

基于CP模块的S7-300_400以太网接收发送功能总结

原创文章，转载请注明出处。

更多实用资料请登录方正智芯官网：www.founderchip.com

作者：北岛李工

CP模块（Communication Processor，比如：CP343-1/Cp443-1）安装完成后，还需要对其进行组态和编程才能实现以太网通信。今天这篇文章，我们来聊聊西门子S7-300/400系列PLC提供的基于CP模块的以太网通信的编程接口（FCs）。



S7-300/400系列PLC总共提供了6个用于CP模块（Communication Processor）以太网通信的功能（FC），请看下面这张表格：

方正智芯(founder chip)——SEND/RECV功能总结				
指令/功能		可用于		功能描述
名称	编号	S7-300	S7-400	
AG_SEND	FC5	X	X	发送数据
AG_RECV	FC6	X	X	接收数据
AG_LSEND	FC50		X	发送数据
AG_LRECV	FC60		X	接收数据
AG_SSEND	FC53		X	发送数据
AG_SRECV	FC63		X	接收数据

对于S7-300系列PLC而言，可以使用AG_SEND（FC5）发送数据，使用AG_RECV（FC6）接收数据，每次最多可以发送或接收**8192**个字节的数据；对于S7-400系列PLC而言，上述六个功能均可以使用，但是发送/接收的字节数有所不同：AG_SEND/AG_RECV在S7-400中每次最多只能发送/接收**240**个字节（是的，240 bytes，你没看错）；如果你需要传输的数据量比较大，可以使用AG_LSEND/AG_LRECV（字母“L”表示“Large”），

每次最多可以发送/接收8192个字节的数据；而功能AG_SEND/AG_SRECV经过特殊的优化，可以在CPU和CP模块之间快速传送大量的数据，其每次最多可以发送/接收1452个字节的数据；

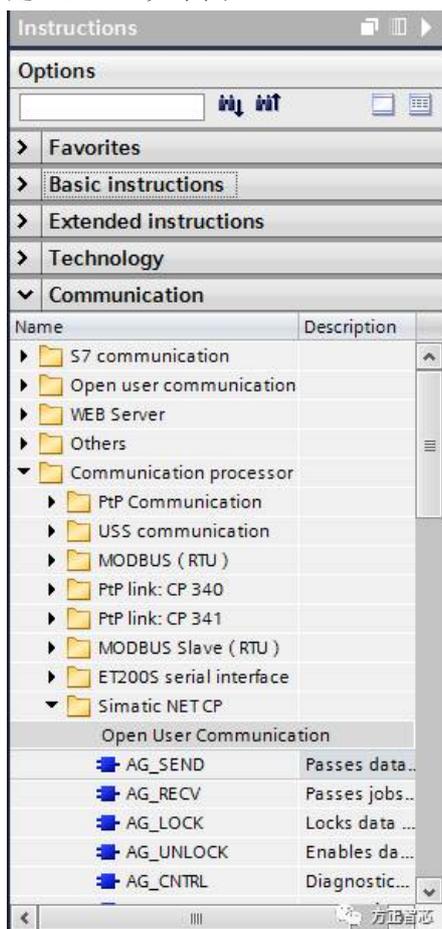
下面这张表格总结了各发送/接收功能（FCs）在不同的CPU环境及不同的通信协议下所支持的单次最大传输的字节数：

方正智芯(founder chip)——SEND/RCV最大支持的字节数				
指令/功能	协议类型			
	ISO	ISO-ON-TCP	TCP	UDP
AG_LSEND(S7-400)	8192 bytes	8192 bytes	8192 bytes	2048 bytes
AG_SEND(S7-300)				
AG_SEND(S7-400)	240 bytes	240 bytes	240 bytes	240 bytes
AG_RECV(S7-400)	240 bytes	240 bytes	-	240 bytes
AG_LRCV(S7-400)	8192 bytes	8192 bytes	8192 bytes	2048 bytes
AG_RECV(S7-300)				
AG_SSEND(S7-400)	1452 bytes	1452 bytes	1452 bytes	1452 bytes
AG_SRECV(S7-400)				

需要说明的是：在S7-400中，AG_RECV不能用于接收TCP协议的数据，要使用AG_LRCV或者AG_SRECV。

以上是对CP模块的以太网通信各功能模块的总结，接下来我们看看如何在博途环境中使用这些功能（FCs）：

首先，在博途的指令列表中找到“通信（Communication）” - “通信处理器（Communication Processor）” - “Simatic NET CP”，在其目录中可以看到“AG_SEND”和“AG_RECV”（例程中组态的CPU是319F），如下图：



通信的编程需要拖动相应的功能到程序块中，然后对其参数进行赋值。我们先来看看AG_SEND的参数列表：

方正智芯(founder chip)—AG_SEND/AG_LSEND/AG_SSEND参数				
参数名称	类型	数据类型	取值范围	功能描述
ACT	Input	BOOL	0,1	当ACT=1时,发送LEN个字节的数据;当ACT=0时,更新DONE, ERROR, STATUS的状态
ID	Input	INT	取决于CPU	唯一连接标识
LADDR	Input	WORD		CP模块的地址
SEND	Input	ANY		要发送的数据(通常使用指针)
LEN	Input	INT	取决于CPU	发送数据的长度
DONE	Output	BOOL	0,1	任务是否完成;1=完成;0=任务还在进行中
ERROR	Output	BOOL	0,1	是否有错误发生;0=没有错误;1=有错误
STATUS	Output	WORD		状态代码
方正智芯				

当参数“ACT”的值为1时开始发送数据,发送的长度在参数“LEN”中定义(注意:不同的CPU和协议长度有所不同,参考本文前面的描述);“ID”和“LADDR”来自硬件组态;要发送的内容以指针的形式给“SEND”赋值;发送完成后“DONE”的值变为1;参数“ERROR”用来表示发送过程是否有错误发生;参数“STATUS”表示当前发送的状态;

同样的,接收功能(AG_RECV)也有一个参数列表,如下图:

方正智芯(founder chip)—AG_RECV/AG_LRECV/AG_SRECV参数				
参数名称	类型	数据类型	取值范围	功能描述
ID	Input	INT	取决于CPU	唯一连接标识
LADDR	Input	WORD		CP模块的地址
RECV	Input	ANY		用来接收数据的地址(通常使用指针)
NDR	Output	BOOL		是否接收到了新的数据
ERROR	Output	BOOL	0,1	是否有错误发生;0=没有错误;1=有错误
STATUS	Output	WORD		状态代码
LEN	Output	INT	取决于CPU	接收到的数据的长度
方正智芯				

“ID”和“LADDR”来自于硬件组态;“RECV”是接收数据的地址(通常是指向DB块的指针);“NDR”是英文“New Data Received”的缩写,其值为1时表示接收到了新的数据;“ERROR”用来标识接收过程中是否有错误发生(1=有错误发生);“STATUS”是接收的状态;“LEN”表示实际接收的数据的长度(以字节为单位);

好了,关于CP模块的以太网通信接口功能(FCs)就先介绍到这里了。相关参考文章:

[西门子以太网模块CP343-1和CP343-1 Lean有什么区别?](#)

官网提供本文PDF版本下载。


长按扫码关注



方正智芯

公众号: founderchip

官方网站: www.founderchip.com

原创工业智能控制领域(PLC、单片机、通信)的技术分享

