

面向精细化工流程控制的通信技术

何晓东¹ 杜红涛¹ 黄嘉明²

(1.珠海市长陆工业自动控制系统股份有限公司, 广东 珠海 519090

2.暨南大学理工学院, 广东 广州 510632)

摘要: 网络实时通信是精细化工流程控制的重要基础环节。以某生产车间精细化工流程控制系统为背景, 根据生产需求, 设计 PC 端与 PLC 的通信架构, 并优化报文收发机制, 使 PLC 的数据可根据系统的设定进行频率有差异地读取, 进而提高通信效率和生产效率。该方法对中小精细化工企业流程控制具有较好的借鉴意义。

关键词: 流程控制; 实时通信; 报文收发机制

中图分类号: TN914.3

文献标识码: A

文章编号: 1674-2605(2021)01-0009-05

DOI: 10.3969/j.issn.1674-2605.2021.01.009

0 引言

根据某生产车间精细化工流程控制系统的生产要求, 需在 PC 端实时查看生产情况与下单操作。PC 端通过实时通信反复轮询读取 PLC 的现场数据, 解析后放置于 PC 端的共享内存中待用。这对 PC 端与 PLC 之间的通信效率与通信质量提出较高要求, 然而数据的实时性有一定差异。PC 端向 PLC 读取数据时, 应根据数据实时性差异有规律地读取, 从而提高通信效率。

1 流程控制系统硬件

精细化工流程控制系统从下到上分为现场层、控制层和中心管理层 3 个层级, 包括的主要硬件如表 1 所示。

表 1 精细化工流程控制系统硬件表

硬件名称	选用产品
主控制器 PLC	1517-3 PN/DP
数字量输入模块	SM521 系列
数字量输出模块	SM522 系列
模拟量输入模块	SM531 系列
模拟量输出模块	SM532 系列
RS485 通信模块	西门子 RS485

现场层主要包括各种传感器、执行机构等设备, 负责工业现场数据采集和执行各种控制命令。

控制层包括 S7-1500 系列 CPU 控制器, 负责对采集的数据进行处理并输出控制信号。

中心管理层包括生产线监控系统、配方管理系统与生产排单系统等。控制层与中心管理层采用工业以太网的方式通信。

2 PC 端与 PLC 通信架构

精细化工流程控制系统的 PLC 采用 S7-1500。首先, 通过数据采集模块把现场数据采集到 PLC 的数据块, 并把数据类型和读写频率等级相同的数据放在相同地址块的连续区域, 以便虚设备批量读取数据和设置扫描级别来提高通信速率^[1-2]。其中, 虚设备定义为记录 PLC 数据块中连续并小于 1000 个字节的数据地址信息与设备信息的虚拟设备^[3]。

流程控制系统的通信架构图如图 1 所示。首先, 初始化虚设备与虚设备队列, 并将虚设备置于虚设备队列中, 虚设备队列用于轮询读取虚设备中的数据; 其次, 初始化写指令队列, 写指令队列用于存放需进行写操作的指令; 再次, 根据读写报文添加机制(轮询各虚设备并按其扫描级别)调用发送与解析包生成读写报文, 并分别将对应的读写报文添加到读写报文队列, 从而保证读取现场数据时, 实时性要求高的数据读取频率也高; 最后, 通道线程查看写报文队列是否存在写报文, 若存在, 则把写报文发送到指定设备

并读回结果报文，再调用发送与解析包解析是否写操作成功；若写报文队列为空，则把读报文队列中的读报文依次发送到指定设备并读回结果报文，再调用发送与解析包把相应的数据解析到共享内存中待用。

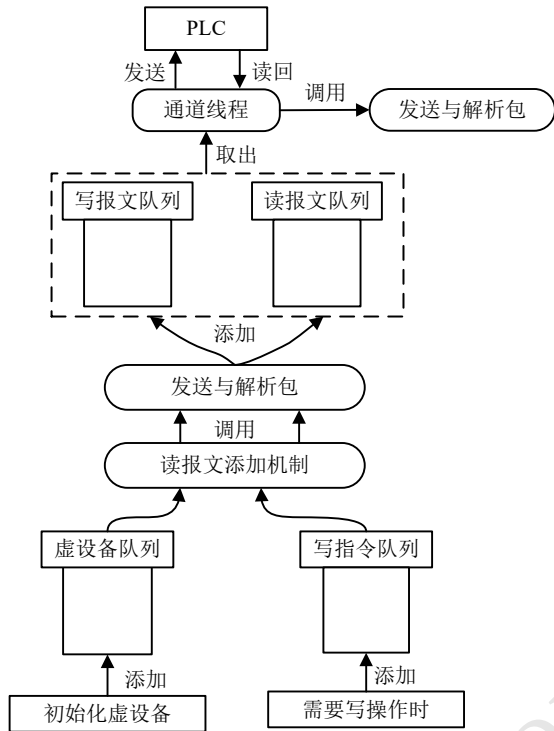


图 1 流程控制系统的通信架构图

3 虚设备与变量定义模块

3.1 虚设备模块设计

虚设备记录通信数据的具体位置信息与设备信息。一个虚设备最多可存放数据块中 1000 个字节连续的地址数据，而一个 TCP 报文长度约为 1480 字节，这样读一个虚设备的数据仅需一条读指令即可。虚设备增加了扫描级别等字段，用于设置该设备的通信频率^[4-6]。

虚设备初始化所需的参数（以 S7 协议为例）如表 2 所示。虚设备参数定义如下：

- 1) 虚设备名称和虚设备编号可区分各虚设备；
- 2) 通信驱动指采用的通信驱动名称；
- 3) 数据种类指数据属于哪个数据块，并由指定数字指代；
- 4) 数据格式用于定义变量格式，字节（8 位）、

字（16 位）和双字（32 位）；

5) 数据具体格式包括整型、无符号整型和浮点数 3 种；

6) 访问方式指访问数据的方式，分为只读、只写和可读可写；

表 2 虚设备初始化所需参数表

序号	字段意义	字段名	类型
1	虚设备名称	Devicename	nvarchar(200)
2	虚设备编号	DeviceNo	int
3	通信驱动	DrvName	nvarchar(100)
4	数据种类	DataType	int
5	数据格式	DataFormat	tinyint
6	具体格式	Deta_format	tinyint
7	访问方式	AccessMode	tinyint
8	开始地址	DataStart	int
9	数据长度	Datalen	int
10	通信地址	AreaNo	tinyint
11	超时时间	OverTimes	int
12	扫描级别	ScanClass	smallint
13	IP 地址	DevName	nvarchar(100)
14	端口号	VFDName	nvarchar(200)

7) 开始地址和数据长度分别指数据在目标设备中的开始位置和读取数据的总长度；

8) 超时时间指虚设备生成对应的读写报文后发送给目标设备，目标设备在指定的超时时间内没有返回结果报文时，将修改设备的扫描级别，使得该设备的通信频率降低，从而减少系统异常等待的时间；

9) 扫描级别是指发送读报文的频率等级，扫描级别包括 1~10, 1000, 2000 共 12 个数值，数值为 1~10 时，数字越小扫描频率越高；扫描级别为 1000 代表该虚设备的数据只读取一次；扫描级别为 2000 代表该虚设备的数据为定时读取；

10) IP 地址和端口号用于指定发送报文目标设备的 IP 地址和端口号。

根据系统的通信变量定义虚设备，虚设备列表如图 2 所示。

虚拟设备表														
	设备名称	驱动名称	端口	数据类型	地址	超时	扫描	开始地址	长度	单元格式	数值类型	访问	设备类	数据描述
1	功能码1	S7NetCom...	0	DB	1	1000	610	200000	500	字(16位)	无符号整型	读写	0	DB2.DBW0
2	功能码2	S7NetCom...	0	DB	1	1000	610	201000	500	字(16位)	无符号整型	读写	0	DB2.DBW1000
3	功能码3	S7NetCom...	0	DB	1	1000	610	202000	500	字(16位)	无符号整型	读写	0	DB2.DBW2000
4	功能码4	S7NetCom...	0	DB	1	1000	610	203000	500	字(16位)	无符号整型	读写	0	DB2.DBW3000
5	功能码5	S7NetComm...	0	DB	1	1000	610	204000	200	字(16位)	无符号整型	读写	0	DB2.DBW4000
6	关键字1	S7NetCom...	0	DB	1	1000	610	211000	500	字(16位)	无符号整型	读写	0	DB2.DBW11000
7	关键字2	S7NetCom...	0	DB	1	1000	610	212000	500	字(16位)	无符号整型	读写	0	DB2.DBW12000

图2 虚设备列表

为简化虚设备定义过程，双击虚设备列表界面即可弹出虚设备定义程序框界面，如图3所示。

定义虚拟设备

通讯驱动 S7NetComm

设备名称 关键字1

读取控制点 0

变化保存 不保存

☐ 忽略写跟踪

本地参数

扫描延时 0

通讯地址 1

超时 1000

扫描级别 610

通讯数据参数

设备类型 0

数据描述 DB2.DBW11000

数据种类 DB

访问方式 读写

开始地址 211000

数据格式 字(16位)

具体格式 无符号整型

数据长度 500

服务器IP 192.168.11.21

TCP 端口 102

删除

确定

取消

图3 虚设备定义程序框界面

在图3中，可输入或选中虚设备参数，然后一键生成虚设备，并记录于数据库中。通过该方式使虚设备定义过程模板化，易于修正。

3.2 变量定义模块设计

虚设备中每个变量代表的具体含义由变量定义模块来完成。该模块主要分为开关量模块、模拟量模块和文本量模块^[5]，它们分别用来定义大小为1个比特、1个字节和多个字节的通信变量位于指定虚设备的位置信息。

3.3 发送与解析模块

发送与解析模块主要完成读写报文生成并填充到读写报文队列、解析返回报文2。通过发送与解析包里的初始化虚设备函数，将数据库中的所有虚设备信息生成对应的虚设备对象填充到虚设备队列中。发送和解析包含有根据虚设备向读报文队列添加对应的读报文方法、根据写指令生成写指令报文并添加到写报文队列的方法、根据虚设备解析对应的读写报文的方法等。通过调用这些方法，使读写报文的生成、

添加，结果报文的解析更加方便。

4 读写报文的添加模块与通道线程设计

4.1 读写报文的添加模块

读报文添加通过虚设备调用发送与解析包中的相应方法，直接将该虚设备生成读指令报文并添加到读报文队列中等待发送。写指令报文根据写指令队列中写指令参数生成，并将对应的写报文添加到写报文队列。写指令中记录写操作的位置信息、数据长度和写数据的值等参数。

本文改进写报文队列的添加机制，改进部分主要体现在读报文队列的添加机制。通过在每个虚设备中定义扫描级别字段，不是简单轮询虚设备后立即调用相应方法向读报文队列中添加相应的读报文，而是在轮询过程中根据扫描级别的设定，使扫描级别等级越高（数值越低）的虚设备添加读报文的频率越高，从而提高实时性要求较高的数据的读写效率。

读写报文的添加规则：首先，在读报文队列没满且读指令队列中没有读指令时，轮询虚设备队列中的虚设备；轮询过程中，轮询到扫描级别为1000的虚设备时，调用发送与解析包中的方法，把对应的读报文依次添加到读指令队列中，此类数据只从现场读取一次；然后，用计数器记录轮询虚设备队列的次数，初始值为1；最后，在读报文队列没满的情况下反复轮询虚设备队列中的虚设备，若计数器数值是轮询虚设备扫描级别数值的倍数且扫描级别不为1000或2000时，分别调用发送与解析包中的方法，把对应的读报文依次添加到读指令队列中；轮询到扫描级别为2000的虚设备时，因该虚设备的数据为定时读取，先看虚设备中的超时时间，判断上次发送时间与系统时间之差是否大于等于报文中标记的超时时间，若大于

等于，则调用发送与解析包中的方法，把对应的读报文依次添加到读指令队列中；若小于，则跳过该虚设备继续轮询下一个虚设备。当写指令队列中存在写指令时，调用发送与解析包中的方法，把对应的写报文依次添加到写指令队列中。

4.2 通道线程设计

通道线程主要完成的工作包括：把读写报文队列中的报文依次发送到具体设备中（PLC），并接收设备返回的结果报文；调用发送与解析包解析返回的数据并置于共享内存中待用；当通信出现问题时，进行日志书写。通道线程的执行流程图如图 4 所示。

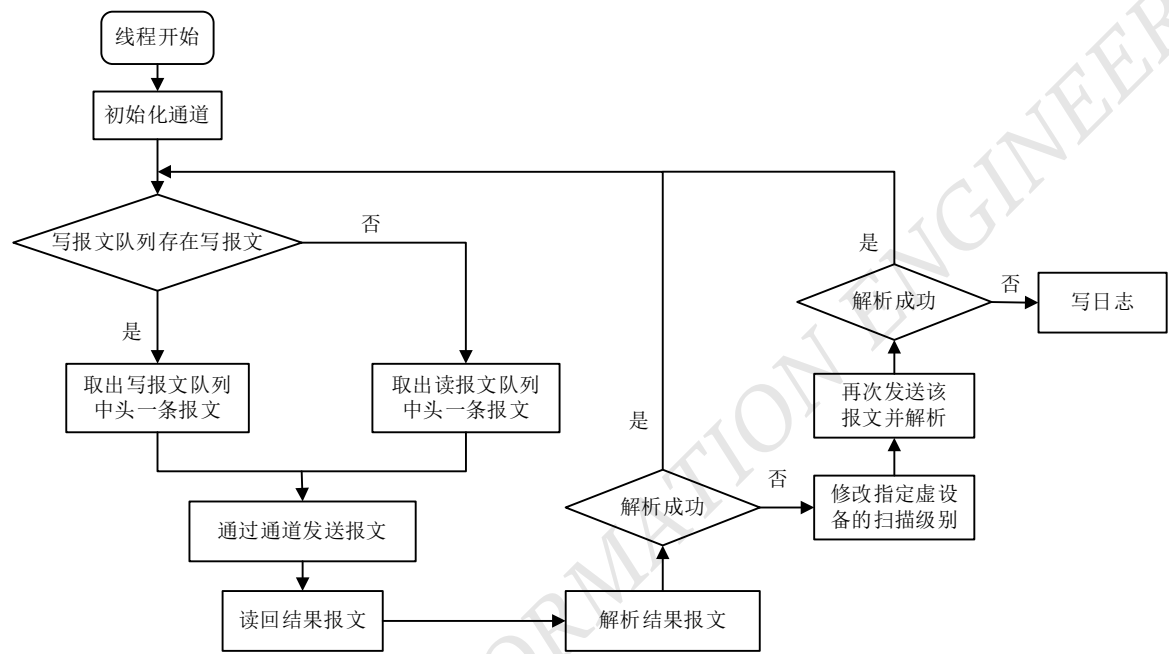


图 4 通道线程的执行流程图

首先，开启一个线程，初始化通道与 ISO_TP 连接；接着，判断写报文队列中是否有写报文，若存在写报文，则从写报文队列中取出第一个写报文，并根据该写报文写指令中的通道信息，把该报文发送到指定设备，在接收到返回的结果报文后，调用发送与解析包解析是否写成功；若写报文队列为空，则取出读报文队列中的第一个读报文，并根据该读报文虚设备中的通道信息，把该读报文发送到指定设备，设备返回结果报文后，通过发送与解析包解析具体数据放置于共享内存中待用。

解析过程中由于某些不确定因素，在发送读写报文后，可能出现较长时间没收到返回的结果报文或返回的结果报文校验不成功现象。若出现上述情况，将该读写报文重新发送到目标设备。若通信还是异常，为不影响其他报文发送，合理分配通信时间，则将该

指令报文的扫描级别修改为 2000（定时读取）。一旦通信正常后，则恢复原来的扫描级别。这样在轮询时通信不会进入异常等待状态，从而提高通信效率。

5 通信结果分析

首先，通过变量模块定义通信变量；然后，通过虚设备依次定义通信变量位于 PLC 数据块中的具体位置信息，并初始化虚设备、虚设备队列、读指令队列、写报文队列和读报文队列；最后，导入发送与解析包，开启通道线程。此时 PLC 与 PC 端的实时通信完成整体搭建，PLC 与 PC 端通信实时状态图如图 5 所示。

由图 5 的发送栏可知：不同的虚设备发送指令包的数目存在一定的差别，从而得出数据读取的频率可以通过配置进行改变。

设备	连接设备	发送	丢包-错误	服务器	最后	提示
配方交互BOOL	✓ 1	57286	1-0	192.168.12.2-0-1	19:42:10	连接成功
配方INT1	✓ 2	4	0-0	192.168.12.2-0-1	17:44:42	连接成功
配方INT2	✓ 3	1	0-0	192.168.12.2-0-1	16:55:16	连接成功
配方INT3	✓ 4	1	0-0	192.168.12.2-0-1	16:55:16	连接成功
配方INT4	✓ 5	1	0-0	192.168.12.2-0-1	16:55:16	连接成功
配方INT5	✓ 6	1	0-0	192.168.12.2-0-1	16:55:16	连接成功
配方INT6	✓ 7	9477	0-0	192.168.12.2-0-1	19:42:10	连接成功
配方INT7	✓ 8	9415	0-0	192.168.12.2-0-1	19:42:10	连接成功
配方INT8	✓ 9	9415	0-0	192.168.12.2-0-1	19:42:10	连接成功
配方REAL1	✓ 10	10002	0-0	192.168.12.2-0-1	19:42:10	连接成功
配方REAL2	✓ 11	9848	0-0	192.168.12.2-0-1	19:42:10	连接成功
配方REAL3	✓ 12	9848	0-0	192.168.12.2-0-1	19:42:10	连接成功
配方REAL4	✓ 13	9848	0-0	192.168.12.2-0-1	19:42:10	连接成功
配方REAL5	✓ 14	9847	0-0	192.168.12.2-0-1	19:42:10	连接成功
配方REAL6	✓ 15	9847	0-0	192.168.12.2-0-1	19:42:10	连接成功
配方REAL7	✓ 16	9846	0-0	192.168.12.2-0-1	19:42:09	连接成功
配方REAL8	✓ 17	9846	0-0	192.168.12.2-0-1	19:42:10	连接成功
配方REAL9	✓ 18	9846	0-0	192.168.12.2-0-1	19:42:10	连接成功
QC检测值INT	✓ 19	1	0-0	192.168.12.2-0-1	16:55:17	连接成功
配方INT9	✓ 20	3	0-0	192.168.12.2-0-1	17:44:42	连接成功
配方INT10	✓ 21	1	0-0	192.168.12.2-0-1	16:55:17	连接成功
当前步骤号	✓ 22	9846	0-0	192.168.12.2-0-1	19:42:10	连接成功
PDA交互BOOL	✓ 23	28143	1-0	192.168.12.2-0-1	19:42:10	连接成功
PDA交互INT	✓ 24	9850	0-0	192.168.12.2-0-1	19:42:10	连接成功
PDA交互REAL	✓ 25	14071	0-0	192.168.12.2-0-1	19:42:10	连接成功

图5 通信连接状态图

经过多次现场测试,得到的PLC与PC端的实时通信测试结果如表3所示。

表3 PLC与PC端的实时通信测试结果

编号	指标	结果
1	丢包率	0.90%
2	错误率	0%
3	数据读取频率是否可设置	是
4	连接成功率	99.8%

综合以上数据分析可得:PLC与PC端的实时通

信在网络与设备状态良好的情况下,丢包率与错误率都较低;丢包、错误与连接失败的主要原因是现场网络在短时间内出现延迟或网速不稳定。

6 结语

本文根据精细化工流程控制系统中数据对实时性要求存在差异的特点,设计PLC与PC端的通信架构,并实现了虚设备模块、变量定义模块、发送与解析模块、读写报文的添加模块和通道线程,从而使PLC端的数据根据系统设定进行有差异地读取,进而合理配置资源,提高通信效率。

参考文献

- [1] 王敏,李峰.精细化工行业发展现状及趋势[J].云南化工,2018,45(10):21-22.
- [2] 常一帆.工业自动化控制的现状及未来发展趋势[J].中国管理信息化,2016,19(12):177.
- [3] 李占国.化工企业液位自动化控制系统设计与实现[J].机电信息,2013(12):153,155.
- [4] 李建民,熊诗波,魏晋宏.西门子S7-200与PC实时通讯的实现方法[J].太原理工大学学报,2003(4):465-467.
- [5] 贾涛.西门子S7-200以太网通讯协议研究[J].电子技术与软件工程,2014(24):30-32.
- [6] 董青青.基于TCP协议的PC与西门子S7-1200PLC通信研究[J].电子测试,2019(19):76-77,79.

Communication Technology for Fine Chemical Process Control

He Xiaodong¹ Du Hongtao¹ Huang Jiaming²

(1.Zhuhai Longtec., Ltd, Zhuhai 519090, China

2.College of Science and Engineering of Jinan University, Guangzhou 510632, China)

Abstract: Network real-time communication is an important part of fine chemical process control. Taking the fine chemical process control system of a production workshop as the background, according to the production demand, the communication architecture between PC and PLC is designed, and the message sending and receiving mechanism is optimized, so that the PLC data can be read differently according to the system setting frequency, so as to improve the communication efficiency and production efficiency. This method can be used for reference in process control of small and medium-sized fine chemical enterprises.

Key words: process control; real-time communication; message sending and receiving mechanism

作者简介:

何晓东,男,1970年生,本科,高级工程师,主要研究方向:工业自动化、信息化系统规划。E-mail: hexiaodong@longtec.com

杜红涛,男,1977年生,本科,工程师,主要研究方向:工业自动化、信息化系统研发。E-mail: duhongtao@longtec.com

黄嘉明,男,1995年生,本科,硕士,主要研究方向:网络通信与信息处理。E-mail: 290045461@qq.com