目录

[1、DNP3.0 协议简介 1](#_Toc495937186)

[1.1 DNP3.0协议分析简介 1](#_Toc495937187)

[1.2 DNP3.0 协议的特点 2](#_Toc495937188)

[2、DNP3.0 协议格式 2](#_Toc495937189)

[2.1数据链路层规约 2](#_Toc495937190)

[2.2 传输功能 4](#_Toc495937191)

[2.3 应用规约 5](#_Toc495937192)

[2.3.1 应用报文格式 5](#_Toc495937193)

[2.3.2 应用报文报头字段的定义 6](#_Toc495937194)

[2.3.3 对象标题 7](#_Toc495937195)

[3、通讯规则 8](#_Toc495937196)

[3.1链路层通讯规则 8](#_Toc495937197)

[3.2应用层通讯规则 9](#_Toc495937198)

# 1、DNP3.0 协议简介

## 1.1 DNP3.0协议分析简介

DNP(Distributed Network Protocol，分布式网络规约)是一种应用于自动化组件之间的通讯协议，常见于电力、水处理等行业。SCADA可以使用DNP协议与主站、RTU、及IED进行通讯。DNP协议标准由IEEE提出，参考了IEC 870-5、以及其他一些IEC协议。主要为了解决SCADA行业中，协议混杂、没有公认标准的问题。DNP协议有一定的可靠性，这种可靠性可以用来对抗恶劣环境中产生的电磁干扰、元件老化等信号失真现象，但不保证在黑客的攻击下、或者恶意破坏控制系统的情况下的可靠性。DNP协议提供了对数据的分片、重组、数据校验、链路控制、优先级等一系列的服务，在协议中大量使用了CRC校验来保证数据的准确性。

## 1.2 DNP3.0 协议的特点

• DNP3.0规约是一种分布式网络协议，适用于要求高度安全、中等速率和中等吞吐量的数据通信领域。  
• DNP3.0规约以IEC870-5标准为基础，该规约非常灵活，满足目前和未来发展的要求，且与硬件结构无关。  
• DNP3.0规约采用网络通信方式。  
• DNP3.0规约支持点对点、一点多址、多点多址和对等的通信方式。  
• DNP3.0规约支持问答式和自动上报数据传输方式。  
• DNP3.0规约支持通信冲突碰撞避免/检测方式，能保证数据传输的可靠性。  
• DNP3.0规约支持传送带时标的量，尤其有利于配电自动化系统采集分时电度值和分析事故原因。  
• 灵活采取适当的扫描方式，DNP3.0规约可以在一定程度上实现实时优先级。

# 2、DNP3.0 协议格式

DNP3.0规约的文本共分4部分：数据链路层规约，传输功能，应用层规约及数据对象库。

## 2.1数据链路层规约

数据链路层规约文件规定了DNP3.0版的数据链路层，链路规约数据单元(LPDU)以及数据链路服务和传输规程。数据链路层采用一种可变帧长格式：FT3。

FT3 帧长格式：一个FT3帧被定义为一个固定长度的报头，随后是可以选用的数据块，每个数据块附有一个 l6 位的 CRC 校验码。固定的报头含有2个字节的起始字，一个字节的长度(LENGH)，一个字节的链路层控制字 (CONTROL)，一个l6位的目的地址，一个16位的源地址和一个l6位的CRC校验码。

块0 块1 块N

-------

起始 起始 长度 链路 目的 源地 CRC 用户 CRC 用户 CRC

字 字 层控 地址 址 校验 数据 校验 …… 数据 校验

0\*05 0\*64 制字 码 码 码

-------

定长的报头 主体

起始字：2字节，0x0564

长度：1字节，是控制字、目的地址、源地址和用户数据之和。255≥长度≥5

目的地址：2个字节，低字节在前

源地址：2个字节，低字节在前

用户数据：跟在报头之后的数据块，每I6个字节一块，最后一个块包含剩下的字节，可以是 l 到16个字节。每个数据块都有一CRC循环冗余码挂在后面。

CRC循环冗余码：2个字节。在一个帧内，挂在每个数据块之后。

控制字与功能码：

通信控制字包含有本帧的传输方向，帧的类型以及数据流的控制信息。

7 6 5 4 3 2 1 0

DIR PRM FCB FCV 功能码

DIR：方向位（direction），表示此帧是由主站发出还是从站发向主站。

FRM：源发标志位（primary），表示此帧是来自原发站还是来自响应站。

FCB：帧的计数位，0、1交替变化，设计此位的目的是进行简单的纠错。

FCV：帧的计数位的有效标志，为1时，FCB位有效。

功能码：

对于原发送方的帧：

0：使远方链路复位

1：使远方进程复位 (Reset of user process)

3：发送用户数据，须对方确认

4：发送用户数据，不须对方确认

9：询问链路状态

对于从方发送帧：

0：肯定确认

1：否定确认

11：回答链路状态

例如：05 64 11 C4 29 00 01 00 70 1C

      05 64：报文头；11：报文长度；C4：控制域；29 00：目的站址；01 00：源站址；70 1C：CRC

## 2.2 传输功能

这部分定义对于DNP数据链路层充当伪传输层的传输层功能。伪传输层功能专门设计用于在原方站和副方站之间传送超出链路规约数据单元(LPDU)定义长度的信息。

传输层报头数据块：

其中：传输层报头——传输控制字，1个字节；数据块——用户数据，1～249个字节。

这部分定义对于 DNP 数据链路层充当伪传输层的传输层功能。伪传输层功能专门设计用于在原方站和从方站之间传送超出链路规约数据单元 (LPDU) 定义长度的信息。其格式如下：

TH （传输层报头） 数据块

由于数据链路层的 FT3 帧格式中的长度字的最大限制为255，因此传输层数据块的最大长度为 255-5 （链路层 control + source + destination ）-1（TH） =249。当应用用户数据长度大于 249 字 节时，传输层将以多帧报文方式传送，并每帧前加 TH 控制字。

如 l234=249+249+249+249+238，分5帧传送。

传输层报头 (TH) 格式：

7 6 5 4 3 2 1 0

FIN FIR 序号

FIN：此位置“1”，表示本用户数据是整个用户信息的最后一帧

FIR：此位置“1”，表示本用户数据是整个用户信息的第一帧

序号：表示这一数据帧是用户信息的第几帧，帧号范围为 0～63，每个开始帧可以是 0～63 中的任何一个数字，下一帧自然增加，63 以后接0

例如：05 64 11 C4 29 00 01 00 70 1C

EE C5 01 3C 02 06 3C 03 06 3C 04 06 95 B3

EE：传输层报头TH。

## 2.3 应用规约

这部分定义了应用层报文(APDU)的格式。这里，主站被定义为发送请求报文的站，而外站则为从属设备。被请求回送报文的RTU或智能终端(IEDs)是事先规定了的。在DNP内，只有被指定的主站能够发送应用层的请求报文，而外站则只能发送应用层的响应报文。

### 2.3.1 应用报文格式

应用请求报文的格式：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Request Header  请求报文 | Object Header  对象标题 | Data  数据 |  | Object Header  对象标题 | Data  数据 |

应用响应报文格式：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Response Header  响应报文 | Object Header  对象标题 | Data  数据 |  | Object Header  对象标题 | Data  数据 |

其中：请求(响应)报头——标识报文的目的，包含应用规约控制信息(APCI)；对象标题——标识后随的数据对象；数据——在对象标题内的指定类型的数据对象。

### 2.3.2 应用报文报头字段的定义

请求报头有两个字段。每个字段为8位的字节，说明如下：

|  |  |
| --- | --- |
| Application Control  应用控制 | Function Code  功能码 |

响应报头有三个字段。 前两个字段为8位的字节，第三个字段为两个字节，说明如下：

|  |  |  |
| --- | --- | --- |
| Application Control  应用控制 | Function Code  功能码 | Internal Indication  内部信号字 |

应用控制：一个字节的长度，格式如下：

7 6 5 4 3 2 1 0

|  |  |  |  |
| --- | --- | --- | --- |
| FIN | FIR | CON | 序号 |

FIR：此位置“1”, 表示本报文分段是整个应用报文的第一个分段

FIN：此位置“l”, 表示本报文分段是整个应用报文的最后一个分段

CON：此位置“l”, 表示接受到本报文时，对方须要给予确认序号：表示分段的序号，1-15

B．功能码：标识报文的目的，一个字节的长度，例如：

请求报文：

1一读，请从站送所指定的数据对象

2一写，向从站存入指定的对象

响应报文：

0一确认

129一响应

130—主动上送

C．内部信号：

共两个字节，l6位，每一位分别表示从站的当前的各种状态。

例如：05 64 11 C4 29 00 01 00 70 1C

EE C5 01 3C 02 06 3C 03 06 3C 04 06 95 B3

C5 01 3C 02 06 3C 03 06 3C 04 06 95 B3部分即为请求帧的应用层报文。

### 2.3.3 对象标题

报文的对象标题指定包含在报文中的数据对象或是被用来响应此报文的数据对象。格式如下：

|  |  |  |
| --- | --- | --- |
| Object  对象 | Qualifier  限定词 | Range  变程（范围） |

A．对象（Object）：

两个字节，指定对象组以及跟在标题后面的对象的变化。对象段的格式如下：

|  |  |
| --- | --- |
| Group  对象组 | Variation  变体 |

对象段规定一个对象组和在该组内的对象变体。对象的组别与变体结合起来可以唯一的规定报文所指定的对象。对象组指定数据的基本形式（如：模拟输入)，对象变体指定数据的形式 （如16位模拟输入或32位模拟输入)。

B．限定词（Qualifier)、变程 (范围，Range)

限定词为一个8位的字节段，规定交程段的意义。变程说明数据对象的数量，起点和终点的索引成所讨论的对象的标识符。

限定词段的格式如下：

|  |  |  |
| --- | --- | --- |
| R | Index Size  索引规模 | Qualifier Code  4位限定词码 |

其中：

R：保留位，置为零。

索引规模（Index Size)：

3个Bits，，规定前置于每个数据对象的索引规模或对象的规模。

在请话求报文中，当限定词码 (Qualifier Code) 等于11时,1、2、3分别代表数据对象前的索引是l、2、4个字节。0无效。4、5、6、7保留。

在响应报文中，或包含数据对象的请求报文的对象标题中：

0：对象没有前缀的索引

1：对象有一个字节的前缀索引

2：对象有两个字节的前缀索引

3：对象有四个字节的前缀索引

4：对象前有一个字节标识对象的大小

5：对象前有两个字节标识对象的大小

6：对象前有四个字节标识对象的大小

7：保留

# 3、通讯规则

## 3.1链路层通讯规则

1. 主站必须在复位了子站的链路之后，才能与该子站进行通讯。当主站检测出与子站的通讯中断之后，要重新复位该子站的链路。
2. 很多情况下，子站也要复位主站的链路。当通讯中断之后，也要重新复位链路。
3. 当副方站的接收缓冲区将要满了，不能再接收数据（指的是应用层数据）时，就会把返回给源方站的应答报文（ACK或NAK）中的DFC位置1，源方站收到这个标志后，就每隔一段时间查询一下副方站的链路状态（PRM=1,FCV=0,FunctionCode=9），副方站就以链路状态帧进行响应（PRM=0,FunctionCode=11,DFC=1或0），直到源方站收到的报文中DFC位清0后，源方站才能继续向该站发送数据或命令。
4. 当源方站发出的链路层报文要求副方站的链路层响应时，副方站必须发出链路层响应（它包括链路层的ACK、NAK、链路状态等），如果该站要作为副方站发出链路层响应还要作为源方站响应应用层报文时，该站必须先发出链路层响应。否则，源方站就会认为报文没有顺利到达副方站，超过链路层的等待时间后，源方站就会重发上次的链路层报文。多次重发后就会认为链路中断，从而导致通讯不正常。
5. 当源方站发出的“CONFIRMED USER DATA”收到了副方站的NAK后，一般来说很可能是FCB位不一致，这时源方站就要发出“测试链路状态”报文，以统一双方的FCB位。

## 3.2应用层通讯规则

1. 召唤数据或发出控制命令的一方，如果在规定的时间内没有收有预期的应答，就会重发应用层报文。多次重发后仍未收到，则认为应用层通讯服务失败。
2. 应用层数据召唤采用的应用层报文序号与响应该数据召唤命令的数据包的应用层报文序号以及对此数据包的应用层确认报文的应用层报文序号应该采用同一个值。
3. 不带品质描述的对象类型一般都有缺省的品质描述，如果以不带品质描述的对象类型召唤某些数据，但其中有些数据元素的品质描述不是缺省的品质描述时，那么，这些数据元素将不会上送。