View** of your FDT Frame Application, double-click the Modbus SL Comm DTM icon. Now select the **Scan** tab.
- In the **Network View** of your FDT Frame Application, right-click the Modbus SL Comm DTM icon and then click **Configuration**. Now select the **Scan** tab.

The figure shows the **Scan** tab of the Modbus SL Comm DTM dialog:



Configuration Commands

The table contains a description of the configuration commands available in the **Scan** tab:

Command	Description
OK	The modifications will be saved and the Modbus Comm DTM window will be closed. The new values will be applied at the next scan.
Cancel	The modifications are canceled and the Modbus Comm DTM window will be closed. The original values will be applied at the next scan.
Apply	Stores the modifications but the Modbus Comm DTM window remains open. The new values will be applied at the next scan.

Scan Parameters for Modbus SL

The table contains a description of the scan parameters available on the **Scan** tab of the Modbus SL Comm DTM:

Command	Description	
Scan Mode	**Scan Mode**:	
	Monopoint	Select this connection type only for direct connections, where the target device is directly connected to the PC (scanned address range: 248).
	Multipoint	Select this connection type only for multipoint connections, where the PC is connected to a Modbus serial line network.
Scan Address Range	**Scan Address Range**:	
	Single	Scans only a single address of one target device in the range between 1...247.
	Range	Scans a specified address range between 1...247.
	All	Scans the complete address range of the Modbus serial connection (all addresses between 1...247.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

Do not use the scan mode “Monopoint” on a Modbus multipoint network.

Only use the scan mode “Monopoint” with point-to-point communication; that is, directly between the PC and the device.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Chapter 5
Cyber Security

Introduction

Cyber security is a branch of network administration that addresses attacks on or by computer systems and through computer networks that can result in accidental or intentional disruptions. The objective of cyber security is to help provide increased levels of protection for information and physical assets from theft, corruption, misuse, or accidents while maintaining access for their intended users.

No single cyber security approach is adequate. Schneider Electric recommends a defense-in-depth approach. Conceived by the National Security Agency (NSA), this approach layers the network with security features, appliances, and processes. The basic components of this approach are:

- risk assessment
- a security plan built on the results of the risk assessment
- a multi-phase training campaign
- physical separation of the industrial networks from enterprise networks using a demilitarized zone (DMZ) and the use of firewalls and routing to establish other security zones
- system access control
- device hardening
- network monitoring and maintenance

This chapter defines elements that help you configure a system that is less susceptible to cyber attacks. For detailed information on the defense-in-depth approach, refer to the *TVDA: How Can I Reduce Vulnerability to Cyber Attacks in the Control Room* on the *Schneider Electric website*.

What Is in This Chapter?

This chapter contains the following topics:

What is Cyber Security?

Introduction

Cyber threats are deliberate actions or accidents that can disrupt the normal operations of computer systems and networks. These actions can be initiated from within the physical facility or from an external location. Security challenges for the control environment include:

- diverse physical and logical boundaries
- multiple sites and large geographic spans
- adverse effects of security implementation on process availability
- increased exposure to worms and viruses migrating from business systems to control systems as business-control communications become more open
- increased exposure to malicious software from USB devices, vendor and service technician laptops, and the enterprise network
- direct impact of control systems on physical and mechanical systems

Sources of Cyber Attacks

Implement a cyber security plan that accounts for various potential sources of cyber attacks and accidents, including:

Source	Description
internal	● inappropriate employee or contractor behavior ● disgruntled employee or contractor
external opportunistic (non-directed)	● script kiddies* ● recreational hackers ● virus writers
external deliberate (directed)	● criminal groups ● activists ● terrorists ● agencies of foreign states
accidental	
* slang term for hackers who use malicious scripts written by others without necessarily possessing a comprehensive understanding of how the script works or its potential impact on a system	

A deliberate cyber attack on a control system may be launched to achieve a number of malicious results, including:

- disrupt the production process by blocking or delaying the flow of information
- damage, disable, or shut down equipment to negatively impact production or the environment
- modify or disable safety systems to cause intentional harm

How Attackers Gain Access

A cyber attacker bypasses the perimeter defenses to gain access to the control system network. Common points of access include:

- dial-up access to remote terminal unit (RTU) devices
- supplier access points (such as technical support access points)
- IT-controlled network products
- corporate virtual private network (VPN)
- database links
- poorly configured firewalls
- peer utilities

Cyber Security Certifications

Schneider Electric developed cyber security guidelines based on the following recommendations:

- Achilles
- ISA Secure

Questions?

To submit a cyber security question, report security issues, or get the latest news from Schneider Electric, visit our *website*.

Schneider Electric Guidelines

Introduction

Your PC system can run a variety of applications to enhance security in your control environment. The system has factory default settings that require reconfiguration to align with Schneider Electric's device hardening recommendations of the defense-in-depth approach.

The following guidelines describe procedures in a Windows 7 operating system. They are provided as examples only. Your operating system and application may have different requirements or procedures.

Disabling Unused Network Interface Cards

Verify that network interface cards not required by the application are disabled. For example, if your system has 2 cards and the application uses only one, verify that the other network card (Local Area Connection 2) is disabled.

To disable a network card in Windows 7:

Step	Action
1	Open **Control Panel** → **Network and Internet** → **Network and Sharing Center** → **Change Adapter Settings**.
2	Right-click the unused connection. Select **Disable**.

Configuring the Local Area Connection

Various Windows network settings provide enhanced security aligned with the defense-in-depth approach that Schneider Electric recommends.

In Windows 7 systems, access these settings by opening **Control Panel** → **Network and Internet** → **Network and Sharing Center** → **Change Adapter Settings** → **Local Area Connection (x).**

This list is an example of the configuration changes you might make to your system on the **Local Area Connection Properties** screen:

- Disable all IPv6 stacks on their respective network cards. (This system example does not require the IPv6 address range and disabling the IPv6 stacks limits vulnerability to potential IPv6 security risks.
- Disable **File and Print Sharing for Microsoft Network**.

Schneider Electric's defense-in-depth recommendations also include the following:

- Define only static IPv4 addresses, subnet masks, and gateways.
- Do not use DHCP or DNS in the control room.

Managing Windows Firewall

Schneider Electric's defense-in-depth approach recommendations include enabling the Windows host firewall on all system PCs. Enable the firewalls for any public or private profile listed.

It is recommended practice that users define firewall rules that refuse connections to or from any unknown/untrusted external host.

Disabling the Remote Desktop Protocol

Schneider Electric's defense-in-depth approach recommendations include disabling remote desktop protocol (RDP) unless your application requires the RDP. The following steps describe how to disable the protocol:

Step	Action
1	In Windows 2008R2 or Windows 7, disable RDP via **Computer** → **System Properties** → **Advanced System Settings**.
2	On the **Remote** tab, deselect the **Allow Remote Assistance Connections to this Computer** check box.
3	Select the **Don't Allow Connection to this Computer** check box.

Updating Security Policies

Update the security policies on the PCs in your system by `gpupdate` in a command window. For more information, refer to the Microsoft documentation on `gpupdate`.

Disabling LANMAN and NTLM

The Microsoft LAN Manager protocol (LANMAN or LM) and its successor NT LAN Manager (NTLM) have vulnerabilities that make their use in control applications inadvisable.

The following steps describe how to disable LM and NTLM in a Windows 7 or Windows 2008R2 system:

Step	Action
1	In a command window, execute `secpol.msc` to open the **Local Security Policy** window.
2	Open **Security Settings** → **Local Policies** → **Security Options**.
3	Select **Send NTLMv2 response only. Refuse LM & NTLM** in the **Network Security: LAN Manger authentication level** field.
4	Select the **Network Security: Do not store LAN Manager hash value on next password change** check box.
5	In a command window, enter `gpupdate` to commit the changed security policy.

Managing Updates

Before deployment, update all PC operating systems using the utilities on Microsoft's **Windows Update** Web page. To access this tool in Windows 2008R2, Windows 7, or Windows XP, select **Start** → **All Programs** → **Windows Update**.

Glossary

C

configuration

The arrangement and interconnection of hardware components within a system and the hardware and software selections that determine the operating characteristics of the system.

CRC

cyclic redundancy check

Messages that implement this error checking mechanism have a CRC field that is calculated by the transmitter according to the content of the message. Receiving nodes recalculate the field. Disagreement in the 2 codes indicates a difference between the transmitted message and the one received.

D

DTM

A DTM (Device Type Manager) is a kind of device driver, which is provided by the field device vendor. The DTM contains the device-specific information and provides a graphical user interface. The DTM can be used to perform monitoring tasks and configuration tasks on the specific device. A DTM is not a standalone application. It requires an FDT Frame Application to run.

E

Ethernet

A LAN wiring and signaling specification used to connect devices within a defined area, for example, a building. Ethernet uses a bus or a star topology to connect different nodes on a network.

F

FDT

The FDT (Field Device Tool) technology standardizes the communication interface between field devices and systems (*www.fdtgroup.org*).

function code

A function code is an instruction set commanding 1 or more slave devices at a specified address(es) to perform a type of action, for example, read a set of data registers and respond with the content.

G

gateway
A program or hardware that passes data between networks

I

interface
The interface represents the physical connection to the network, for example a network card or a USB to RS 232 converter.

IP
Internet protocol.

That part of the TCP/IP protocol family that tracks the Internet addresses of nodes, routes outgoing messages, and recognizes incoming messages.

L

LAN
local area network.

A short-distance data communications network.

M

master/slave model
The direction of control in a network that implements the master/slave model is from the master to the slave devices.

MB
abbreviation for Modbus

Modbus
Modbus is an application layer messaging protocol. Modbus offers many services specified by function codes.

S

SL
abbreviation for Serial Line

T

TCP

transmission control protocol.

A connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP suite of protocols.

telegram

A data packet used in serial communication.

Index