SIEMENS

SIMATIC Ident

RFID 系统
SIMATIC RF300 系统的组态和参数分配

配置手册

05/2023
C79000-G8952-C695-01

法律资讯

警告提示系统

为了您的人身安全以及避免财产损失，必须注意本手册中的提示。人身安全的提示用一个警告三角表示，仅与财产损失有关的提示不带警告三角。警告提示根据危险等级由高到低如下表示。

⚠ 危险
表示如果不采取相应的小心措施，**将会**导致死亡或者严重的人身伤害。

⚠ 警告
表示如果不采取相应的小心措施，**可能**导致死亡或者严重的人身伤害。

⚠ 小心
表示如果不采取相应的小心措施，可能导致轻微的人身伤害。

注意
表示如果不采取相应的小心措施，可能导致财产损失。

当出现多个危险等级的情况下，每次总是使用最高等级的警告提示。如果在某个警告提示中带有警告可能导致人身伤害的警告三角，则可能在该警告提示中另外还附带有可能导致财产损失的警告。

合格的专业人员

本文件所属的产品/系统只允许由符合各项工作要求的**合格人员**进行操作。其操作必须遵照各自附带的文件说明，特别是其中的安全及警告提示。 由于具备相关培训及经验，合格人员可以察觉本产品/系统的风险，并避免可能的危险。

按规定使用 Siemens 产品

请注意下列说明：

⚠ 警告
Siemens 产品只允许用于目录和相关技术文件中规定的使用情况。如果要使用其他公司的产品和组件，必须得到 Siemens 推荐和允许。正确的运输、储存、组装、装配、安装、调试、操作和维护是产品安全、正常运行的前提。必须保证允许的环境条件。必须注意相关文件中的提示。

商标

所有带有标记符号 ® 的都是 Siemens AG 的注册商标。本印刷品中的其他符号可能是一些其他商标。若第三方出于自身目的使用这些商标，将侵害其所有者的权利。

责任免除

我们已对印刷品中所述内容与硬件和软件的一致性作过检查。然而不排除存在偏差的可能性，因此我们不保证印刷品中所述内容与硬件和软件完全一致。印刷品中的数据都按规定经过检测，必要的修正值包含在下一版本中。

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
德国

C79000-G8952-C695-01
Ⓟ 04/2023 本公司保留更改的权利

Copyright © Siemens AG 2023.
保留所有权利

目录

简介

1

组态手册的用途

本手册提供有关 SIMATIC RF300 系统参数分配的信息。

本手册适合以下人员使用：

- 调试工程师
- 组态工程师
- 程序员
- 服务技术人员

手册主题

本手册涵盖以下与 SIMATIC RF300 系统参数分配各方面相关的主题。

- RF300 系统的输入参数
  用于对通过通信模块操作的 RF300 阅读器进行编程的参数。
- RF300 系统的 P2P 模式
  两个 RF300 阅读器之间的直接对等通信。
- ISO 隧道
  通过 RF300 阅读器将任何 ISO 命令从控制器传送到发送应答器，而无需由阅读器解析

所需的基本知识

本组态手册假定读者已具有自动化工程和识别系统的一般知识。

本文档适用范围

本文档适用于“SIMATIC RF300”系统手册（2022 年 11 月版）中介绍的已供货的所有 SIMATIC RF300 型号（Scanmode 型号除外）。

商标

以下商标以及可能未由注册商标符号 ® 标记的其它名称均为 Siemens AG 的注册商标：

SIMATIC ®、SIMATIC RF ® 和 MOBY ®

文档中的定位

有关 SIMATIC RF300 系统的信息，请参见《SIMATIC RF300 (https://support.industry.siemens.com/cs/ww/en/ps/15003/man)》系统手册。

输入参数

2

本部分是对以下所列手册内容的增补，用于补充新的 RF300 功能的使用信息：

- 功能手册《Ident 配置文件和 Ident 块》
- 功能手册《用于 MOBY U、MOBY D、RF200、RF300 的 FB 45》
- 《RF182C 通信模块》操作说明
- 《带 FC 44 的 RF160C 通信模块》操作说明
- 《SIMATIC RF120C》操作说明

说明

STEP 7 (TIA Portal) 中 RF120C 的组态

请注意，对于通信模块 RF120C，可在 TIA Portal 中基于工艺对象"SIMATIC Ident > TO_Ident"或通过通信模块 "属性"(Properties) 选项卡中的参数（"Ident 设备/系统 > 通过 FB 分配的参数/光学阅读器"(Ident device/system > Parameters via FB/optical readers)）进行组态。

- "SIMATIC RF185C、RF186C、RF188C、RF186CI、RF188CI"操作说明
- "SIMATIC RF166C"操作说明

2.1 说明

如果在 SIMATIC S7-1200 或 S7-1500 控制器上通过通信模块操作 RF300 阅读器，建议使用 "SIMATIC Ident > TO_Ident"工艺对象通过 STEP 7 (TIA Portal) 执行参数分配。可通过工艺对象快速、轻松地实现参数分配。但是，如果阅读器是通过第三方控制器操作的，或者需要特定的已定义设置，则可使用上述输入参数对阅读器执行参数分配。

如果为工艺对象使用 "阅读器参数分配 > 常规阅读器"(Reader parameterization > General reader) 设置，也需要输入参数。参数通过 Ident 配置文件和"WRITE_CONFIG"命令传送到阅读器。

下文介绍的参数包含在 TIA Portal STEP 7 V16 及更高版本中。

说明

使用 STEP 7 (TIA Portal) 进行参数分配时的限制。

请注意，某些参数（例如信号量方法）只能通过“复位参数的字节序列”激活。

要激活这些参数，必须选择“属性”(Properties) 选项卡中的“常规阅读器”(General reader) 参数（“组态 > 基本参数 > 阅读器参数分配”(Configuration > Basic parameters > Reader parameter assignment)）。然后，如下文所述，必须调整“阅读器参数”(Reader parameters) 中的字节值。

如果未通过控制器 (PROFINET) 操作 RF300 阅读器，还可以通过各通信模块（例如 RF18xC/RF18xCI、RF166C）的 WBM 执行参数分配。

2.2 常规说明

第 1 代阅读器的注意事项

可以为部件编号为“6GT2801-xABxx”的阅读器分配参数，从而与兼容 RF300 或 ISO 15693 的发送应答器配合使用。

第 2 代阅读器的注意事项

部件编号为“6GT2801-xBAxx”的阅读器也可与 ISO 14443 发送应答器（MIFARE Classic，MOBY E）进行通信。除此之外，也可在参数中设置“常规模式”(General mode)。借助此模式，无需选择特定空中接口协议（RF300、ISO 15693、ISO 14443）即可处理所有发送应答器类型。如果仅使用一个或两个发送应答器类型，建议仅启用相关的空中接口协议，以缩短访问时间。

如需对混合操作编程（选择多个发送应答器类型，例如“常规模式”(General Mode)），请谨记各种发送应答器类型的存储器大小不同。如果发送应答器的存储容量不足以存储数据卷，则会生成错误消息。

通过第 2 代阅读器，带有参数“ATTRIBUTE = 0x83”（FB 45：Mode 03）的“变量状态”(Tag status)命令可用于所有类型（RF300、ISO 15693、ISO 14443 [MIFARE Classic，MOBY E]）的发送应答器。此外，借助分配适当参数的通信模块，还可通过 MOBY I 协议操作阅读器。MOBY I 协议仅支持用于 RF300 发送应答器，并可由阅读器自动识别。

阅读器固件 V1.7 的变更

阅读器固件 V1.7 修订了以下功能/参数：

- 针对 RF350R 的“RESET”命令
  在新的固件版本中，可以通过“RESET”命令指定天线类型。这些个别调整有助于提高阅读器（天线）和发送应答器之间通信的抗干扰能力。
- 可将任何密钥与 MIFARE Classic 发送应答器搭配使用
  在新的固件版本中，可以将任何密钥存储在阅读器上，取代永久集成的 MOBY E 密钥。这意味着，其他供应商的 MIFARE Classic 发送应答器也可以使用其各自的密钥进行处理。此外，新增“NC”模式，这样便可为 MIFARE Classic 发送应答器提供自己的密钥。
- 信号量方法
  在新的固件版本中，使用信号量方法增加了附加控制机制，以确保数据一致性。

有关密钥使用和信号量方法的说明，请参见“RF300 的输入参数”表。

地址分配的含义

凭借“Init”命令，地址信息具有下列含义：

- 完整“Init”：地址 = 0 或地址 = 发送应答器的存储器大小
  这意味着已对整个地址范围进行初始化。
- 部分“Init”：地址 ≠ 0
  这意味着初始化取决于指定地。
- 地址 > 发送应答器的存储器大小
  效果为不执行命令并生成错误消息。

2.3 RF300 的输入参数

下表列出了需要通过 Ident 配置文件、Ident 块和 FB 45 的功能块以及通信模块进行参数分配的输入参数借助应用程序块“Reset_RF300”、“Reset_Univ”，或通过“Ident_Profile/Advanced_Cmd”（或“init_run”和 FB 45），可使用“RESET”命令将这些参数从通信模块传送到阅读器中。

表格 2-1　RF300 的 Ident 配置文件或 Ident 块的输入参数

参数	说明
param （组态数据的字节 6）	“init_run”（RESET）命令可将所有输入参数传输至阅读器。使用 RF300 时，该位必须置为“True”。 关于 FB 45 的说明：如需在 MOBY I 模式下使用第 2 代 RF300 阅读器，该位须置为“False”。 关于 Ident_Profile 的说明：对于字节 6，存在两个有效值。 • 对于快速重置（MOBY I 模式），值为“0x05” • 对于慢速重置，值为“0x0A”。
scanning_time （组态数据的字节 9）	位 0...1：保留（将分配值“0”）。 位 2...4：调制深度 • 0：0%（默认值） • 1：7% • 2：10% • 3：15% • 4：20% • 5：25% • 6：30% • 7：100% 位 5...7：输入衰减 • 0：默认值（默认衰减存储在固件中，具体取决于阅读器类型和空中接口协议） • 1：0 dB • 2：5 dB • 3：10 dB • 4：15 dB • 7：-5 dB

参数	说明
param （组态数据的字节 10，位 0 ... 3）	以下值一般可用于 RF300： • 5：单标签模式 注：如需在 MOBY I 模式下操作第 2 代阅读器，必须将值置为"1"。
param （组态数据的字节 10，仅位 4）	此参数为发送应答器类型 RF300 和 ISO 14443（MIFARE Classic，MOBY E）启用 ECC 模式。 可能值： • 0：ECC 模式关闭。 • 1：ECC 模式开启。
Ident 块 TAG_CONTROL Ident 配置文件 param （组态数据的字节 10，位 5 ... 7）	该参数可打开或关闭阅读器上的存在性检查功能。 可能值： • 0：在不执行存在性检查的情况下运行 [1] 天线永久开启。 • 1：在执行存在性检查的情况下运行 天线永久开启。 • 2：在不执行存在性检查且采用信号量方法（RF300、ISO 14443 [MIFARE Classic]）的情况下运行 天线永久开启。 • 3：在执行存在性检查且采用信号量方法（RF300、ISO 14443 [MIFARE Classic]）的情况下运行 天线永久开启。 • 4：在不执行存在性检查的情况下运行 天线关闭。仅当发送以下命令之一时，才会开启天线：Read、Write、Init、Tag-Status • 6：在不执行存在性检查且采用信号量方法（RF300、ISO 14443 [MIFARE Classic]）的情况下运行 天线关闭。仅当发送以下命令之一时，才会开启天线：Read、Write、Init、Tag-Status
	[1] MOBY I 迁移时 LED 行为的说明： 在"不执行存在性检查"模式下，阅读器的 LED 保持为蓝色，直到初次访问（读取/写入/初始化）发送应答器时为止。在无其它访问或不执行命令时，LED 呈绿色闪烁。发送命令后，LED 呈绿色或橙色点亮，具体取决于发送应答器是否处于天线范围内。

<table>
<tr><th>参数</th><th colspan="2">说明</th></tr>
<tr><td rowspan="5">option_1
（组态数据的字节 11）</td><td colspan="2">允许使用以下值：</td></tr>
<tr><td>值</td><td>含义</td></tr>
<tr><td>0x00</td><td>只能通过切断阅读器电源来复位因发生故障而闪烁的 LED 指示灯。</td></tr>
<tr><td>0x01</td><td>成功执行某个命令后，会复位因发生故障而闪烁的 LED 指示灯。这只会影响通信错误（例如 FB 45：0x01、0x06/Ident 配置文件：0xE1FE0200、0xE2FE0100），不会复位其它错误。</td></tr>
<tr><td>0x02</td><td>因发生故障而闪烁的 LED 指示灯由“init_run”或“WRITE-CONFIG”（基于“Init”(RESET)）复位。</td></tr>
<tr><td>0x03</td><td>因发生故障而闪烁的 LED 指示灯由“init_run”或“WRITE-CONFIG”（基于“Init”(RESET)）复位，或者在成功执行命令后复位。</td></tr>
<tr><td rowspan="2">Ident 块:
RF_POWER
Ident 配置文件：
distance_limiting
（组态数据的字节 12）</td><td colspan="2">注：该参数预期供经培训的用户使用。Siemens 建议未经培训的用户使用默认值。
第 1 代阅读器：借助此参数，可更改第 1 代 (6GT2801-3AB10) RF380R 阅读器的发射功率（输出功率）。进行此操作时请注意，更改发射功率将影响限制范围（上/下操作距离）内的检测以及相邻 RF380R 之间应保持的最小距离。
超出指定范围的设置将设置默认值 (1.25 W)。此时，出于兼容性原因，将不输出错误消息。
第 2 代阅读器：由于可根据阅读器和转发器间距自动优化功率限值，因此第 2 代 (6GT2801-3BAx0) RF380R 阅读器不需要此设置。出于兼容性原因，依然认可该设置。请注意，值“0x02”、“0x03”和“0x04”可降低发送功率。</td></tr>
<tr><td>位 0...3：发射功率
（第 1 代阅读器）
允许使用以下值：
• 2：0.5 W
• 3：0.75 W
• 4：1.0 W
• 5：1.25 W（默认值）
• 6：1.5 W
• 7：1.75 W
• 8：2.0 W</td><td>位 4...7：天线类型
（第 2 代 RF350R 阅读器）
要改进抗干扰通信。
允许使用以下值：
• 0：未指定（默认值）
• 1：ANT 1
• 2：ANT 3
• 3：ANT 3S
• 4：ANT 8
• 5：ANT 12
• 6：ANT 12（6GT2398-1CC10，包含一根 0.6 m 长的集成天线连接电缆）
• 7：ANT 18
• 8：ANT 18（6GT2398-1CA10，包含一根 0.6 m 长的集成天线连接电缆）
• 9：ANT 30</td></tr>
</table>

参数	说明
发送应答器数量（组态数据的字节 13 和 14）	将分配值“0x0001”。
field_on_control（组态数据的字节 15）	将分配值“0x00”。

<table>
<tr><th>参数</th><th colspan="3">说明</th></tr>
<tr><td>Ident 块:
TAG_TYPE
Ident 配置文件：
field_on_time
（组态数据的字节 16）</td><td colspan="3">选择使用的发送应答器类型。
采用值“0x01”/“0x31”（ISO 15693 常规模式）时，第 2 代阅读器始终使用特定发送应答器实现最佳性能时所用的 ISO 指令。采用第 1 代阅读器时，值“0x01”通过基本 ISO 命令激活常规 ISO 模式. 采用此设置时，发送应答器的性能通常受到限制，但每个 ISO 兼容发送应答器均可基本保证正常工作。
系统手册“SIMATIC RF300”中指定的所有 ISO 15693 发送应答器 (MDS D) 均支持这些 ISO 命令。
可设置下列值：
<table>
<tr><th>值</th><th>含义</th><th>适用于...</th></tr>
<tr><td>0x00</td><td>RF300 (RF3xxT)</td><td>第 1 代和第 2 代</td></tr>
<tr><td>0x01</td><td>ISO 15693 常规
通过基本 ISO 命令激活常规 ISO 模式。采用此设置时，每个 ISO 兼容发送应答器均可基本保证正常工作。</td><td>第 1 代和第 2 代</td></tr>
<tr><td>0x03</td><td>ISO 15693（MDS D3xx，Infineon）</td><td>第 1 代和第 2 代</td></tr>
<tr><td>0x04</td><td>ISO 15693（MDS D4xx，Fujitsu - 2 KB）</td><td>第 1 代和第 2 代</td></tr>
<tr><td>0x05</td><td>ISO 15693（MDS D1xx，NXP）</td><td>第 1 代和第 2 代</td></tr>
<tr><td>0x06</td><td>ISO 15693（MDS D2xx，TI）</td><td>第 1 代和第 2 代</td></tr>
<tr><td>0x07</td><td>ISO 15693（MDS D261，STM）</td><td>第 1 代和第 2 代</td></tr>
<tr><td>0x08</td><td>ISO 15693（MDS D5xx，Fujitsu - 8 kB）</td><td>第 2 代</td></tr>
<tr><td>0x10</td><td>RF300 (RF3xxT)</td><td>第 2 代</td></tr>
<tr><td>0x20</td><td>ISO 14443（MIFARE Classic，MOBY E，MDS E6xx）</td><td>第 2 代</td></tr>
<tr><td>0x2F</td><td>ISO 14443 (MIFARE Classic)
在开放模式下，可更改 MIFARE Classic 发送应答器上的密钥资料（请参见下文的“将替代密钥与 MIFARE Classic 发送应答器搭配使用”章节）</td><td>第 2 代</td></tr>
<tr><td>0x31</td><td>常规模式
激活“常规模式”(General Mode) 以处理 RF300、ISO 15693 和 ISO 14443（MIFARE Classic，MOBY E）类型的发送应答器。采用此设置时，所有兼容的发送应答器均可基本保证正常工作。</td><td>第 2 代</td></tr>
</table></td></tr>
</table>

参数	说明		
	0x40	P2P 主站	第 2 代
	0x4F	P2P 设备	第 2 代
	0xFF	=ISO（设置"scanning_time"和"fcon"）	第 1 代和第 2 代
	请注意，可结合各设置或发送应答器系列（例如 ISO 15693 常规 + RF300）。此时，需要结合相关十六进制值（ISO 15693 常规 [0x01] + RF300 [0x10] = 0x11）。 **注** • ISO 15693：不支持以下特殊功能： – AFI（应用程序系列标识符） – DSFID（数据存储格式标识符） – 芯片特定的附加功能，例如 EAS、Kill 命令等 • 无效参数将被确认并返回错误消息"0xE6FE0300"或"0x15"。		

2.4 产品特定信息

说明

通过 RF182C 使用功能和命令

功能和命令与操作说明"通信模块 RF182C"（2010 年 10 月版，第 6.1 节"命令概述"和 A 部分"命令和确认帧"）中的内容相同。

RF300 支持通信模块 RF182C 的以下命令：

- RESET
- GetReaderStatus (mode 01, 06)
- GetTagStatus (mode 01, 02, 03)（RF300 模式下）
- GetTagStatus (mode 03)（ISO 模式下）
- writeTagData
- readTagData
- initializeTag
- setAnt

说明

通过 RF160C 使用功能和命令

功能和命令与操作说明"采用 FC 44 的 RF160C 通信模块"（2010 年 5 月版，第 5 节"参数分配"）中的内容相同。

操作说明中使用的参数名称对应于 FB 45 中的参数名称（参见上表）。更新的参数值见上表。参数名称和参数值也适用于 FC 44。

说明

“SIMATIC RF300”系统手册中的详细信息

有关状态查询相关参数值的详细信息，请参见第 10.2 节“诊断功能 - STEP 7”。在第 7 至 9 节中，可以找到与“Init”、“Write”和“Read”命令相关的通信模块的寻址发送应答器和硬件参数信息。

2.5 可将替代密钥与 MIFARE Classic 发送应答器搭配使用

替代密钥

要求

要使用替代密钥，需要全面了解有关要组态的 MIFARE Classic 发送应答器结构的信息（地址和访问权限）。同时，还有必要使用应用示例中的函数块。

工作原理

原则上，可以将任何密钥存储在阅读器上，取代永久集成的 MOBY E 密钥。每个分区（最多 40 个分区）最多可存储 2 个不同的密钥（A、B）。如果存储了不同的密钥，则阅读器将自动使用这些密钥取代 MOBY E 密钥。

以下应用示例介绍了如何在阅读器上存储密钥。

应用示例 (https://support.industry.siemens.com/cs/ww/en/ps/15003/ae)

请注意，这些替代密钥不会永久保存。重新启动阅读器（关闭/打开电源）会删除替代密钥，并且 MOBY E 密钥会再次自动激活。在这种情况下，需要将替代密钥再次传送到阅读器。

在“ISO 14443（MIFARE Classic，MOBY E，MDS E6xx）”模式下，可通过“ftim = 0x20”读写这些发送应答器的用户数据，前提是已将分配给对应分区的相应密钥存储在阅读器和发送应答器上。如果要使用 B 密钥访问（读取、写入）发送应答器，则需要考虑到：线性寻址以地址“0x8000”开头，而非以地址“0x0000”开头。

“NC”模式

要求

请注意，只有经过培训的用户才能使用“NC”模式。要使用“NC”模式，需要全面了解有关要组态的 MIFARE Classic 发送应答器结构的信息（地址和访问权限）。处理不当可能导致对发送应答器的访问被永久、不可修复地锁定。

工作原理

如果还要启用对密钥的读写访问以及对任何 MIFARE Classic 发送应答器的访问权限，则需要使用“ftim = 0x2F”启用“NC”模式。在该模式下，可处理 1k 发送应答器的所有 1024 字节或 4k 发送应答器的 4096 字节。如果要使用 B 密钥访问（读取、写入）发送应答器，则需要考虑到：线性寻址以地址“0x8000”开头，而非以地址“0x0000”开头。

注：注意，“NC”模式在“常规模式”(General Mode) 下不可用。不能将“NC”模式与 ECC 或信号量方法结合使用。

2.6 ECC 模式

工作原理

在 ECC 模式下，阅读器能以较高概率检测到 RF300/IEC 14443 发送应答器（MIFARE CLASSIC，MOBY E）上的位错误。如有可能，在读访问期间会返回更正的数据（发送应答器上的数据保持不变）。进行写访问时，会更正发送应答器上的相关数据（如有可能）。ECC 模式只能用于已完全初始化（ECC 位置位）并因此而进行 ECC 格式化的发送应答器。为此，发送应答器被分成 16 个字节的块，其中 14 个字节为用户数据预留，2 个字节用于 ECC 信息 (CRC)。这会导致可用存储空间缩小约 1/8。

如果检测到并更正了位错误，则在“STATUS”输出参数中发出警告“0xF0FE0002”；对于 FB 45，参数“ANZ_ECC = True”置位。如果无法更正位错误，则输出错误“0xE1FE0700”或“0x0B”。

2.7 信号量方法

与 ECC 方法类似，此方法可增加数据完整性。它可以独立于 ECC 方法使用，也可以与 ECC 方法搭配使用。借助信号量方法，可检查“Write”命令或“Init”命令是否正确完成。一旦激活了该方法，特定阅读器便会将其应用于每个“Read”/“Write”或“Init”命令。

说明

与 RF320T 发送应答器的兼容性

不能将信号量方法与 RF320T 发送应答器搭配使用。

要求

- 信号量方法只能用于“RF300”和“ISO 14443（MIFARE Classic，MOBY E）”模式（“ftim = 0x00/0x10/0x20”）。
- 通过设置“Reset”命令的“param”字节（位 6）来执行激活。
- 在阅读器中激活信号量方法后，需要使用完整的“Init”命令对受影响的发送应答器进行一次初始化。

工作原理

信号量的状态存储在发送应答器的最后一个可写字节中。这表示，在使用信号量方法时，将无法使用完整的存储区。信号量可读取但无法写入。读取时，以下状态之间有区别：

- “写操作已启动”(0xAA)
- “写操作已完成”(0x55)

“Init”或“Write”命令将信号量设置为“写操作已启动”状态，并在成功完成命令后将其设置为“写操作已完成”状态。在“Read”/“Write”命令之前和在局部“Init”之前，都将检查信号量的状态。

基于“Read”命令的检查示例

阅读器读取发送应答器的最后一个字节并检查信号量是否为“写操作已完成”状态。如果所得结果是确定的，将执行“Read”命令。如果所得结果是否定的，则会确认“Read”命令，并提示错误“E1FE0600”或“0x04”。在这种情况下，不会执行“Read”命令，也不会读取任何数据。

该方法与“Write”命令和局部“Init”命令相同。如果检查成功完成，则阅读器将信号量设置为“写操作已启动”。成功完成“Write”命令或局部“Init”后，信号量将设置为“写操作已完成”。

链

对于命令部分“Init”、“Read”或“Write”，首先检查信号量是否为“写操作已完成”，如果状态不正确，完整序列中止，确认后返回错误消息“E1FE0600”或“0x04”。仅针对这些命令执行一次检查，也就是说，如果其中一条命令在序列中再次出现，将不再执行检查。如果完整的“Init”命令是序列的一部分，并且命令部分跟随“Init”、“Read”或“Write”，将不再检查包含这些命令的信号量的状态。如果序列中某个命令位于完整“Init”命令前，则执行检查。

请注意，将信号量设置为“写操作已启动”始终在序列的第一个“Init”或“Write”命令中完成。“写操作已完成”状态仅在链的末端设置，类似于完整的“Init”命令。

注意
错误 如果在执行“Write”/“Init”期间出错，必须使用完整的“Init”命令再次对发送应答器进行初始化。

注意
使用信号量和 ECC 方法减小 ECC 内存 使用 ISO 14443 发送应答器（MIFARE Classic，MOBY E）时，如果将信号量方法与 ECC 方法一起使用，则 ECC 块的数量会减少一个（14 字节用户存储器）。

P2P 模式

3

3.1 说明

第二代 SIMATIC RF300 阅读器互相之间可直接通信。该通信模式被称为对等通信 (P2P) 或阅读器 - 阅读器通信，且其工作原理与跟 MOBY I 的对话操作相关。

如果在 SIMATIC S7-1200 或 S7-1500 控制器上通过通信模块操作 RF300 阅读器，建议使用“SIMATIC Ident > TO_Ident”工艺对象通过 STEP 7 (TIA Portal) 执行参数分配。但是，如果阅读器是通过第三方控制器操作的，则使用下文介绍的参数“ftim”对阅读器执行参数分配。

工作原理

在阅读器 - 阅读器通信中，通过使用阅读器参数分配来指定 P2P 主站设备和 P2P 设备。设备不再作为阅读器，而是作为可由主站控制器和设备控制器进行写入和读取的虚拟的、不稳定的收发器或数据存储器。请注意，断电后存储在设备存储器中的数据会立即丢失。

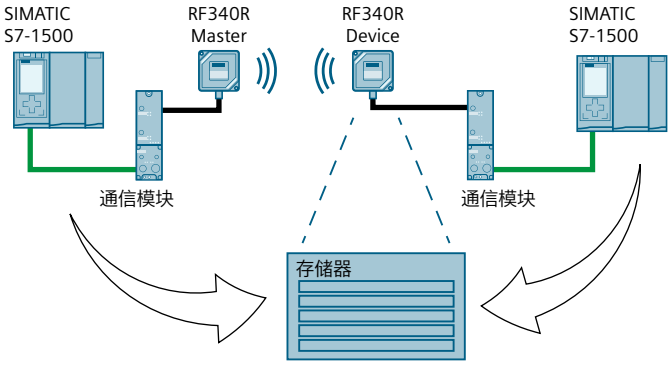

图 3-1　阅读器 - 阅读器通信如何工作

阅读器 - 阅读器通信在帧中通过“ftim”参数组态。根据所设置的值，相应的阅读器会成为 P2P 主站或 P2P 设备。

在混合运行中，主站可以额外处理 ISO 或 RF300 收发器。

可以在“ftim”参数中设置以下值，以使用阅读器 - 阅读器通信：

- 0x40 = P2P 主站
- 0x41 = 带有 ISO 收发器 (MDS Dxxx) P2P 主站及混合运行
- 0x50 = 带有 RF300 收发器的 P2P 主站及混合运行
- 0x4F = P2P 设备

P2P 设备具有 64 KB 可用存储空间。这使得有效值在"0x0000"到"0xFFFF"之间。注意，在阅读器 - 阅读器通信中，没有 OTP 存储器以及地址可以用于访问 UID。不支持 Ident 块 "Read_UID"。UID 看使用"MDS Status/Tag Status"命令读取。

可通过主站空中接口（读取/写入/Init 命令）或设备控制器访问设备存储器。

存在性检查

阅读器 - 阅读器通信支持 P2P 主站和 P2P 设备的存在性检查。对于主站，该功能等同于阅读器 - 收发器通信的功能。对于设备，存在性显示则是作为主站和设备间通信指示器。

3.2 命令结构和字段数据

P2P 通信的命令集

命令的结构或确认帧与标准阅读器 - 收发器通信相关。

阅读器 - 阅读器通信中允许使用以下命令 (FB 45/Ident profile)：

- Read / Physical-Read
- Write / Physical-Write
- SLG-Status (mode 1) / Reader-Status (0x81)
- MDS-Status (mode 3) / Tag-Status (0x83)
- Reset / Write-Config
- Set-ANT / Put
- Repeat（仅主站）
- Init / Format

通过 MDS Status（模式 3）/Tag Status (0x83) 进行诊断

相比于阅读器 - 阅读器通信和阅读器 - 收发器通信，“MDS Status/Tag Status”命令的内容不相同。在执行“MDS Status/Tag Status”命令后，设备的确认包含以下内容：

表格 3-1　通过 MDS Status（模式 3）/Tag Status (0x83) 进行诊断，相对应于 UDT 230。

参数	大小	说明
UID	数组为 [1...8] 的字节	唯一标识符号 每个设备均有唯一的 UID。在阅读器 - 阅读器通信中，UID 的首个字节通常分配为“V”或“0x56”。这样可以立即检测到 P2P 设备。余下的 UID 是由阅读器的序列号生成的。
MDS_type	1 字节	阅读器类型 • 'A' = RF310R • 'B' = RF340R • 'C' = RF350R • 'D' = RF380R
IC_version	1 字节	保留
size	2 个字节	P2P 设备存储器大小（- 1 字节）
lock_state	1 字节	保留
block_size	1 字节	始终分配“01”。
nr_of_blocks	1 字节	始终分配“FF”。

P2P 通信中的字段数据

表格 3-2　第 2 代 RF300 阅读器在阅读器 - 阅读器通信的字段数据

	传输窗口的长度		工作距离 (S_a)	限制距离 (S_g)
	x 方向 (L_x)	y 方向 (L_y)		
RF310R 到 RF310R	55	55	10...20	60
RF340R 到 RF340R	110	110	10...60	80
RF350R 到 ANT1	100	100	30...80	100
RF350R 到 ANT18	13	13	5...12	15

	传输窗口的长度		工作距离 (S_a)	限制距离 (S_g)
	x 方向 (L_x)	y 方向 (L_y)		
RF350R 到 ANT30	20	20	5...20	25
RF380R 到 RF380R	130	110	20...120	130

在阅读器到阅读器间最小的距离的情况下，该值在《SIMATIC RF300 系统手册》中描述。

P2P 通信的通信时间

对于阅读器到阅读器或阅读器到天线的空中接口的通信时间，具有以下近似公式：

$$t_K \approx \text{ceil}\,(n_{Byte}/32) * (2{,}25\ \text{ms}) + 88\ \mu\text{s} * n_{Byte}$$

t_k： 阅读器到阅读器或阅读器到天线的通信时间

ceil 取整函数

n_{bytes} 用户数据量（以字节为单位）

注意公式仅适用独立命令。对于链接命令，实际值可能会更高。

ISO 隧道

4

4.1 说明

ISO/IEC 15693 标准定义了可用于根据该标准指定的发送应答器的命令。SIMATIC RF300 系统支持 ISO/IEC 15693 标准中定义的发送应答器命令的常用命令。但是，RF300 阅读器可能无法处理/解析少量芯片特定的 ISO 命令。下文基于具体应用示例介绍了如何使用这些命令。

工作原理

利用 ISO 隧道，可将 RF300 阅读器不支持的受影响命令通过阅读器从控制器发送到发送应答器。但本例中的阅读器是“有隧道”的。这意味着受影响的 ISO 命令始终会发送到“Write”和“Read”命令中嵌入的阅读器。阅读器处理“Write”/“Read”命令，并将其中嵌入的 ISO 命令直接转发到发送应答器，或将其确认转发到控制器。为此，会在写入命令的消息帧中传送 ISO 命令，在读取命令中传送 ISO 确认。

通过这种方法，可使用所有 ISO 和供应商特定命令来满足以下条件：

- 发送应答器或其中安装的芯片支持该 ISO 命令。
  要确定发送应答器芯片是否支持相应命令，请参见芯片数据表。
- 仅可执行返回响应帧或确认的 ISO 命令。

注意
受支持命令的限制 ISO/IEC 15693-3 标准中定义的以下命令不能用于 ISO 隧道： • Inventory • Stay Quiet • Fast Read Multiple Blocks • Fast Extended Read Multiple Blocks • Challenge 也不能使用以下供应商特定命令： • 所有 Fast... 命令 • Inventory Read 如有必要，可在使用发送应答器或命令之前检查发送应答器是否支持此命令。

应用示例：增加 OPT 存储器

一个典型应用示例是以用户存储器为代价增加 OTP 存储器的命令。利用 RF300 阅读器，可使用“Write”命令从地址“0xFF80”开始写入存储区，然后再对其进行写保护。此选项仅限于 16 个最重要的地址。通过“Lock Block”ISO 命令，可对发送应答器用户存储区中的各个存储块进行写保护。

可使用“Lock Block”命令执行该存储器转换，以锁定块，并可使用“Get Multiple Block Security Status”读出各个存储块的状态。

4.2 命令执行

可使用 Ident 配置文件或 Ident 块“IID_CMD_STRUCT”执行嵌入的 ISO 命令。

要求

“Write”/“Read”命令始终需要按指定顺序成对执行。

操作步骤

要执行嵌入的 ISO 命令，请按以下步骤操作：

1. 在“0xFFF8”地址上执行“Write”命令。
   命令的长度必须与要执行的 ISO 命令一致。有关命令的长度，请参见相关发送应答器芯片的数据表。要执行的 ISO 命令必须输入到写入命令的缓冲区中。

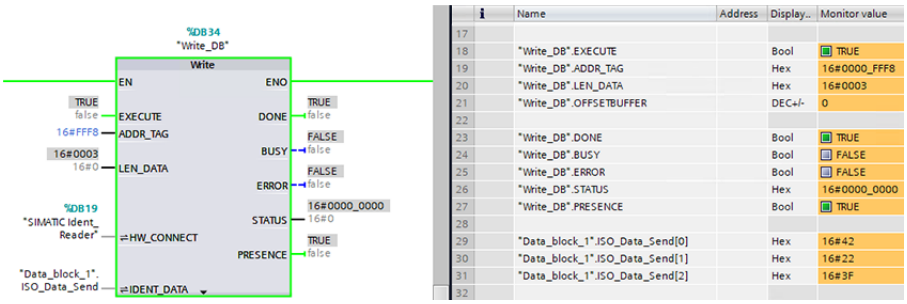

图 4-1　“Write”命令

2. 在“0xFFF8”地址上执行“Read”命令。
   命令长度必须 ≥ 预期收到的确认长度。ISO 命令的确认存储在读取命令的缓冲区中。确认额数据必须由用户评估。

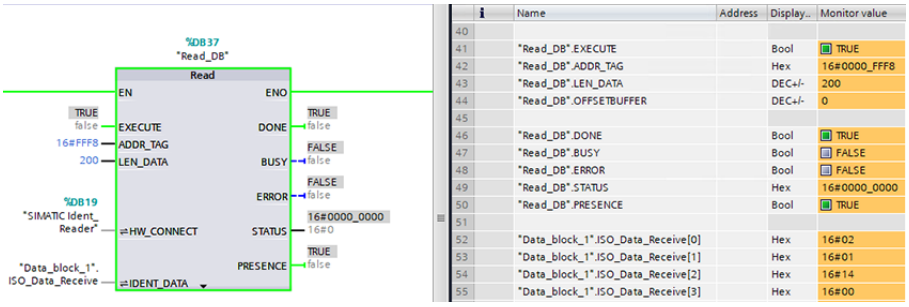

图 4-2　“Read”命令

两个命令的“STATUS”输出参数（“ERROR = TRUE”）指示命令是否已正确执行。如果在读取命令的确认中输入状态“00”，则消息帧仅接收有效的 ISO 确认。

说明

链接命令结构

请注意，两个命令可以链接执行。也可将命令作为较大命令链的一部分进行发送。

错误消息

表格 4-1 “STATUS”字节可能的错误消息

错误消息	说明
0xE1FE0200	存在性错误 发送应答器已脱离阅读器的传输 窗口。该命令仅执行了一部分。 读取命令：“IDENT_DATA” 无有效数据。 写入命令：刚离开天线场的发送应答器包含不完整的数据记录。 可能的原因： • 阅读器与发送应答器之间未一直保持 有效的工作距离。 • 组态错误：待处理的数据记录 过大（动态模式）。 • 超时：天线场中无发送应答器。
0xE1FE0300	地址错误 指定的存储器地址出错 （尝试访问不存在或不可访问的 存储区）。
0xE2FE0100	空中接口存在故障，无法对发送应答器进行处理。
0xE4FE0300	未检测到天线。可能的原因： • 未连接天线。 • 天线电缆出现故障。
0xE6FE0100	参数分配错误；可能的原因： • 未知命令 • 参数不正确 • 不允许该函数 ISO 确认长度大于读取确认中允许的最大消息帧大小。

4.3 ISO 命令的结构

ISO 命令/确认的结构始终遵循一致的模式。下表概括列出了 ISO 命令/确认的一般结构。

表格 4-2 ISO 命令的结构

参数/ 字段名称	长度	说明
Flags	1 字节	控制命令结构和发送应答器响应行为的位数组。 • 位 0：Subcarrier 定义发送应答器响应期间的调制行为（RF300 始终为“0”）。 • 位 1：Data rate 确定发送应答器的传输速度（RF300 始终为“1”）。 • 位 2：Inventory 确定命令是否为类似 Inventory 的命令，其中“Flags”参数的位 4 ... 7 的含义有改变。对于 RF300，该位必须始终为“0”，因为它不支持类似于 Inventory 的命令。 • 位 3：协议扩展 可能需要在发送应答器和命令特定的基础上进行设置。有关此位的更多信息，请参见芯片数据表。 • 位 4：Select 仅当之前通过 ISO 命令“SELECT”选择了发送应答器时，该发送应答器才会响应命令。一般只有多标签应用需要设置此位。 • 位 5：已寻址 仅限 UID（标签 ID）已通过命令参数发送的发送应答器。一般只有多标签应用需要设置此位。 • 位 6：Option 可能需要在发送应答器和命令特定的基础上进行设置。有关此位的更多信息，请参见芯片数据表。 • 位 7：保留 始终需要为“0”。 本文未介绍类似 Inventory 的命令的位 4 ... 7 的含义，因为 RF300 系统不支持这些位。
命令	1 或 2 个字节	要执行的命令的代码。ISO 标准命令有 1 字节的代码，供应商特定命令有 2 字节的代码。有关这些命令的更多信息，请参见 ISO/IEC 15693-3 或芯片数据表。

参数/ 字段名称	长度	说明
参数/ 数据	0 ... n 个字节	这里会根据所选命令传送其它参数。例如： • 发送应答器的 UID（使用已寻址命令） • 地址（使用读取或写入命令） • 写入到发送应答器的数据 有关参数和数据的更多信息，请参见 ISO/IEC 15693-3 或芯片数据表。
CRC	2 个字节	命令前面字节的校验和。对于 RF300，不需要传送 CRC 值，因为阅读器会自动确定该值。

表格 4-3　ISO 确认的结构

参数/ 字段名称	长度	说明
Flags	1 字节	更详细地描述确认帧中数据的结构和含义的位数组。 • 位 0：Error 如果该位已置 1，则会在“Data”参数中输入 1 字节代码。 • 位 1 ... 7：保留 一般情况下始终为“0”。
参数/ 数据	0 ... n 个字节	如果在“Flags”参数中将位 0 置 1，此处会输出 1 字节的错误代码。 否则，会根据所选命令在此处输入其它参数/数据。例如： • 有关发送应答器的状态信息 • 有关锁定存储器块的状态信息 • 从发送应答器读取的数据 有关参数和数据的更多信息，请参见 ISO/IEC 15693-3 或芯片数据表。
CRC	2 个字节	命令前面字节的校验和。对于 RF300，不会返回 CRC 值，因为阅读器会自动校验该值。

4.4 示例帧

下文介绍的 ISO 命令“Lock Block”和“Get Multiple Block Security Status”可用于锁定存储器块和读出 Lock 信息。

ISO 命令“Lock Block”

通过此命令，最多可锁定 ISO 发送应答器用户存储器的一个存储器块，从而仅可对其进行读访问。例如，随后可将该存储器块用作 OTP 扩展。请注意，该锁定是永久性的，不能再取消。

利用下表，可根据自身需求组态命令并评估结果。

表格 4-4 “Lock Block”命令的结构

参数	说明
Flags（8 位）	选择取决于使用的发送应答器类型 允许的值： • 0x02： – ISO 15693 常规 – MDS D1xx，NXP – MDS D261、STM 或 NXP – MDS D3xx，Infineon – MDS D4xx，Fujitsu - 2 KB – MDS D5xx，Fujitsu - 8 KB • 0x42： – ISO 15693 常规 – MDS D200，TI
Cmd（8 位）	命令选择 值必须为“0x22”（“LockBlock”）。
BlockNumber（8 位）	通过块编号，始终会从块 0x00 开始寻址发送应答器用户存储器中的锁定。在配有 Infineon、NXP、TI 和 STM 芯片的发送应答器中，存储器块大小为 4 字节，在发送应答器 MDS D4xx (Fujitsu - 2 kB) 中，存储器块大小为 8 字节，MDS D5xx (Fujitsu - 8 kB) 为 32 字节。 允许的值： • 0x00...0x1B：MDS D1xx，NXP（112 字节） • 0x00...0x3F：MDS D2xx、STM 或 TI（256 字节） • 0x00...0x4E：MDS D261（AS“C”），NXP（316 字节） • 0x00...0xF7：MDS D3xx，Infineon（992 字节） • 0x00...0xF9：MDS D4xx，Fujitsu - 2 KB（2000 字节） • 0x00...0xFF：MDS D5xx，Fujitsu - 8 KB（8192 字节）

表格 4-5 “Lock Block”确认的结构

参数	说明
LengthISO（8 位）	消息帧的字节数（不包括长度字节）
Flags（8 位）	有关命令是否成功执行的信息。 允许的值： • 0x00：命令得到肯定确认。 • 0x01：命令得到否定确认。
ErrorCode（8 位）	命令得到否定确认时的错误消息或错误代码。 有关详细信息，请参见 “错误消息 (页 34)”部分。

ISO 命令“Get Multiple Block Status”

通过此命令，可读出发送应答器多个存储器块的 Lock 信息。请注意，每个块仅传送一个字节的数据。

利用下表，可根据自身需求组态命令并评估结果。

表格 4-6 “Get Multiple Block Security Status”命令的结构

参数	说明
Flags（8 位）	选择取决于使用的发送应答器类型 允许的值：0x02 • ISO 15693 常规 • MDS D1xx，NXP • MDS D200，TI • MDS D261、STM 或 NXP • MDS D3xx，Infineon • MDS D4xx，Fujitsu - 2 KB • MDS D5xx，Fujitsu - 8 KB
Cmd（8 位）	命令选择 值必须为“0x2C”（“Get Multiple Block Security Status”）。

参数	说明
BlockNumber（8 位）	通过块编号，始终会对要从中读出状态的发送应答器用户存储器中的第一个块进行寻址。在配有 Infineon、NXP、TI 和 STM 芯片的发送应答器中，存储器块大小为 4 字节，在发送应答器 MDS D4xx (Fujitsu - 2 kB) 中，存储器块大小为 8 字节，MDS D5xx (Fujitsu - 8 kB) 为 32 字节。 允许的值： • 0x00...0x1B：MDS D1xx，NXP（112 字节） • 0x00...0x3F：MDS D2xx、STM 或 TI（256 字节） • 0x00...0x4E：MDS D261（AS“C”），NXP（316 字节） • 0x00...0xF7：MDS D3xx，Infineon（992 字节） • 0x00...0xF9：MDS D4xx，Fujitsu - 2 KB（2000 字节）[1)] • 0x00...0xFF：MDS D5xx，Fujitsu - 8 KB（8192 字节）[1)] [1)] 指定的 BlockNumber 必须始终可被 8 整除。
NumberofBlocks（8 位）	要读出其状态数据的块数。“NumberofBlocks = 0x00”表示将读取一个块。第一个块编号与块数之和不得超过发送应答器中的总块数。允许的最大块数取决于发送应答器芯片。 允许的最大值： • 0x1B：MDS D1xx，NXP（112 字节） • 0x3F：MDS D2xx、STM 或 TI（256 字节） • 0x4E：MDS D261（AS“C”），NXP（316 字节） • 0xF7：MDS D3xx，Infineon（992 字节） • 0x3F：MDS D4xx，Fujitsu - 2 KB（2000 字节）[1)] • 0xFF：MDS D5xx，Fujitsu - 8 KB（8192 字节） [1)] 执行一次命令最多可读取 64 个块。

表格 4-7　发生错误时“Get Multiple Block Security Status”确认的结构

参数	说明
LengthISO（8 位）	消息帧的字节数（不包括长度字节）
Flags（8 位）	有关命令是否成功执行的信息。 允许的值： • 0x00：命令得到肯定确认。 • 0x01：命令得到否定确认。
ErrorCode（8 位）	命令得到否定确认时的错误消息或错误代码。 有关详细信息，请参见 “错误消息 (页 34)”部分。

表格 4-8　未发生错误时"Get Multiple Block Security Status"确认的结构

参数	说明
LengthISO（8 位）	消息帧的字节数（不包括长度字节）
Flags（8 位）	有关命令是否成功执行的信息。 允许的值： • 0x00：命令得到肯定确认。 • 0x01：命令得到否定确认。
BlockSecurityStatus 0（8 位）	有关存储器块是否锁定的信息。 允许的值： • 0x00：受影响的块未锁定。 • 0x01：受影响的块已锁定。
BlockSecurityStatus 1（8 位）	
…	
BlockSecurityStatus n（8 位）	

4.5 错误消息

执行 ISO 命令时可出现下列错误消息。这些错误消息基于 ISO/IEC 15693 标准。有关供应商特定的错误代码，请参见相应供应商的数据表。

表格 4-9　ISO 特定的错误消息

错误代码	说明
0x01	命令不受支持，即请求代码未知。
0x02	命令未被识别，例如发生格式错误。
0x03	命令选项不受支持。
0x04	无法及时处理命令。
0x0F	发生错误（没有附加信息），或特定的错误代码不受支持。
0x10	指定的存储器块不可用（不存在）。
0x11	指定的存储器块已锁定，不能再次锁定。
0x12	指定的存储器块已锁定，不能更改其内容。
0x13	指定的存储器块编程不成功。
0x14	指定的存储器块锁定不成功。
0x15	指定的存储器块受到保护。

错误代码	说明
0x40	常规密码错误。
0xA0 ... 0xDF	用户特定命令的错误代码。
所有其它情况	系统预留，供将来使用

4.6 ISO 发送应答器概述

下表简要列出了 ISO/IEC 15693 发送应答器中安装的芯片及其供应商 (MDS D)。

表格 4-10　发送应答器中安装的芯片

发送应答器	供应商	芯片
MDS D1xx	NXP	I-Code SLI； I-Code SLI-X
MDS D200	Texas Instruments (TI)	Tag-it HF-I 2048
MDS D261	• 修订版 B：STM • 修订版 C：NXP	• LRI2k • I-Code SLI-X2
MDS D3xx	Infineon	SRF 55V10P
MDS D4xx	Fujitsu - 2 kB	MB89R118
MDS D5xx	Fujitsu - 8 kB	MB89R112

供应商特定的偏差

一些供应商的芯片有着与其它芯片不同的特定行为。这会影响以下供应商的芯片：

- NXP (MDS D1xx)
  如果发送的 ISO 命令不正确，发送应答器会返回"Presence error"错误消息。命令会按照天线场中无发送应答器的情况执行。
- Fujitsu
  通过"Get Multiple Block Security Status"ISO 命令，对 MDS D4xx 发送应答器执行一次命令最多可读取 64 个命令（"BlockNumber ≤ 0x3F"参数）。对于发送应答器 MDS D4xx 和 MDS D5xx，BlockNumber 始终需要可被 8 整除。

附录 A

Industry Online Support

除产品文档外，还可以通过以下网址的 Siemens Industry Online Support 综合在线信息平台获取支持：
链接： (https://support.industry.siemens.com/cs/de/en/)

除新闻外，还介绍了以下内容：

- 项目信息：手册、常见问题解答、下载资料、应用程序示例等
- 联系人，技术论坛
- 提交支持请求的选项：
  链接： (https://support.industry.siemens.com/My/ww/en/requests)
- 我们的服务提供：
  针对我们的产品和系统，我们还提供大量服务，支持机器或系统使用的每个阶段 - 从规划和实施到调试，直至维护和现代化。

有关联系数据，请访问以下 Internet 网址：
链接： (https://www.automation.siemens.com/aspa_app/?ci=yes&lang=en)

“工业标识”主页

有关识别系统的最新常规信息，请访问 Internet 上的“主页 (www.siemens.com/ident)”。

在线的产品目录和订购系统

可通过 工业商城主页 (https://mall.industry.siemens.com) 查找到在线的产品目录和在线的订购系统。

SITRAIN - Training for Industry

该培训包括 300 多门与基本主题、扩展知识和专业知识相关的课程，以及个别部门的高级培训 - 可在 130 余个地点开展培训。课程也可单独组织，并于您的所在地进行授课。

有关培训课程以及如何联系客户顾问的详细信息，请访问以下 Internet 网址：

链接： (https://new.siemens.com/global/en/products/services/industry/sitrain.html)