Modbus 串行通讯设备类型管理器
用户手册

02/2019

EIO0000000371.06

www.schneider-electric.com

Schneider Electric

本文档中提供的信息包含有关此处所涉及产品之性能的一般说明和/或技术特性。本文档并非用于(也不代替) 确定这些产品对于特定用户应用场合的适用性或可靠性。任何此类用户或设备集成商都有责任就相关特定应用场合或使用方面对产品执行适当且完整的风险分析、评估和测试。Schneider Electric 或其任何附属机构或子公司对于误用此处包含的信息而产生的后果概不负责。如果您有关于改进或更正此出版物的任何建议、或者从中发现错误、请通知我们。

本手册可用于法律所界定的个人以及非商业用途。 在未获得施耐德电气书面授权的情况下，不得翻印传播本手册全部或部分相关内容、亦不可建立任何有关本手册或其内容的超文本链接。施耐德电气不对个人和非商业机构进行非独占许可以外的授权或许可。 请遵照本手册或其内容原义并自负风险。与此有关的所有其他权利均由施耐德电气保留。

在安装和使用本产品时，必须遵守国家、地区和当地的所有相关的安全法规。出于安全方面的考虑和为了帮助确保符合归档的系统数据，只允许制造商对各个组件进行维修。

当设备用于具有技术安全要求的应用场合时，必须遵守有关的使用说明。

未能使用施耐德电气软件或认可的软件配合我们的硬件，则可能导致人身伤害、设备损坏或不正确的运行结果。

不遵守此信息可能导致人身伤害或设备损坏。

目录

安全信息

重要信息

声明

在试图安装、操作、维修或维护设备之前，请仔细阅读下述说明并通过查看来熟悉设备。下述特定信息可能会在本文其他地方或设备上出现，提示用户潜在的危险，或者提醒注意有关阐明或简化某一过程的信息。

在“危险”或“警告”标签上添加此符号表示存在触电危险，如果不遵守使用说明，会导致人身伤害。

这是提醒注意安全的符号。提醒用户可能存在人身伤害的危险。请遵守所有带此符号的安全注意事项，以避免可能的人身伤害甚至死亡。

⚠ 危险

危险表示若不加以避免，将**会导致**严重人身伤害甚至死亡的危险情况。

⚠ 警告

警告表示若不加以避免，可能**会导致**严重人身伤害甚至死亡的危险情况。

⚠ 小心

小心表示若不加以避免，可能**会导致**轻微或中度人身伤害的危险情况。

注意

注意用于表示与人身伤害无关的危害。

请注意

电气设备的安装、操作、维修和维护工作仅限于有资质的人员执行。施耐德电气不承担由于使用本资料所引起的任何后果。

有资质的人员是指掌握与电气设备的制造和操作及其安装相关的技能和知识的人员，他们经过安全培训能够发现和避免相关的危险。

关于本书

概览

文档范围

本用户手册旨在介绍如何使用 Modbus 的通信设备类型管理器 (Comm DTM)。

有效性说明

本文档已使用 Modbus Communication Library V2.5 版本更新。

关于产品的资讯

⚠ 警告

失去控制

- 任何控制方案的设计者都必须考虑到控制路径可能出现故障的情况，并为某些关键控制功能提供一种方法，使其在出现路径故障时以及出现路径故障后恢复至安全状态。这些关键控制功能包括紧急停止、越程停止、断电重启以及类似的安全措施。
- 对于关键控制功能，必须提供单独或冗余的控制路径。
- 系统控制路径可包括通讯链路。必须对暗含的无法预料的传输延迟或链路失效问题加以考虑。
- 遵守所有事故预防规定和当地的安全指南。[1]
- 为了保证正确运行，在投入使用前，必须对设备的每次执行情况分别进行全面测试。

不遵循上述说明可能导致人员伤亡或设备损坏。

[1] 有关详细信息，请参阅 NEMA ICS 1.1（最新版）中的“安全指导原则 - 固态控制器的应用、安装和维护”以及 NEMA ICS 7.1（最新版）中的“结构安全标准及可调速驱动系统的选择、安装与操作指南”或您特定地区的类似规定。

第1章
硬件和软件要求

本章包含了哪些内容？

本章包含了以下主题：

系统要求

硬件要求

要求	最小值	建议
计算机	Pentium 4 或同等处理器	
RAM	1 GB	2 GB
系统驱动器上的可用硬盘空间	100 MB	
安装驱动器上的可用硬盘空间	100 MB	
交换文件	1024 MB	2048 MB
监视器显示	256 色 SVGA 800 x 600 分辨率	真彩色 XGA 1024 x 768 分辨率

软件要求

软件操作系统

操作系统	版本/服务包	特别注意事项
Windows 7 32 位	SP1	安装 Modbus SL 通讯 DTM 需要管理员访问权限
Windows 7 64 位	SP1	
Windows 8.1, 10 Professional	–	

PC 上安装的软件

软件	版本	特别注意事项
Microsoft.NET Framework	V2.0 SP2	–
FDT 帧应用程序	FDT 1.2 或 FDT 1.2.1	Modbus SL Comm DTM 需要符合 FDT 标准的 FDT 帧应用程序。FDT 帧应用程序必须支持 Microsoft.NET Framework 2.0。
Schneider Modbus serial PC 驱动程序	有关 Schneider Modbus serial PC 驱动程序版本的信息，请参阅 Schneider Electric Modbus 通讯库的 *发行说明*文件。	–

兼容性

FDT 兼容性

Modbus Comm DTM 符合 FDT 标准 FDT 1.2 和 FDT 1.2.1。它基于 FDT Modbus Annex 1.0。

Modbus 兼容性

Modbus Comm DTM 支持在 Modbus 应用协议规范 V1.1b 中指定的 Modbus 服务。

注意事项

Modbus 连接

最大 Modbus 并发连接数为 4。 缺省情况下，安装 Modbus 驱动程序后，会创建 Modbus 连接。

如果需要更多连接，请执行以下步骤：

- 打开 Windows **控制面板**。
- 双击**驱动程序管理器**图标。
- 打开 **Modbus Serial 驱动程序**选项卡
- 配置并启动 Modbus Serial PC 驱动程序的所有 4 个实例。
- 检查是否所有实例都在运行（系统托盘中存在 4 个 Modbus Serial 驱动程序图标）。

注意： 要执行这些步骤，需要管理员访问权限。

安装和删除

安装

双击 *setup.exe* 文件，然后按照安装向导中的说明操作。

删除

要删除您的计算机上的 DTM，请选择**开始 → 设置 → 控制面板 → 添加/删除程序**。

第2章
连接类型和通讯模型

简介

本章概述不同的配置，这些配置可用于建立 Modbus 通讯。

本章包含了哪些内容？

本章包含了以下主题：

连接类型

简介

Modbus SL 通讯 DTM 可用于建立基于不同连接类型的 Modbus 通讯。

串行连接

Modbus SL 通讯 DTM 可用于通过标准 PC 串行端口建立 Modbus 通讯。

USB/RS232、USB/RS485 转换器连接

Modbus SL 通讯 DTM 可用于通过 USB/RS232 或 USB/RS485 转换器建立 Modbus 通讯。

注意： Modbus SL 通讯 DTM 仅支持 USB 转换器，该转换器可作为虚拟 COM 端口进行访问。

USB 连接

Modbus SL 通讯 DTM 可用于通过下列电缆建立 Modbus 通讯：

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

直接 USB 连接

Modbus SL 通讯 DTM 允许通过 USB 建立直接连接。仅特定 Schneider Electric 设备支持这种连接类型，例如通过使用 Altivar 61 和 71 可变速度驱动的 ATV-IMC 集成控制器卡。

要建立直接 USB 连接，可执行以下步骤：

步骤	操作
1	在 DTM GUI 中选择**配置**选项卡。
2	启用复选框 **使用以下网关 TCP/IP 地址。**
3	输入 IP 地址 **90.0.0.1**

步骤	操作
4	单击 **确定**或**应用**以验证输入。  现在即可通过把对应的设备 DTM 切换到在线模式来建立与目标设备的通讯。

网关连接

Modbus SL 通讯 DTM 可以用于建立到 Modbus 串行设备（位于 Modbus TCP/Modbus 串行网关后面）的 Modbus 通讯。在这种情况下，连接通过 PC 的以太网网络适配器建立。

蓝牙连接

Modbus SL 通讯 DTM 可用于通过蓝牙建立 Modbus 通讯。

注意： Modbus SL 通讯 DTM 仅支持执行蓝牙串行端口配置文件 (SPP) 的蓝牙适配器。

通讯模型

简介

本章介绍 Modbus SL 通讯 DTM 支持的不同通讯模型。

注意： FDT 技术并非开发用于实时数据传输。根据您采用的系统和通讯模块，数据可能不会反映实际的实时设备状态。

⚠ 警告

无效设备状态信息

由于传输的数据可能无法反映实际的设备状态，因此请勿将 Modbus Comm DTM 用于时间紧要的控制或监控任务。FDT 技术不适用于此用途。

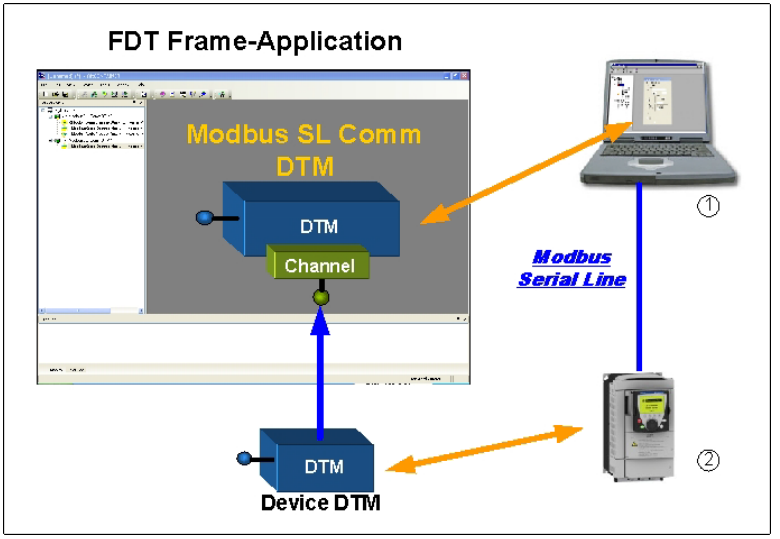
不遵循上述说明可能导致人员伤亡或设备损坏。

直接连接

Modbus SL 通讯 DTM 可以用于在 PC 与目标设备之间建立直接 Modbus 通讯。

对于直接连接，支持以下物理连接类型：

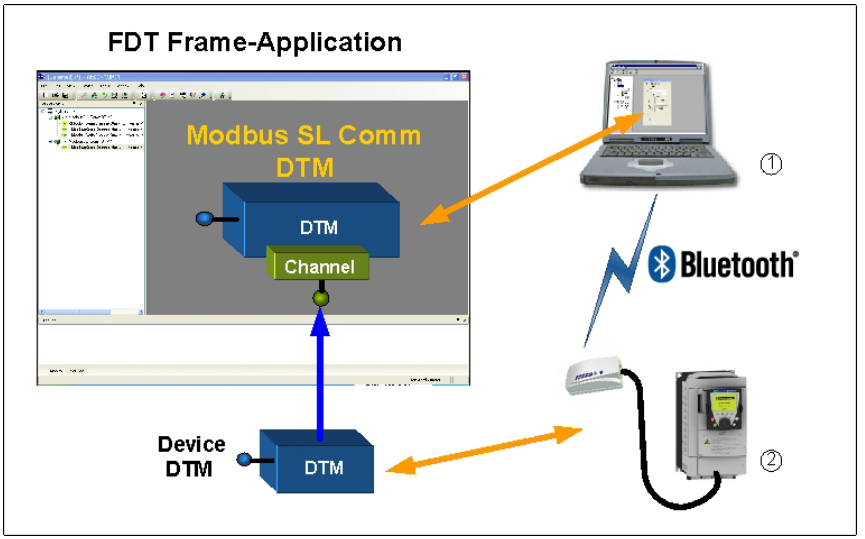
- RS-232
- RS-485，通过使用 RS232/RS485 转换器
- USB，通过使用 USB/串行线路转换器
- USB，通过使用直接 USB 电缆（参见硬件手册了解正确的电缆参考号）



1 安装了 Modbus SL 通讯 DTM 的 PC
2 目标设备

蓝牙连接

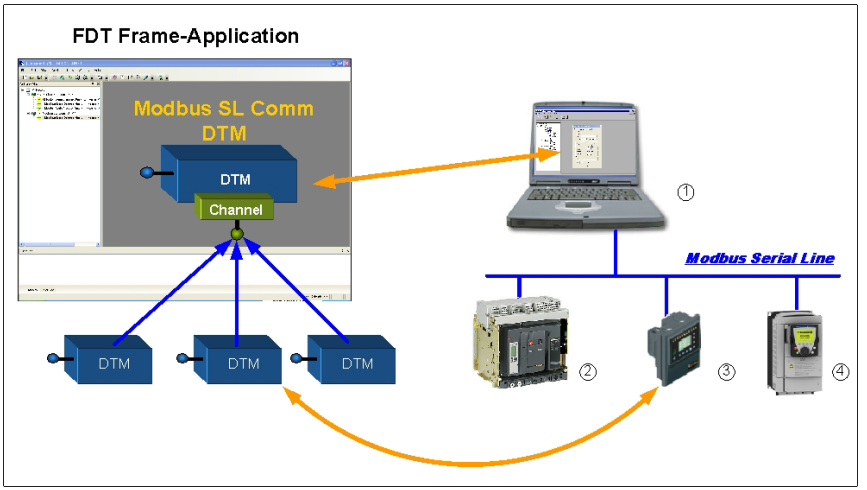
Modbus SL 通讯 DTM 可以用于通过蓝牙在 PC 与目标设备之间建立直接 Modbus 通讯。



1 安装了 Modbus 串行通讯 DTM 的 PC
2 目标设备

总线连接

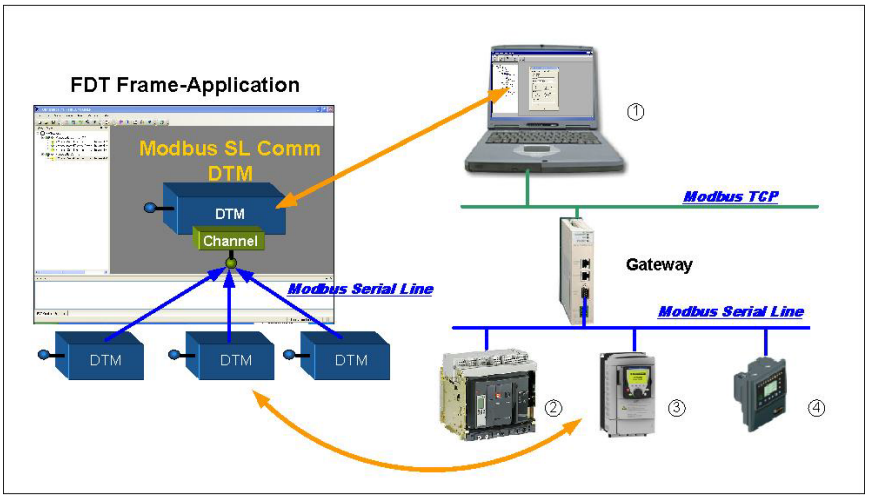
Modbus SL 通讯 DTM 可以与 RS232/RS485 转换器一起使用，以建立到 Modbus 串行线路总线的 Modbus 通讯。



1 安装了 Modbus SL 通讯 DTM 的 PC
2-4 目标设备

网关连接

Modbus SL 通讯 DTM 可以用于建立到 Modbus 串行设备（位于 Modbus TCP/Modbus 串行线路网关后面）的 Modbus 通讯。



1 安装了 Modbus SL 通讯 DTM 的 PC
2-4 目标设备

第3章
图形用户界面

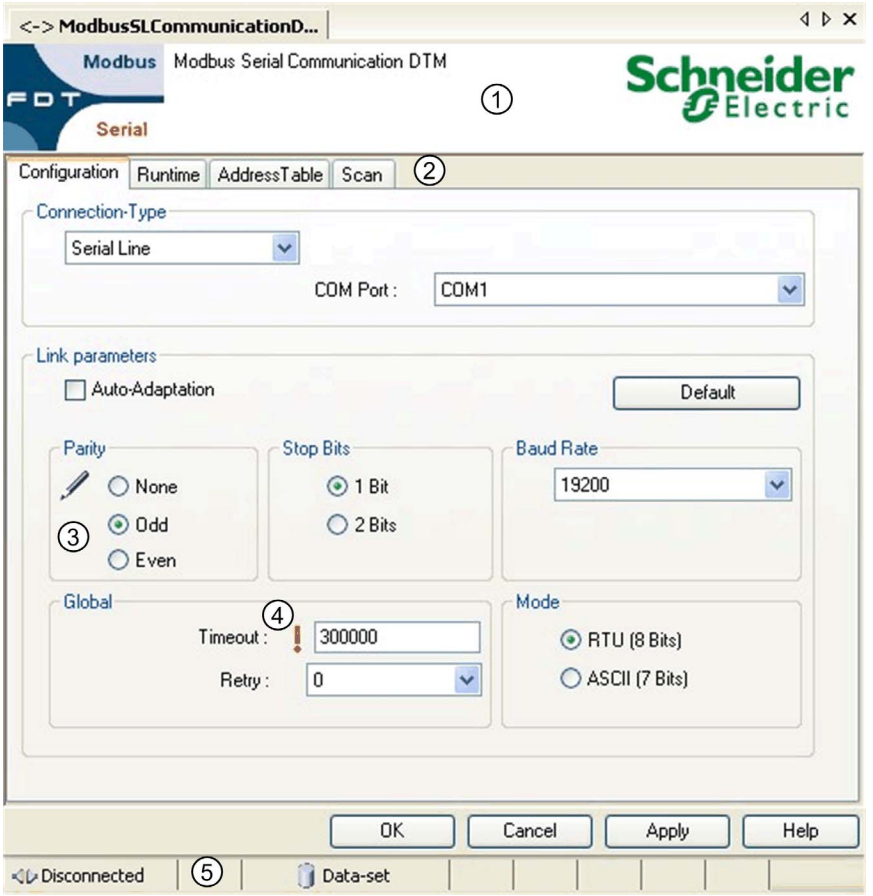
图形用户界面

概述

本章介绍 Modbus SL Comm DTM 的图形用户界面 (GUI)。

简介

下图显示 DTM 的 GUI（图形用户界面）。



1 标识区域
2 选项卡菜单
3-4 参数状态图标
5 状态栏

标识区域

标识区域显示 DTM 的名称和版本。

选项卡菜单

使用选项卡菜单可访问 DTM 提供的不同功能。

参数状态图标

参数状态图标提供有关参数的当前状态的信息。

可能的参数状态

图标	含义
	参数已修改，且具有无效值。
	参数已修改，且具有有效值

状态栏

状态栏提供有关 DTM 的当前状态的信息。

可能的连接状态

图标	文本	含义	DTM 状态
	正在连接	正在连接	进入在线模式
	已连接	已连接	在线
	正在断开连接	正在断开连接	进入离线模式
	已中断	已中断	检测到通讯中断
	已断开	已断开	所有其他状态

可能的数据源状态

图标	文本	行为
	数据集	显示的值加载自实例数据集。只有实例数据集中的更改值会受到影响。
	数据集已锁定	显示的值加载自实例数据集。数据集已锁定。

第4章
配置

本章包含了哪些内容？

本章包含了以下主题：

配置选项卡

简介

Modbus SL 通讯 DTM 的**配置**选项卡包含用于不同连接类型的通讯参数。

配置选项卡

您可以通过多种方式访问 Modbus Serial Comm DTM 的**配置**选项卡：

- 在 FDT 帧应用程序的网络视图中，双击 Modbus SL 通讯 DTM 图标。
- 在 FDT 帧应用程序的网络视图中，右键单击 Modbus SL 通讯 DTM 图标，然后单击**配置**。

下图显示 Modbus SL 通讯 DTM 对话框的**配置**选项卡：

连接类型

在 Modbus SL 通讯 DTM 的**配置**选项卡上的**连接类型**列表中，可以选择 Modbus 通讯的连接类型。

下表包含可供选择的连接类型的列表：

连接类型	说明
串行线路	应针对以下连接选择此连接类型： ● RS-232 ● RS-485 ● USB 到 RS-232 转换器 ● USB 到 RS-485 转换器
远程网关	对于与 Modbus TCP/Modbus SL 网关后面的串行设备的 Modbus 通讯，请选择此连接类型。
蓝牙	如果应通过蓝牙建立到目标设备的通讯，请选择此连接类型。
USB	如果您要进行直接 USB 连接，请选择此种连接类型。

按钮

下表介绍**配置**选项卡中提供的按钮。

命令	说明
确定	将保存所有参数，并关闭 Modbus SL 通讯 DTM 窗口。在下一次连接时将应用新参数值。
取消	取消所有参数修改，并关闭 Modbus SL 通讯 DTM 窗口。在下一次连接时将应用原始值。
缺省	显示缺省参数值。
应用	保存参数，但是 Modbus SL 通讯 DTM 窗口仍处于打开状态。在下一次连接时将应用新参数值。

串行配置

简介

本章介绍用于 RS232/RS485 连接的参数。

串行参数

下表介绍串行线路连接的通讯参数。

参数	说明	缺省值
自适应	启用/禁用自适应功能，该功能可以用于自动检测 Modbus 串行线路的通讯参数。	已禁用
COM 端口	PC COM 端口	COM1
波特率 (Bit/s)	串行线路波特率	19200
校验位	串行线路校验位	偶
停止位	停止位的数目	1
超时	Modbus 从站响应超时	3000 毫秒
重试	出现通讯超时时，Modbus Comm DTM 在串行连接上重新发送 Modbus 请求的次数	0
模式	传输模式： ● RTU（8 位） ● ASCII（7 位）	RTU

Modbus SL 通讯 DTM 的蓝牙配置

简介

本章介绍蓝牙连接的 Modbus SL 通讯 DTM 配置

蓝牙配置

下表介绍蓝牙连接的参数。

参数	说明
蓝牙	此组合框包含找到的虚拟 COM 端口（这些端口由 PC 上安装的蓝牙适配器提供）的列表。选择用于建立 Modbus 通讯的 COM 端口。 **注：**如果无法选择所需的 COM 端口，请尝试通过下面的配置建立连接： ● 将**连接类型**设置为串行线路 ● 在组合框中选择所需 COM 端口
全局超时	Modbus 从站响应超时
重试次数	出现通讯超时时，Modbus SL 通讯 DTM 在蓝牙连接上重新发送 Modbus 请求的次数。

Modbus SL 通讯 DTM 的远程网关配置

简介

本章介绍用于远程网关连接的 Modbus SL 通讯 DTM 配置。

远程网关配置

下表介绍远程网关连接的参数。

参数	说明
远程网关	在其后面放置目标设备的 Modbus SL 通讯 DTM 网关 IP 地址
全局超时	Modbus 从站响应超时
重试次数	出现通讯超时时，Modbus SL 通讯 DTM 重新发送 Modbus 请求的次数。

Modbus SL 通讯 DTM 的 USB 连接配置

简介

本章介绍用于直接 USB 连接的 Modbus SL 通讯 DTM 的配置。

USB 连接配置

下表介绍 USB 连接的参数。

参数	说明
全局超时	Modbus 从站响应超时
重试次数	出现通讯超时时，Modbus SL 通讯 DTM 重新发送 Modbus 请求的次数。

运行时选项卡

简介

Modbus SL 通讯 DTM提供不同类型的运行时信息。本章介绍 Modbus SL 通讯 DTM 提供的信息以及日志功能的配置。

运行时选项卡

Modbus SL 通讯 DTM 提供不同类型的运行时信息，可以用于监控建立的通讯。

运行时信息位于 Modbus SL 通讯 DTM 的**运行时**选项卡上，可以通过以下方式访问该选项卡：

- 在 FDT 帧应用程序的网络视图中，双击 Modbus SL 通讯 DTM 图标。现在选择**运行时**选项卡。
- 在 FDT 帧应用程序的网络视图中，右键单击 Modbus SL 通讯 DTM 图标，然后单击**配置**。现在选择**运行时**选项卡。

下图显示 Modbus SL 通讯 DTM 对话框的**运行时**选项卡：

配置命令

表格介绍**运行时**选项卡中提供的配置命令。

命令	描述
确定	将保存这些参数，并关闭 Modbus SL 通讯 DTM 窗口。在下一次连接时将应用新参数值。
取消	取消参数修改，并关闭 Modbus SL 通讯 DTM 窗口。在下一次连接时将应用原始值。
浏览	打开文件浏览器以指定日志文件路径
复位	将所有运行时参数复位为零

命令	描述
应用	保存参数，但是 Modbus SL 通讯 DTM 窗口仍处于打开状态。在下一次连接时将应用新参数值。

运行时参数

表格介绍 Modbus SL 通讯 DTM 的**运行时**选项卡中提供的运行时参数：

命令	描述
连接	到 Modbus SL 通讯 DTM 的活动连接数。
发送的消息数	Modbus SL 通讯 DTM 已发送的消息数。
接收的消息数	Modbus SL 通讯 DTM 已接收的消息数。
异常	Modbus SL 通讯 DTM 已接收的 Modbus 异常消息数。
超时数	接收时检测到的超时错误数。

日志文件

Modbus SL 通讯 DTM 可以用于创建日志文件。在**日志文件**框中，必须指定用于存储日志文件的路径。

表格介绍将写入日志文件的信息，具体取决于所选择的**日志模式**：

日志模式	描述
已停用	禁用日志文件功能。
错误日志	日志文件中只写入有关已检测到的超时错误和已接收到的 Modbus 异常的信息。
全部日志	除有关已检测到的超时错误和已接收到的 Modbus 异常的信息外，日志文件中还将写入有关已发送的 Modbus 请求、已收到的 Modbus 响应以及从设备 DTM 收到的请求的信息。

改善网络安全的建议

日志文件通常包含敏感数据，例如

- 设备地址
- 设备名称
- 网络拓扑详细信息
- 网络配置详细信息

这些数据存储在您 PC 的硬盘上。如果不再需要日志文件，请尽快删除，或者将其存放在安全位置，仅允许经过授权的访问。

地址表

简介

Modbus Comm DTM 提供一个地址表，该表列出已连接的设备 DTM 及其目标地址。本章介绍地址表中提供的信息以及设备目标地址的配置。

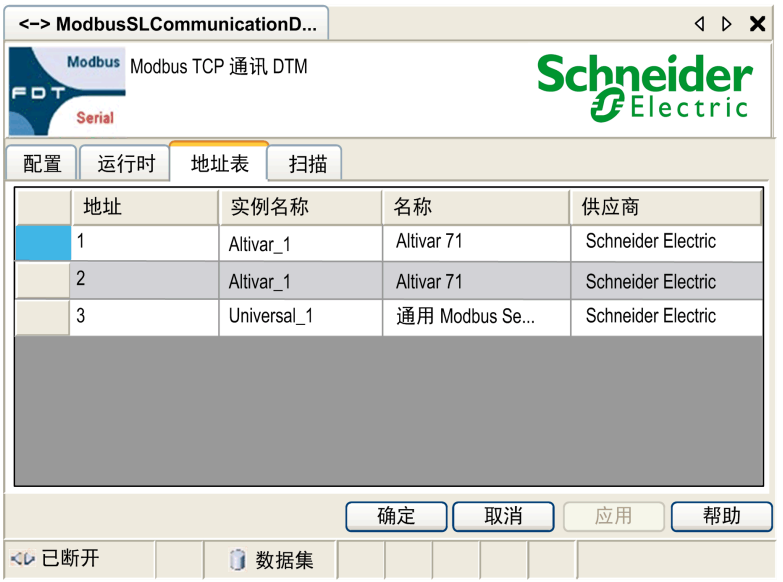
地址表

Modbus SL Comm DTM 提供一个地址表，该表列出已连接的设备 DTM 及其目标地址。在此地址表中，可以指定已连接设备 DTM 的目标地址。

可以通过以下方式访问**地址表**选项卡：

- 在 FDT 帧应用程序的网络视图中，双击 Modbus SL Comm DTM 图标。现在选择**地址表**选项卡。
- 在 FDT 帧应用程序的**网络视图**中，右键单击 Modbus SL Comm DTM 图标，然后单击**配置**。现在选择**地址表**选项卡。

下图显示 Modbus SL Comm DTM 对话框的**地址表**选项卡：



配置命令

下表介绍**地址表**选项卡中提供的配置命令

命令	说明
确定	保存修改，并关闭 Modbus SL Comm DTM 窗口。在下一次连接时将应用新值。
取消	取消修改并关闭 Modbus SL Comm DTM 窗口。在下一次连接时将应用原始值。
应用	保存修改，但 Modbus SL Comm DTM 窗口保持打开状态。在下一次连接时将应用新值。

地址信息

下表介绍 Modbus SL Comm DTM 的**地址表**选项卡中提供的地址信息：

参数	说明
地址	硬件设备的目标地址，应通过已连接的 DTM 进行配置
实例名称	DTM 的实例名称
名称	DTM 特定名称
供应商	DTM 供应商名称

地址分配

Modbus SL Comm DTM 的地址表可以用于指定硬件设备的目标地址，该地址应通过特定 DTM 进行配置。要指定目标地址，必须在 DTM 的相应**地址**字段中输入新地址，然后通过单击**应用**按钮或单击**确定**按钮来验证此修改。

⚠ 警告

MODBUS SL 的意外设备操作

请勿在连接有多个 Modbus 设备的总线上与具有地址 248 的设备进行通讯。

只使用地址 248 建立与某一设备的点对点连接；也就是，在 PC 与设备之间直接进行连接。

不遵循上述说明可能导致人员伤亡或设备损坏。

扫描配置

简介

Modbus Comm DTM 可用于为 FDT 扫描指定扫描地址的范围。本章介绍用于 FDT 扫描的扫描参数配置。

扫描选项卡

Modbus SL Comm DTM 支持扫描功能，正如在 FDT 规格 V1.2.1 中所定义的。该扫描功能可以用于自动生成底层通讯网络的网络拓扑。Modbus SL Comm DTM 可以用于指定扫描地址的范围。

扫描参数位于 Modbus SL Comm DTM 的**扫描**选项卡上，可以通过以下方式访问该选项卡：

- 在 FDT 帧应用程序的**网络视图**中，双击 Modbus SL Comm DTM 图标。现在选择**扫描**选项卡。
- 在 FDT 帧应用程序的**网络视图**中，右键单击 Modbus SL Comm DTM 图标，然后单击**配置**。现在选择**扫描**选项卡。

下图显示 Modbus SL 通讯 DTM 对话框的**扫描**选项卡：

配置命令

下表介绍**扫描**选项卡中提供的配置命令：

命令	说明
确定	保存修改，并关闭 Modbus Comm DTM 窗口。在下一次扫描时将应用新值。
取消	取消修改，并关闭 Modbus Comm DTM 窗口。在下一次扫描时将应用原始值。
应用	保存修改，但 Modbus Comm DTM 窗口仍保持打开状态。在下一次扫描时将应用新值。

Modbus SL 的扫描参数

下表介绍 Modbus SL 通讯 DTM 的**扫描**选项卡中提供的扫描参数：

命令	说明	
扫描模式	**扫描模式**：	
	单点	此连接类型仅适用于直接连接，其中的目标设备直接连接到 PC（扫描的地址范围： 248）。
	多点	此连接类型仅适用于多点连接，其中的 PC 连接到 Modbus 串行线路网络。
扫描地址范围	**扫描地址范围**：	
	单个	仅扫描一个目标设备的单个地址，范围介于 1-247 之间。
	范围	扫描介于 1-247 之间的指定地址范围。
	所有	扫描 Modbus 串行连接的整个地址范围（介于 1-247 之间的所有地址）。

⚠ 警告

意外的设备操作

请勿在 Modbus 多点网络上使用“单点”扫描模式。

仅对点对点通讯使用“单点”扫描模式 ；也就是，在 PC 与设备之间直接进行通讯。

不遵循上述说明可能导致人员伤亡或设备损坏。

第5章
网络安全

简介

网络安全是一种网络管理分支，用于应对在计算机系统上或由计算机系统发起的攻击，这些攻击会通过网络执行，可以导致意外或故意的破坏。网络安全的目的是对信息和有形资产提供增强的保护，从而在维护目标用户的访问权限时防止被盗、被破坏、不当使用或出现意外事故。

单一的网络安全方法往往难以满足需求。Schneider Electric 建议采用深度防御方法。本方法由 National Security Agency (NSA) 提出，将网络分为安全功能、设备和流程三层。此方法的基本组成部分包括：

- 风险评估
- 基于风险评估结果而建立的安全计划
- 多阶段培训活动
- 使用控制区 (DMZ) 将工业网络从企业网络中进行物理分离，并使用防火墙和路由建立其他安全区域
- 系统访问控制
- 设备加强
- 网络监控和维护

本章定义有助于您配置不易受到网络攻击影响的系统的要素。有关深度防御方法的详细信息，请参阅 *TVDA：在 Schneider Electric website 上的控制室中如何减少网络攻击漏洞*。

本章包含了哪些内容？

本章包含了以下主题：

何为网络安全？

简介

网络威胁是指可破坏计算机系统和网络正常操作的蓄意行为或意外行为。这些行为可在物理设施内或从外部位置发起。控制环境的安全挑战包括：

- 各种物理和逻辑界限
- 多个站点和较大的地理范围
- 对流程可用性安全实施的负面影响
- 随着业务控制的通讯越来越开放，从业务系统到控制系统的迁移越来越容易接触蠕虫和病毒
- 通过 USB 设备、供应商和服务专员的笔记本电脑以及企业网络越来越多地接触恶意软件
- 控制系统对物理和机械系统的直接影响

网络攻击的来源

实施考虑网络攻击和意外的各种潜在来源的网络安全计划，包括：

来源	描述
内部	● 员工或合同工的行为不当 ● 员工或合同工不满
外部机会（非指引）	● 脚本小子* ● 消遣型黑客 ● 病毒编写人员
外部故意（受引导）	● 犯罪团体 ● 积极分子 ● 恐怖分子 ● 外国机构
意外	
*黑客的俗称，他们使用他人编写的恶意脚本，而不必全面理解脚本的运行方式及其对系统的潜在影响	

可能启动对控制系统的蓄意网络攻击，以实现大量的恶意结果，包括：

- 通过阻止或延迟信息流来破坏生产流程
- 损坏、禁用或关闭设备，对生产或设备产生负面影响
- 修改或禁用安全系统，导致刻意的损坏

攻击者如何获得访问权限

网络攻击者绕过周边防御，可获得对控制系统网络的访问权限。访问的共同点包括：

- 拨号接入远程终端 (RTU) 设备
- 供应商访问点（如技术支持访问点）
- IT 控制的网络产品
- 公司虚拟专用网络 (VPN)
- 数据库链接

- 防火墙配置不佳
- 对等实用工具

网络安全认证

Schneider Electric 基于以下建议制定网络安全指南：

- Achilles
- ISA Secure

是否有疑问？

要提交网络安全疑问，报告安全问题，或从 Schneider Electric 获取最新新闻，请访问我们的 *website*。

Schneider Electric 指南

简介

您的 PC 系统可运行各种应用程序来增强您的控制环境中的安全性。系统具有出厂默认设置，要求重新配置以与 Schneider Electric 的深度防御方法的设备加强建议保持一致。

下面的指南介绍了 Windows 7 操作系统中的流程。这些仅作为示例提供。您的操作系统和应用程序可能有不同的要求或流程。

禁用未使用的网络接口卡

验证是否禁用应用程序不需要的网络接口卡。例如，如果您的系统有 2 个网络卡，且应用程序只使用一个，则验证是否禁用另一个网络卡（本地连接 2）。

在 Windows 7 中禁用网络卡：

步骤	操作
1	打开**控制面板 → 网络和 Internet → 网络和共享中心 → 更改适配器设置**。
2	右键单击未使用的连接。选择**禁用**。

配置本地连接

各种 Windows 网络设置可增强与 Schneider Electric 建议的深度防御方法一致的安全性。

在 Windows 7 系统中，通过打开**控制面板 → 网络和 Internet → 网络和共享中心 → 更改适配器设置 → 本地连接 (x)** 来访问这些设设置。

以下列表是您可能在**本地连接属性**屏幕上对系统进行的配置更改的示例：

- 禁用各个网络卡上的所有 IPv6 堆栈。（本系统示例不要求 IPv6 地址范围，禁用 IPv6 堆栈可限制导致 IPv6 潜在安全风险的漏洞。
- 禁用**Microsoft 网络的文件和打印机共享**。

Schneider Electric 的深度防御建议还包括以下内容：

- 仅定义静态 IPv4 地址、子网掩码和网关。
- 在控制室内不要使用 DHCP 或 DNS。

管理 Windows 防火墙

Schneider Electric 的深度防御方法建议包括启用所有系统 PC 上的 Windows 主机防火墙。启用列出的任何公共或专用配置文件的防火墙。

建议的做法是用户定义防火墙，拒绝连接到未知/不受信任的外部主机或拒绝来自这类主机的连接。

禁用远程桌面协议

Schneider Electric 的深度防御方法建议包括禁用远程桌面协议 (RDP)，除非您的应用程序要求 RDP。以下步骤介绍了如何禁用该协议：

步骤	操作
1	在 Windows 2008 R2 或 Windows 7 中，可通过**计算机 → 系统属性 → 高级系统设置**禁用 RDP。
2	在**远程**选项卡上，取消选中**允许远程协助连接这台计算机**复选框。
3	选择**不允许连接这台计算机**复选框。

更新安全策略

通过命令窗口中的 gpupdate 更新您系统中与 PC 相关的安全策略。有关详细信息，请参考与 Microsoft 相关的 gpupdate 文档。

禁用 LANMAN 和 NTLM

Microsoft LAN Manager 协议（LANMAN 或 LM）及其后续 NT LAN Manager (NTLM) 具有使其在控制应用程序中的使用不合适的漏洞。

以下步骤介绍了如何在 Windows 7 或 Windows 2008 R2 中禁用 LM 和 NTLM：

步骤	操作
1	在命令窗口中，执行 secpol.msc 以打开**本地安全策略**窗口。
2	打开**安全设置 → 本地策略 → 安全选项**。
3	选择**仅发送 NTLMv2 响应。在**网络安全：LAN 管理器身份验证级别**字段中拒绝 LM & NTLM**。
4	选择**网络安全：不要在下次更改密码时存储 LAN Manager 的哈希值**复选框。
5	在命令窗口中，输入 gpupdate 以提交更改的安全策略。

管理更新

部署前，使用 Microsoft **Windows 更新** Web 页面上的实用程序更新所有 PC 的操作系统。要在 Windows 2008R2、Windows 7 或 Windows XP 中访问此工具，请选择**开始 → 所有程序 → Windows 更新**。

术语

主站/从站模型

在实现主站/从站模型的网络中，控制方向为从主站到从站设备。

以太网

用于连接有限区域（如一座建筑）内设备的局域网接线和信令规范。以太网采用总线或星形拓扑结构来连接网络上的不同节点。

功能代码

功能代码是一个指令集，用于命令指定地址处的一个或多个从站设备执行某种类型的操作，例如读取一组数据寄存器并通过内容进行响应。

接口

接口表示对于网络的物理连接，例如网络卡或 USB 到 RS 232 转换器。

电报

在串行通讯中使用的数据包。

网关

在网络之间传递数据的程序或硬件

配置

一个系统内硬件组件的布局和互连以及硬件和软件的选择，可决定系统的运行特性。

CRC

循环冗余校验

实现此错误校验机制的消息具有一个 CRC 字段，该字段由发射器根据消息的内容进行计算。接收节点会重新计算该字段。如果 2 个代码不一致，则表示传输的消息与接收到的消息之间存在差异。

DTM

DTM（设备类型管理器）是一种设备驱动程序，由现场设备供应商提供。DTM 包含设备特定信息，并提供图形用户界面。DTM 可以用于对特定设备执行监控任务和配置任务。DTM 不是独立的应用程序。需要 FDT 帧应用程序才能运行。

FDT

FDT（现场设备工具）技术对现场设备与系统之间的通讯接口进行标准化 (*www.fdtgroup.org*)。

IP

因特网协议。

TCP/IP 协议系列中用于跟踪节点的因特网地址、对传出消息进行路由并识别传入消息的协议。

LAN

局域网。

短距离数据通讯网络。

MB

Modbus 的缩写

Modbus

Modbus 是一种应用层消息传递协议。Modbus 可提供多种用功能代码指定的服务。

SL

串行线路的缩写

TCP

传输控制协议。

一种面向连接的传输层协议，它提供可靠的全双工数据传输。TCP 属于 TCP/IP 协议组。

索引