网络编程作了相应的阐述. 文献[7]设计了一种基于IEC60870-5-104 规约的硬件通信模块平台, 实现了规约在工业通信领域的应用. 文献[8–10]分别介绍了规约在光伏电站、变电站辅助系统以及水电厂中的应用.

目前, 基于 IEC60870-5-104 规约的通信技术的研究渐渐趋于成熟, 然而随着工业标准规范的提高, 不同场合中的实际需求给系统软件的开发和升级不断地提出了难题. 综上研究发现, 在系统软件的设计过程中对于系统动态配置技术和海量数据传输技术仍然缺乏深入的探讨. 考虑到在实际应用中控制站和被控站会根据不同情况进行扩展和变动, 系统动态配置技术的研究能够很好地解决这个问题, 增加了系统的兼容性和开放性. 此外, 文件传输技术能够解决大部分远动系统中存在的海量数据信息的发布问题, 适应了多种场合中数据信息繁杂的情况.

2 系统概述

2.1 系统结构

图 1 显示了海底电缆综合在线监测系统的一般结构, 被控站 (服务器端) 的监测设备将采集到的数据存储在数据库服务器中, 等待控制站 (客户端) 的数据召唤.

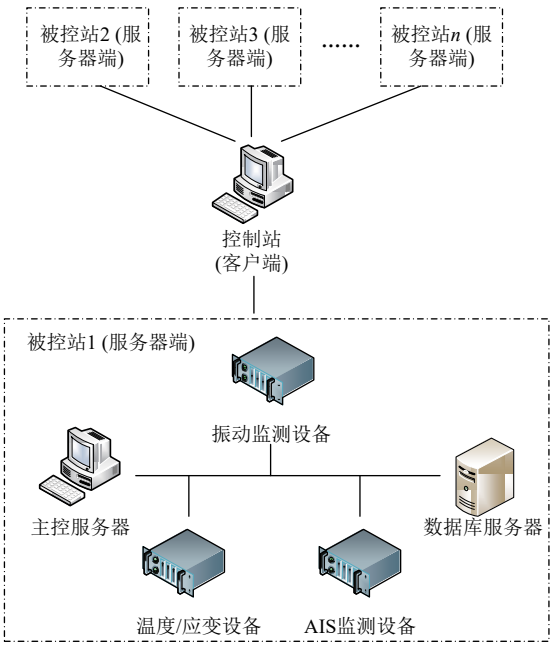

图 1 海底电缆综合在线监测系统

2.2 数据类型

应用于该系统的数据按其类型和数量的大小大致可以根据表 1 所示进行划分. 其中单一类型、数量小的数据可以通过 IEC60870-5-104 规约中的类型标识 TypeID=9(归一化遥测值), 11(标度化遥测值), 13(短浮点遥测值) 等 APDU 数据报文进行传输. 报警和 AIS 这类数据类型比较复杂, 包含整型、字符型、浮点型等多种数据类型. 针对这种类型复杂的数据信息, 本文考虑将不同类型的数据信息组合成字符串, 再根据配置好的信息对象地址用文件进行传输.

表 1 需要传输的数据类型

	单一类型数据	复杂类型数据
数据量小	电能、护层监测、设备状态	报警、AIS
数据量大	温度、应变、扰动	

对于温度、应变、扰动这些单一类型但是数量比较大的数据, 利用 IEC60870-5-104 规约定义的 APDU 进行数据传输有一定的局限性, 据此本文也考虑采用文件形式进行传输.

3 IEC60870-5-104 规约介绍

IEC60870-5-104 规约采用标准传输协议子集的 IEC60870-5-101 网络访问, 用于网络通信中的数据传输. 它规定将 IEC60870-5-104 的应用层与 TCP/IP 提供的传输功能相结合, 采用平衡方式通信, 即通信双方都可以发起信息传输, 一旦链路建立成功, 变化信息除了响应召唤应答还可以主动发送而无需等待查询. 同时规约详细定义了应用规约控制信息 (APCI) 以及三种格式报文 (I、S、U) 的用途和使用方法, 并且规定了 TCP 连接的端口号等重要参数.

图 2 所示是 IEC60870-5-104 规约对于 APDU 的定义, 它包括 APCI 和 ASDU 两个部分, APCI(应用规约控制信息) 定义了数据流的起点、APDU 的长度和控制域. 控制域定义了保护报文不致丢失和重复传送的控制信息、报文传输的启动/停止,以及传输连接的监视等信息. IEC60870-5-104 规约在延续了 IEC60870-5-101 规约中 ASDU(应用服务数据单元) 内容的基础上, 扩展了相应的部分, 定义了数据传输过程中信息的类型、传送原因、公共地址和信息对象地址等信息.

IEC60870-5-104 规约定义了两个方向上用于传输不同报文的信息类型标识, 分别是监视方向 (被控站到控制站) 的过程信息和系统信息, 以及控制方向 (控制站到被控站) 的过程信息和系统信息. 基于 IEC60870-5-104 规约的主要通信过程有: TCP 的连接建立和站初始化、首次握手启动连接、总召唤、对时、累计量 (电度) 总召唤以及遥控/遥调过程.

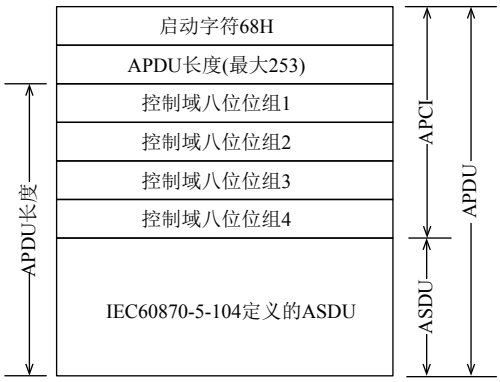

图 2 远动配套标准的 APDU 定义

4 系统建模分析

4.1 系统层次结构

图 3 所示为基于 IEC60870-5-104 规约的数据发布系统的层次结构, 主要分为伺服应用、协议处理和数据媒介三个层次.

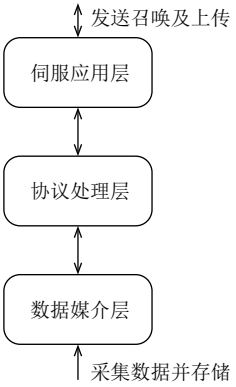

图 3 基于 IEC60870-5-104 规约的数据发布系统的层次结构

(1) 伺服应用层: 作为被控站的最高层, 在启动连接后伺服应用层一直处于等待监听的状态, 当接收到来自控制站数据请求的报文后开始向控制站发送由数据媒介层提取出来的数据.

(2) 协议处理层: 系统的中间层, 主要完成基于 IEC60870-5-104 规约的底层动态配置和数据处理功能, 针对伺服应用层发来的数据请求报文进行解析, 同时进行相关的数据库操作.

(3) 数据媒介层: 该层存储监测设备采集的数据信息. 每个监测平台都有相应的数据库, 监测系统将采集到的数据信息不断地刷新填入到每个数据库每张表相应的字段中. 当收到召唤开始传输数据时, 被控站将数据库中的数据提取出来填入到 APDU 中并赋予其相应的地址进行传输, 考虑到存储容量和实时性的问题, 每个数据库也会作定期地刷新删除.

4.2 系统运行流程

启动连接后系统开始读取配置, 此时被控站处于监听并等待召唤状态, 若在规定的时间范围内没有收到控制站发来的召唤报文命令则判定为等待超时, 须重新连接. 当被控站收到了控制站发来的召唤报文命令后便开始对其进行解析并组织数据类型及地址, 从而从数据库中提取相应的数据并按一定频率发送至控制站, 待所有数据发送完之后被控站将发送结束召唤的报文命令终止数据传输.

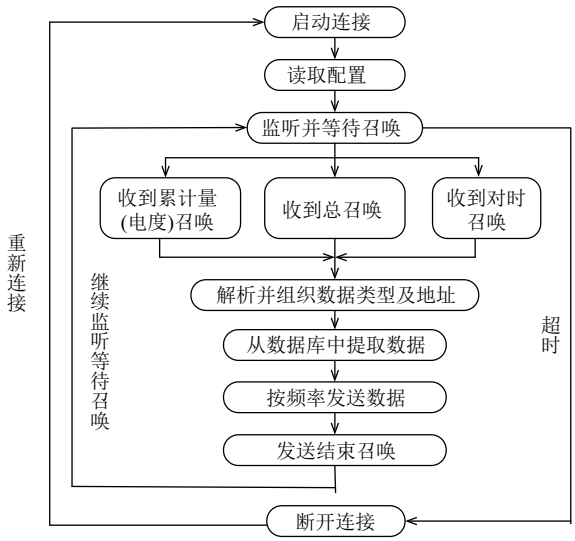

图 4 系统运行流程

4.3 系统主要线程设计

图 5 所示为系统的主要线程设计, 数据库连接线程主要实现数据库的连接及相关操作, 数据发送和接收显示线程主要实现控制站和被控站的数据交互. 通信双方在启动连接后开始读取配置, 随后进入等待监听状态, 当通信一方接收到数据库中读取的数据后开始对其进行打包整理, 最后发送至另一方解析并显示.

5 关键技术及解决方案

5.1 控制站和被控站的动态配置技术

控制站和被控站的动态配置是远端发布系统中非常重要的环节, 它解决了控制站和被控站对于每个物理量、数据类型及其地址分配的约束问题, 使得通信双方的数据传输有章可循.

(1) 单一类型数据的动态配置

类型单一且数量比较小的数据信息对象可以通过 IEC60870-5-104 规约定义的 APDU 进行数据传输, 为此需要设计信息对象、地址以及在数据库中的存储位置之间的映射关系. 设计的映射方案如表 2 所示, 信息量的个数取决于信息数量的大小, 在数据库 SeaCableMonitor (存储位置: D:\MySQL\SeaCableMonitor)中建有三张表 Current、ProtectiveLayer 和 State, 分别用于存储电能、护层监测和设备状态三种数据信息, 每张表分别包含若干记录 (行) 和字段 (列), 记录显示每条通道的电缆数据信息, 字段存储某一时刻下的电缆编号、位置、时间以及信息量等数据信息, 监测设备将某一时刻采集到的数据存于每张表相应的字段下. 当被控站收到数据请求时, 从相应表的字段中取出并赋予信息对象地址, 从而打包发送至控制站.

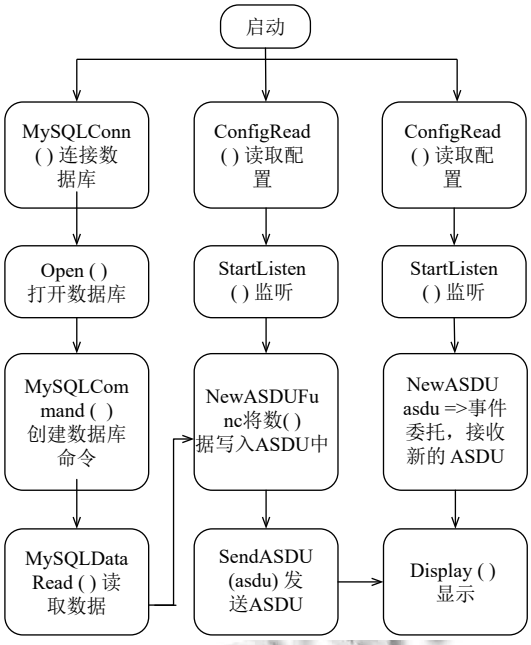

图 5 系统主要线程设计

表 2 信息对象地址分配

信息对象名称	对应地址 (十六进制)	信息量个数	表	字段	数据类型
电能	000001H~005000H	20 480	Current	电能	浮点型
护层监测	005001H~00A000H	20 480	Protective-Layer	护层监测	浮点型
设备状态	00A001H~00A200H	512	State	设备状态	整型

(2) 文件传输的动态配置

文件传输的动态配置需要解决的问题是生成数据文件的存储位置以及建立文件的节名和信息对象之间的映射关系, 文件存储在 D:\SeaCableMonitor\Files 目录下, 表 3 显示了文件节名信息对象的映射关系.

表 3 文件名与信息对象映射关系

文件节名	信息对象
01	温度
02	应变
03	扰动
04	报警
05	AIS
…	…

综合考虑可扩展、互操作、可视化等多种特性,本文选取 XML(扩展标记语言) 实现以上动态配置. XML 是一种简单的数据存储语言, 当控制站或者被控站需要扩展或者改变时, 只要修改配置文件而不需要处理繁杂的源代码. 下面的代码显示了信息对象及其地址的配置过程:

```
<MsgConfig>
  <MsgType>信息类型
  < TypeId Code='9'>归一化遥测值</Code>
  ……
  </MsgType>
  <MsgAddr>信息对象地址
  <Current_Begin addr='0x1'>电能信息起始地址</Current_Begin>
  <Current_End addr='0x5000'>电能信息结束地址</Current_End>
  ……
  </MsgAddr>
</MsgConfig>
```

5.2 海量数据及复杂类型数据的文件传输技术

IEC60870-5-104 规约中定义的信息体地址的范围是 1~65 534, 即最大能容纳 65 534 个数据, 而 ASDU 的最大长度是 249(APDU 最大值=255 减去启动和长度八位位组), 这样信息体的字节数就很可能会超过 ASDU 的最大长度, 显然无法进行海量数据传输. 此外, 报警和 AIS 这类数据信息包含了整型、字符型、浮点型等多种数据类型, 导致了数据传输过程中信息体的字节数不固定, 无法进行地址分配. 鉴于以上两种情况, 本文考虑采用文件传输的方案.

文件传输用于远动系统中信息体的字节数超过 ASDU 规定的最大长度的情况, 以分段的形式将数据

信息传送到目的地. 两个方向上传输的文件结构相同, 通常一个文件包含若干个节, 一个节包含若干个段, 两个方向按照段的顺序进行传输. 在远动系统中, 文件可以双向传输, 表 4 所示为 IEC60870-5-104 规约定义的用于文件传输的类型标识.

表 4 文件传输的类型标识

报文类型 (十进制)	报文语意	编码
120	文件已准备好	F_FR_NA_1
121	节已准备好	F_SR_NA_1
122	召唤目录, 选择文件, 召唤文件, 召唤节	F_SC_NA_1
123	最后的节, 最后的段	F_LS_NA_1
124	确认文件, 确认节	F_AF_NA_1
125	段	F_SG_NA_1
126	目录	F_DR_TA_1
127	保留	

监视方向 (被控站到控制站) 的文件传输主要用于通知控制站已发生事件并已登录大量数据. 在开始进行文件传输之前, 被控站须向控制站发送一个文件目录 DIRECTORY PDU F_DR, 将文件数量、登录时间和事件类型等信息以 PDU 的形式告知控制站. 收到目录 PDU 后, 控制站发送一个 SELECT_FILE PDU F_SC 通知被控站开始选择文件. 此时被控站返回 FILE_READY PDU F_FR 表示文件已准备好, 可以进行文件召唤. 接下来被控站根据文件结构将文件逐节逐段地上传至控制站. 待所有文件传输结束后, 被控站将已成功传输文件的数据记录删除, 为新文件腾出空间. 控制方向 (控制站到被控站) 的文件传输主要用于下载参数表或程序, 控制站安排传输数据文件的类型、数量和规模, 不需要传输目录. 表 5 和表 6 所示为 IEC60870-5-104 规约定义的文件传输的目录 ASDU(TypeID=F_DR_TA_1) 和段 ASDU(TypeID=F_SG_NA_1) 的定义.

表 5 文件传输的目录 ASDU 定义 (类型标识: F_DR_TA_1)

ASDU 定义	字节数
类型标识 (TYP)	1
可变结构限定词 (VSQ)	1
传送原因 (COT)	2
ASDU 公共地址 (CA)	2
信息对象地址 (IOA)	3
文件名或子目录名 (NOF)	2
文件长度 (LOF)	3
文件的状态 (SOF)	1
文件建立的时间 (CP56Time2a)	7

表 6 文件传输的段 ASDU 定义 (类型标识: F_SG_NA_1)

ASDU 定义	字节数
类型标识 (TYP)	1
可变结构限定词 (VSQ)	1
传送原因 (COT)	2
ASDU 公共地址 (CA)	2
信息对象地址 (IOA)	3
文件名 (NOF)	2
节名字 (NOS)	1
段的长度 (LOS)	1
段	n

注意: (1) 文件传输时的信息对象地址不表示任何信息, 统一设置成 000000.

(2) 段的长度最大值在 234(当链路域、数据单元标识符合信息对象地址为最大长度) 和 240(当链路域、数据单元标识符合信息对象地址为最小长度) 之间.

6 实验用例

本文以某海上风电场在线监测系统工程项目为应用实例, 传输海缆某一时刻采集到的电能数据以及温度数据.

6.1 单一类型数据的传输

以单个电能数据的传输为例, 设置配置参数信息如表 7 所示.

表 7 单个电能数据传输配置信息

配置信息	参数	解释
TypeID	9	类型标识为归一化遥测值
InformationObjectAddress	1	信息对象地址为 1
Quantity	1	信息数量为 1
TransmitionCause	20	传送原因为响应站召唤
TransmissionTime	60	传输频率为 60
CommonAddress	1	公共地址为 1

系统启动读取配置完成之后等待数据召唤, 利用 Wireshark 软件对通信过程进行网络抓包分析得到控制站收到的报文如表 8 所示.

从表 8 中可以看到传输的归一化遥测值的编码是 10a1(16 进制), 如果要得到具体的传输值则需要通过给定的参数进行进一步计算, 例如假设满码值为 5000 A, 则传输值为:

$$\frac{4257\,(10A1H)}{32768\,(8000H)}\times 5000A = 649.6A \qquad (1)$$

得到的电能数据为 649.6 A.

6.2 文件数据的传输

以系统某一次温度数据文件的传输为例, 表 9 为其参数配置信息, 从中可以知道, 文件的长度为 750 KB,

节的长度为 7680 B, 段的长度为 120 B, 则节和段的数量分别为:

$$\frac{750\times1024}{7680}=100(\text{节}) \quad (2)$$

$$\frac{7680}{120}=64(\text{段}) \quad (3)$$

表 8 控制站接收类型标识 TypeID=9 的归一化遥测报文

报文	报文解释
68	启动
10	长度
0600	发送序号
0200	接收序号
09	类型标识 9, 带品质描述的遥测
01	可变结构限定词, 一个遥测数据
1400	传输原因 14, 响应总召唤
0100	公共地址
010000	信息对象地址, 从 0x0001 开始第 0 号遥测
a110	遥测值为 10a1
00	品质描述词

表 9 温度数据文件传输配置信息

配置信息	参数	解释
TypeID	125	类型标识为文件段传输
TransmitionCause	13	传送原因为文件传输
CommonAddress	1	公共地址为 1
InformationObjectAddress	0	信息对象地址为 0
FileName	1	文件名为 1, 温度文件
FileLength	750	文件长度为 750KB
SectionName	1	节名为 1
SectionLength	7680	节的长度为 7680B
SegmentLength	120	段长度为 120B
TransmissionTime	60	传输频率为 60

同样用 Wireshark 软件对该温度数据文件传输过程进行网络抓包分析, 可以得到报文如下 (仅显示传输的第一节第一段的报文):

表 10 显示了文件传输中控制站接收到类型标识 TypeID=7 d 的段报文, 根据配置信息可以解析出控制站收到了文件名为 1, 节名为 1(温度) 以及段内容为 1 的文件数据信息.

7 结束语

本文深入分析了 IEC60870-5-104 规约的结构模型和通信过程, 设计并实现了基于该规约的海底电缆综合在线监测系统数据远端发布系统, 针对其中存在的系统动态配置和海量数据传输关键技术作了分析与研究, 最后通过实验用例验证了该系统的可行性. 本文的研究结果适用于更宽泛的电力系统场合以及更丰富的数据类型传输, 具有可观的应用价值.

表 10 文件传输中控制站接收类型标识 TypeID=7d 的段报文

报文	报文解释
68	启动
12	长度
0600	发送序号
0200	接收序号
7 d	类型标识 7 d, 段
01	可变结构限定词
0d00	传输原因, 文件传输
0100	公共地址
000000	信息对象地址
0100	文件名, 温度数据文件
01	节名
78	段长度
01	段

参考文献

1 全国电力系统控制及其通信标委会. DL/T 634.5104–2002 远动设备及系统 第 5104 部分: 传输规约 采用标准传输协议子集的 IEC60870–5–101 网络访问. 北京: 中华人民共和国电力出版社, 2002.

2 中华人民共和国国家质量监督检验检疫总局. GB/T 18657.5–2002 远动设备及系统 第 5 部分: 传输规约 第 5 篇: 基本应用功能. 北京: 中国标准出版社, 2002.

3 中华人民共和国国家质量监督检验检疫总局. GB/T18657.4–2002 远动设备及系统 第 5 部分: 传输规约 第 4 篇: 应用信息元素的定义和编码. 北京: 中国标准出版社, 2002.

4 全国电力系统控制及其通信标委会. DL/T 634.5101–2002 远动设备及系统 第 5101 部分: 传输规约 基本远动任务配套标准. 北京: 中国电力出版社, 2002.

5 赵渊, 沈智健. 基于 TCP/IP 的 IEC60870-5-104 远动规约在电力系统中的应用. 电网技术, 2003, 27(10): 56–60, 71. [doi: 10.3321/j.issn:1000-3673.2003.10.014]

6 鞠阳, 张惠刚. IEC60870-5-104 远动规约的设计及其应用. 继电器, 2006, 34(17): 55–58, 66.

7 孙俊男, 刘明哲, 徐皑冬, 等. 基于 IEC60870-5-104 远动规约的 PLC 通信模块的设计与实现. 高技术通讯, 2016, 26(4): 389–395. [doi: 10.3772/j.issn.1002-0470.2016.04.009]

8 陶学军, 徐奉友, 王艳领. IEC 60870-5-104 协议在光伏电站中的应用. 机电工程技术, 2014, 43(3): 40–44. [doi: 10.3969/j.issn.1009-9492.2014.03.012]

9 韩小军, 蔡东升, 黄琦, 等. 基于 IEC104 远动规约的智能变电站辅助平台测试系统设计与实现. 电测与仪表, 2014, 51(14): 104–109. [doi: 10.3969/j.issn.1001-1390.2014.14.023]

10 洪林, 陈鹏. 基于 IEC104 规约的水电厂远动通信实时性及安全性的优化措施. 水电自动化与大坝监测, 2014, 38(3): 37–39, 56. [doi: 10.3969/j.issn.1671-3893.2014.03.010]