RTU 上行通信 IEC104 协议简述

目录

1. RTU IEC104 协议基本参数

- 基于 IEC60870-5-104 协议；
- 最大帧长度为 255Byte；
- 帧间隔：50ms；
- TCP/IP 网络通信端口号 2404；
- 采用平衡传输，每个节点（包括主站、厂站）均可以启动报文发送。

2. 应用规约控制单元（APDU）格式

- 应用规约数据单元：APDU(Application protocol data unit)
- 应用规约控制信息：APCI(Application protocol control information)
- 应用服务数据单元：ASDU(Application protocol control unit)

<table>
<tr><td>起始字 0X68</td><td rowspan="6">APCI</td><td rowspan="7">APDU</td></tr>
<tr><td>APDU 长度</td></tr>
<tr><td>控制域 1</td></tr>
<tr><td>控制域 2</td></tr>
<tr><td>控制域 3</td></tr>
<tr><td>控制域 4</td></tr>
<tr><td>IEC 60870-5-101 和 IEC 60870-5-104 定义的 ASDU</td><td>ASDU</td></tr>
</table>

2.1 应用规约控制信息（APCI）格式

为了检出 ASDU 的启动和结束，每个 APCI 包括下列的定界元素：一个启动字符，ASDU 的规定长度，以及控制域（见下图）。可以传送一个完整的 APDU（或者，出于控制目的，仅仅是传送 APCI 域）。

<table>
<tr><td>起始字 68H</td><td rowspan="5">APCI</td></tr>
<tr><td>APDU 长度</td></tr>
<tr><td>控制域八位位组 1</td></tr>
<tr><td>控制域八位位组 2</td></tr>
<tr><td>控制域八位位组 3</td></tr>
<tr><td>控制域八位位组 4</td></tr>
</table>

启动字符 0X68 定义了数据流中的起点。APDU 的长度域定义了 APDU 体的长度，它包括 APCI 的四个控制域八位位组和 ASDU。第一个被计数的八位位组是控制域的第一个八位位组，最后一个被计数的八位位组是 ASDU 的最后一个八位位组。ASDU 的最大长度限制在 249 以内，因为 APDU 域的最大长度是 253（APDU 最大值=255 减去启动和长度八位位组），控制域的长度是 4 个八位位组。

控制域定义了保护报文不至丢失和重复传送的控制信息、报文传输启动/停止、以及传输连接的监视等控制信息。控制域的计数器机制是根据 ITU-T X.25 标准中推荐的 2.3.2.2.1 至 2.3.2.2.5 来定义的。

2.1.1 I 帧 APCI 格式

I 帧的控制域包含发送序列号和接收序列号两个参数，参数在控制域中的格式如下图所示。两个序列号在每个 APDU 和每个方向上都应按顺序加一。发送序列号和接受序列号在 0~32767 之间循环。发送方增加发送序列号而接受方增加接收序列号。接收站认可连续正确接收的一个 APDU 或者多个 APDU，将最后一个正确接收的 APDU 的发送序列号作为接收序列号返回。这个接收序列号是对所有发送序列号小于或等于该号的 APDU 的有效确认。如只在一个方向进行较长的数据传输，就得在另一个方向发送 S 格式认可这些 APDU。这种方法应该在两个方向上采用。在创建一个 TCP 连接后，发送和接收序列号都被设置成 0。

控制域	**D7**	**D6**	**D5**	**D4**	**D3**	**D2**	**D1**	**D0**
控制域 1	发送序列号 N(S) LSB							0
控制域 2	发送序列号 N(S) MSB							
控制域 3	接收序列号 N(R) LSB							0
控制域 4	接收序列号 N(R) MSB							

2.1.2 S 帧 APCI 格式

S 格式具有计数的监视功能，S 格式帧为短帧，长度 6 个字节。接收方接收到 I 帧数据，但本身没有信息要发送的情况下，S 帧用于确认接收到对方的帧。其控制域格式如下图所示：

控制域	D7	D6	D5	D4	D3	D2	D1	D0
控制域 1	0						0	1
控制域 2	0							
控制域 3	接收序列号 N(R) LSB							0
控制域 4	接收序列号 N(R) MSB							

2.1.3 U 帧 APCI 格式

U 格式帧具有不计数的控制功能，长度为 6 个字节的固定帧长。用于控制报文。控制域格式如下图所示：

控制域	D7	D6	D5	D4	D3	D3	D1	D0
控制域 1	TEST		STOP		START		1	1
	C	V	C	V	C	V		
控制域 2	0							
控制域 3	0							
控制域 4	0							

C：表示确认

V：表示生效

U 格式帧使用到以下三种命令：

1) 启动 U 帧，用于启动应用层传输控制命令：
   - 主站发送：680407000000
   - 从站返回：68040B000000
2) 停止 U 帧，用于停止应用层传输控制命令：
   - 主站发送：680413000000
   - 从站返回：680423000000
3) 测试 U 帧，双方均无发送时，维持链路活动状态控制命令：
   - 主站发送：680443000000
   - 从站返回：680483000000

2.2 应用服务数据单元（ASDU）格式

IEC 60870-5-3 描述了远动系统传输帧中的基本应用数据单元，并定义了用于配套标准中的应用服务数据单元(ASDU),其结构如下图所示：

类型标识	数据单元标识符	ASDU
可变结构限定词		
传输原因 LSB		
传输原因 MSB（0X00）		
公共体地址 LSB		
公共体地址 MSB		
IEC 60870-5-104 定义的一个或多个信息对象	信息对象	

应用服务数据单元(ASDU)由数据单元标识符和一个或多个信息对象所组成。数据单元标识符在所有应用服务数据单元中常有相同的结构，一个应用服务数据单元中的信息对象常有相同的结构和类型，它们由类型标识域所定义。

2.2.1 类型标识：

类型标识定义了后续信息对象的结构、类型和格式。在 IEC60870-5-101 7.2.1.1 中定义类型标志<136..255>为特殊应用(专用范围)，因此自定义的类型标志选择此范围。结合油田实际传感器的需求，总结并将所有信息按照传感器进行分类，总结类型标志如下表所示：

主站发送的类型标识列表

类型标识	功能	类别	所属传感器	格式	备注
0X64	总召唤	遥测	RTU	WORD	标准 IEC104 规约
0X65	电能召唤	电度	智能电表	WORD	
0X67	时钟同步	校时	RTU	CP56Time2a	
0X2D	单点遥控	遥控	RTU	BYTE	
0X31	设点命令，标度化值	遥调	RTU	WORD	
0X88	总召唤测量值	遥信/遥测	所有传感器	BYTE/WORD	非标（自定义）
0X89	召唤示功图数据	遥测	示功图数据	WORD	
0X8A	召唤电功图数据	遥测	电工图数据	WORD	
0X8B	召唤历史数据	遥测	RTU	WORD	
0X8C	召唤 RTU 参数	遥测	RTU	WORD	
0X8D	召唤传感器参数	遥测	所有传感器	WORD	
0X8E	召唤谐波数据	遥测	智能电表	WORD	
0X8F	召唤计量车数据	遥测	计量车	WORD	
0X90	召唤注采阶段数据	遥测	注采设备	WORD	
0X91	召唤所有功图数据	遥测	示功图、电工图	WORD	
0X92	召唤起井有功功率	遥测	RTU	WORD	
0X93	召唤井口回压数据	遥测	RTU	WORD	
0X94	召唤存储历史 SOE 数据	遥测	RTU	WORD	
0X95	召唤预留传感器数据	遥测	RTU	WORD	

从站返回信息帧的类型标识列表

类型标示	功能	备注
0X64	总召唤确认/结束	标准 IEC104 规约
0X65	电能召唤确认/结束	
0X67	对时确认	
0X2D	单点遥控返校、执行和撤销	
0X31	单点遥调返校、执行和撤销	
0X88	总召唤测量值确认/结束	非标
0X89	召唤示功图数据确认、上传/结束	
0X8A	召唤电功图数据确认、上传/结束	
0X8B	召唤历史数据确认、结束	
0X4D	历史遥测（带 CP56Time2a 时标）	
0X4F	历史遥信（带 CP56Time2a 时标）	
0X5C	历史电度（带 CP56Time2a 时标）	
0X5F	历史功图（带 CP56Time2a 时标）	
0X8C	召唤 RTU 数据确认、上传、结束	
0X8D	召唤传感器参数确认、上传、结束	
0X8E	召唤谐波数据确认、上传、结束	
0X8F	召唤计量车数据确认、上传、结束	
0X90	召唤注采数据确认、上传、结束	
0X91	召唤所有功图数据确认、结束（带 CP56Time2a 时标）	
0X92	召唤起井有功功率	
0X93	召唤井口回压数据	
0X94	召唤存储历史 SOE 数据	
0X95	召唤预留传感器数据	

2.2.2 可变结构限定词：

定义了信息元素的数目和信息体地址类型，长度一个字节。

D7	D6	D5	D4	D3	D2	D1	D0
SQ	Num						

说明：

- SQ=0：表示每个信息对象分别带有地址。应用服务数据单元可以由一个或者多个同类的信息对象所组成。
- SQ=1：表示同类的信息元素序列(即同一种格式测量值)。信息对象地址是顺序信息元素的第一个信息元素的地址。后续信息元素的地址是从这个地址起顺序加 1。
- Num：信息体的数目。

2.2.3 传输原因：

在应用服务数据单元（ASDU）中，其数据单元标识符的第三和第四个八位位组定义为传送原因。此 RTU 系统中目前第三个八位位组表示原因，第四个八位位组常 0 用于扩展，所使用的传输原因如下表所示：

主站发送的传输原因

传输原因	用法	备注
0X06	激活	
0X08	停止激活	

从站发送的传输原因

传输原因	用法	备注
0X03	突发	主动上送
0X05	被请求	
0X07	激活确认	
0X09	停止激活确认	
0X0A	激活停止	
0X2C	未知类型标识	
0X2D	未知传输原因	
0X2E	未知公共地址	
0X2F	未知信息对象地址	

2.2.4 公共体地址：

即 RTU 地址，长度 2 个字节，低位在前。

2.2.5 信息体地址：

即信息对象的地址，长度为 3 个字节，低字节在前。

3. 定时器定义

RTU 内部定时器的定义和操作如下表所示：

动作	T1	T2	T3
到时时间	15s	10s	20s
到时处理	断开链接	断开链接	发送 U 测
开启定时器条件	发送 U 测试帧	发送完所有 I 帧	建立连接
关闭定时器条件	接收 U 测试帧	收到 S/I 帧	链接断开
复位定时器条件	不发生复位	不发生复位	收到 I/S/U 帧

4. 未被确认的 I 帧最大数目 k 和最迟确认数目 W

参数	缺省值	注释
K	12	发送状态变量的最大不同的接收序号
W	8	接收 w 个 I 格式 APDUS 之后的最后的认可

主站（客户端）保证最多接收 8 帧 I 帧发送一帧 S 帧确认，并且在召唤命令发出并且接收到最后一帧 I 帧或者突发上送之后发送 S 帧确认。RTU 端当超过 K 个 I 帧得不到确认，或者最后一帧 I 帧超过 10s 得不到确认将断开链接，重新进入监听状态。

RTU 的测量信息包括 RTU 测量值信息、状态信息、报警信息及时间信息等，测量值信息包括：RTU 的 I/O 接口数据、COM4(第 3 路 RS485)接口的数据（最多 32 点）、ZigBee 无线传感器数据（最多 32 点）、COM3(第 2 路 RS485)接口的电表参数、COM2(第 1 路 RS485)的变频器数据、示功图数据、电流封闭曲线数据、有功功率封闭曲线数据、功率因数封闭曲线及电功图等数据。

5. 总召唤机制

总召唤过程：

1) 主站启动总召唤；

2) 从站以总召唤确认帧应答；

3) 从站生成并向主站发送遥信、遥测的总召唤报文，报文不包含时标；

4) 从站向主站发送总召唤结束报文。

帧序号	方向	类型标识	传输原因	说明	备注
1	主站--->从站	0X64	0X06	主站发起总召唤	
2	从站--->主站	0X64	0X07	从站返回总召唤确认	

3~5	从站--->主站	0X01	0X14	从站发送遥信信息	
6~n	从站--->主站	0X0B	0X14	从站发送遥测信息	
n+1	从站--->主站	0X64	0X0A	从站发送总召唤结束	

6. 电度总召唤机制

电度总召唤过程：

1) 主站启动电度总召唤；

2) 从站以电度总召唤确认帧应答；

3) 从站生成并向主站发送电度总召唤报文；

4) 从站向主站发送电度总召唤结束报文。

帧序号	方向	类型标识	传输原因	说明	备注
1	主站--->从站	0X65	0X06	主站发起电度总召唤	
2	从站--->主站	0X65	0X07	从站返回电度总召唤确认	
3~n	从站--->主站	0X0F	0X05	从站发送电度数据	
n+1	从站--->主站	0X65	0X0A	从站发送电度召唤结束	

7. 时钟同步机制

主站发对时报文，从站以报文的镜像确认。

帧序号	方向	类型标识	传输原因	说明	备注
1	主站--->从站	0X67	0X06	主站发送校时命令	
2	从站--->主站	0X67	0X07	从站返回校时结束	

8. 遥控机制

遥控分为三种情况处理：正常遥控、从站拒绝、主站撤销。

8.1 正常遥控

正常遥控过程：

1) 主站启动遥控帧；

2) 从站返回遥控反校；

3) 主站发送遥控执行；

4) 从站返回遥控结束。

帧序号	方向	类型标识	传输原因	QOS	说明	备注
1	主站--->从站	0X2D	0X06	0X80	主站发送遥控确认	
2	从站--->主站	0X2D	0X07	0X80	从站返回遥控反校	
3	主站--->从站	0X2D	0X06	0X00	主站发送遥控执行	
4	从站--->主站	0X2D	0X0A	0X00	从站返回遥控结束	

8.2 从站拒绝

从站拒绝遥控过程：

1) 主站启动遥控帧；

2) 从站返回遥控结束。

帧序号	方向	类型标识	传输原因	QOS	说明	备注
1	主站--->从站	0X2D	0X06	0X80	主站发送遥控确认	
2	从站--->主站	0X2D	0X0A	0X80	从站返回遥控结束	

8.3 主站撤销

主站撤销遥控过程：

1) 主站启动遥控帧；

2) 从站返回遥控反校；

3) 主站发送遥控撤销；

4) 从站返回遥控结束。

帧序号	方向	类型标识	传输原因	QOS	说明	备注
1	主站--->从站	0X2D	0X06	0X80	主站发送遥控确认	
2	从站--->主站	0X2D	0X07	0X80	从站返回遥控反校	
3	主站--->从站	0X2D	0X08	0X00	主站发送遥控撤销	
4	从站--->主站	0X2D	0X0A	0X00	从站返回遥控结束	

9. 遥调机制

9.1 正常遥调

正常遥调过程：

1) 主站启动遥调帧；

2) 从站返回遥调反校；

3) 主站发送遥调执行；

4) 从站返回遥调结束。

帧序号	方向	类型标识	传输原因	QOS	说明	备注
1	主站--->从站	0X31	0X06	0X80	主站发送遥调确认	
2	从站--->主站	0X31	0X07	0X80	从站返回遥调反校	
3	主站--->从站	0X31	0X06	0X00	主站发送遥调执行	
4	从站--->主站	0X31	0X0A	0X00	从站返回遥调结束	

9.2 从站拒绝

从站拒绝遥调过程：

1) 主站启动遥调帧；

2) 从站返回遥调结束。

帧序号	方向	类型标识	传输原因	QOS	说明	备注
1	主站--->从站	0X31	0X06	0X80	主站发送遥调确认	
2	从站--->主站	0X31	0X0A	0X80	从站返回遥调结束	

9.3 主站撤销

主站撤销遥调过程：

1) 主站启动遥调帧；

2) 从站返回遥调反校；

3) 主站发送遥调撤销；

4) 从站返回遥调结束。

帧序号	方向	类型标识	传输原因	QOS	说明	备注
1	主站--->从站	0X31	0X06	0X80	主站发送遥调确认	
2	从站--->主站	0X31	0X07	0X80	从站返回遥调反校	
3	主站--->从站	0X31	0X08	0X00	主站发送遥调撤销	
4	从站--->主站	0X31	0X0A	0X00	从站返回遥调结束	

10.非标召唤机制

非标数据召唤包括总召唤测量值、召唤示功图数据、召唤电功图数据、召唤历史数据、召唤 RTU 参数、召唤传感器参数、召唤谐波数据、召唤计量车数据、召唤注采阶段数据。

非标数据召唤采用标准 IEC104 协议总召唤的机制，根据油田的实际需要，测量值总召

唤采集需要频繁读取的信息，包括 RTU 内部的遥信信息。这样做可以减少上位机读取数据的压力，同时提高传输的效率。

类型标识见 2.2.1 的主站类型标识数据表，测量值总召唤过程如下：

1) 主站启动召唤；

2) 从站以确认帧应答；

3) 从站生成并向主站发送信息的报文，报文不包含时标；

4) 从站向主站发送结束报文。

帧序号	方向	类型标识	传输原因	说明	备注
1	主站--->从站	见 2.2.1 表	0X06	主站发送测量值总召唤	
2	从站--->主站	见 2.2.1 表	0X07	从站发送测量值总召唤确认	
3~n	从站--->主站	0X01	0X05	从站发送遥信信息	
n+1~m	从站--->主站	0X0B	0X05	从站发送遥测信息	
m+1	从站--->主站	见 2.2.1 表	0X0A	从站发送测量值总召唤结束	

11.变位遥信机制

召唤遥测过程：

1)从站主动上送变位遥信；

2)从站主动上送相应的遥测值。

帧序号	方向	类型标识	传输原因	说明	备注
1	从站--->主站	0X1E	0X03	从站发送变位遥信	带时标
2	从站--->主站	0X23/0X25	0X03	从站发送变位遥测信息	带时标

12.历史数据召唤机制

历史数据的召唤过程依然可以采用总召唤的机制来完成，网络通讯恢复后，主站可以正常采集数据，从站优先考虑正常的数据采集，当从站接收到历史数据采集命令后，从站按照上面的方式首先发送起始帧，然后发送历史数据信息帧，最后发送结束帧。如果没有历史数据，从站直接发送结束帧。

历史数据召唤过程：

1) 主站启动历史数据召唤

2) 从站以历史召唤确认帧应答

3) 从站生成并按照优先级发送遥信、遥测等历史数据报文，报文包含时标

4) 从站向主站发送总召唤结束报文

RTU 存在历史数据

帧序号	方向	类型标识	传输原因	说明	备注
1	主站--->从站	0X8A	0X06	主站发起召唤	带起始和结束时标
2	从站--->主站	0X8A	0X07	从站返回确认	
3~n	从站--->主站	0X1E/0X23/0X25	0X14	从站发送信息	带时标
n+1	从站--->主站	0X8A	0X0A	从站发送结束	

12.1 RTU 没有历史数据

帧序号	方向	类型标识	传输原因	说明	备注
1	主站--->从站	0X8A	0X06	主站发起召唤	带起始和结束时标
2	从站--->主站	0X8A	0X0A	从站发送结束	

上位机不发送历史数据召唤命令，RTU 不会主动上送历史数据。如果没有历史数据需要发送，RTU 在接收到历史数据采集命令后，直接发送结束帧。

13.地址分配

根据油田需求，频繁采集的测量值、示功图数据、电功图数据、谐波数据、计量车数据、注采阶段数据还可以在 0X4001~0X5000（遥测地址范围）内进行详细的地址范围区分。

信息类型	地址范围	备注
遥信	0X0001~0X1000	标准 IEC104 规约
测量值	0X4001~0X5000	
计量车数据	0X5001~0X5100	非标准（自定义）
注采数据	0X5101~0X5200	
谐波数据	0X5201~0X5400	
示功图数据	0X5401~0X5800	
电功图数据	0X5801~0X6000	
遥控	0X6001~0X6100	标准 IEC104 规约
遥调	0X6201~0X6400	
电度	0X6401~0X6600	
RTU 配置信息	0X1001~0X2000	非标准（自定义）
现场设备及传感器配置信息	0X2001~0X4000	
历史数据	0X7000~	