基于非安全级DCS通讯站中链路参数设置分析及研究

Analysis and Research of Link Parameters Setting in Communication Station Based on Non-Security Level DCS

★北京广利核系统工程有限公司 迟宗岭

摘要：在CPR1000核电项目机组工程中，非安全级核电站数字化仪控系统（NC-DCS系统）应用软件平台采用的是MACS6.2.0系统，涉及到的第三方设备不参与逻辑运算，且只在HMI流程图中显示和报警的数据，均采用通讯站进行数据传输，涉及逻辑运算的则采用硬接线方式直接采集数据。通讯站硬件采用的是一款OAMA01A（或OAMA03A）型工控机嵌入式微型计算机，一款无风扇全封闭嵌入式微型计算机。软件采用的是以Linux-2.6.16.25为蓝本的裁剪版的操作系统，由于Linux系统在工程应用上有许多优点，便于工程师编程和调用程序，同时，也是一款开放性的操作系统，因此受到编程者的青睐。在CPR1000核电机组项目调试和运行过程中，有时发现部分通讯站上传的数据点显示迟缓，刷新频率明显和设计预期不相符。为此本文结合了现场调试经验，分析了数据上传迟缓的原因及后续采取的措施，详细描述了链路参数的设置规则，对由链路参数设置或者操作过程不规范等原因，导致L2层数据显示迟缓的根源进行了总结分析，为后续机组优化参数提供了参考，同时也为同类型机组及今后华龙一号的调试提供借鉴。

关键词：通讯站；链路参数；故障

Abstract: In the CPR1000 nuclear power project, the digital instrument control system(NC-DCS system) platform for non-safe nuclear power plants uses Macs 6.2.0, which involves third-party equipment that does not participate in logical operations. And only the data displayed and alerted in the HMI flow chart uses communication stations for data transmission, and hard-wired methods for logic operations are used. The communication station hardware uses an OAMA01A (or OAMA03A) industrial control machine embedded microcomputer, a fan-free fully enclosed embedded microcomputer. The software uses a tailored version of the operating system based on Linux-2 .6.16.25. Since the Linux system has many advantages in engineering applications, it is easy for engineers to program and invoke programs. At the same time, it is also an open operating system. It is therefore favored by programmers. During the debugging and operation of the CPR1000 nuclear power plant project, it is sometimes found that the data points uploaded by some communication stations are slow to display, and the refresh frequency is obviously inconsistent with the actual scene. In this paper, combined with the field debugging experience, the reasons for the delay in data upload and the measures taken are analyzed. At the same time, the setting rules of link parameters are described in detail, and the link parameters are set or the operation process is not standardized. The root causes of the delay in L2 layer data display are summarized and analyzed, and operational experience feedback is compiled to provide reference for the optimization parameters of subsequent units. At the same time, it also provides reference for the commissioning of the same type of unit and Hualong No. 1.

Key words: Communication station; Link parameters; Faults

1 前言

在CPR1000核电厂非安全级DCS通讯站调试过程中，有时遇到Level2层（DCS操作监视层）显示数据和实时值不一致，或者刷新频率明显迟缓。本文主要探讨通讯站组态中添加点表和链路表信息，从通讯链路参数以及点表配置、现场维护人员操作等方面对问题进行分析，并且根据分析情况提出处理优化方案。

2 通讯站组态

Linux在工程中的优势使其受到了许多DCS系统工程师的青睐，因此，在CPR1000核电站项目工程中也不例外，第三方通讯便采用其作为操作系统。

通讯站主要用于与上层（Level2）、下层（Level0）第三方设备进行数据交互，由于第三方设备的多样性，需要在工程总控组态中对特殊的数据库类型进行组态。正确的数据库组态是通讯站进行正常的关键因素，使用者务必按照组态规则执行。通讯站的主要功能是实现与第三方系统通讯。通讯协议支持Modbus RTU、Modbus TCP、IEC 104。下面对具体的组态过程和注意事项做具体的描述。

2.1 添加通讯站

首先，在MACS6.2.0正式平台上，已经建立的工程上，添加通讯站并对其进行组态。

通讯站组态需要按照以下步骤进行：创建新工程，通讯站添加与设置，增加通讯站，设置通

讯站号；定义通讯站变量，选择数据类型，添加变量点数据，添加点表和链路表信息。通讯站的组态流程如图1所示。

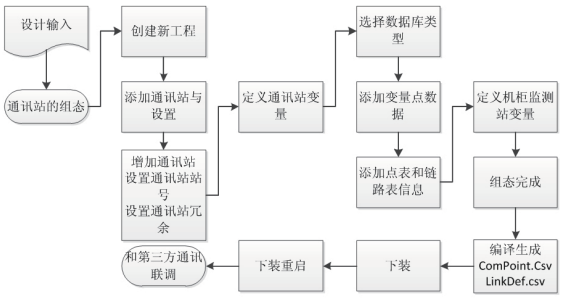

图1 通讯站组态流程示意图

2.2 链路参数和点表配置

在添加完成变量点数据后，需要在数据库中添加通讯点（COMTAG）和通讯链路（COMLINK），本文结合现场调试经验，重点描述分析通讯点和通讯链路的配置。

通讯链路（COMLINK）参数和通讯点（COMTAG）表务必按照以下规则进行配置，否则，将会导致通讯异常，链路不通等异常问题出现。

通讯链路（COMLINK）数据组态规则、输入方式及注意事项的主要参数详细设置如表1所示。

表1 链路表参数配置点项说明

名称	组态规则
站号	输入数字
链路号	输入数字
链路类型	0：保留 1：Modbus RTU 2：Modbus TCP 3：IEC 60870-5-104
子链路类型	输入子链路字符串
链路参数区	按具体格式输入

链路参数区（LP）组态配置顺序和格式说明的主要参数详细设置如表2所示。

表2 链路参数区（LP）组态格式说明

链路类型（LT）	链路参数（LP）配置顺序和格式说明
Modbus RTU协议	（1）备用站操作模式；（2）通讯站使用的串口号；（3）波特率；（4）数据位；（5）停止位；（6）校验位；（7）读串口超时时间；（8）读串口等待延迟时间；（9）字节顺序；（10）发送帧间间隔；（11）最大帧长度；（12）读输入操作失败最多重复次数；（13）写操作失败最多重复次数。
Modbus TCP	（1）备用站操作模式；（2）第三方IP地址；（3）端口号；（4）超时时间；（5）字节顺序；（6）最大帧长度；（7）发送帧间间隔；（8）读输入操作失败最多重复次数；（9）写操作失败最多重复次数。
IEC 60870-5-104	（1）备用站操作模式；（2）第三方IP地址；（3）建立连接的超时t0；（4）发送或测试APDU的超时t1；（5）无数据报文时确认的超时t2（t2<t1）；（6）长时间空闲状态下发送测试帧的超时t3；（7）未被确认的I格式APDU最大数目k；（8）最迟确认APDU的最大数目w；（9）单命令（类型标识45）执行模式；（10）设定命令（类型标识49）执行模式。

通讯点表（COMTAG）定义表的主要参数详细设置如表3所示。

表3 通讯点表（COMTAG）定义说明

名称	用途
数据类型	通讯点的源点数据类型
数据长度	点在共享内存中存储的空间大小
功能码	Modbus协议中的功能码，IEC 104协议中的类型标识
地址	Modbus协议中的寄存器地址，IEC 104协议中的信息对象地址

2.3 建立数据库，设置链路参数，生成CSV表

组态完毕后，经过工程总控编译生成点表ComPoints.csv和链路表LinkDef.csv。然后通过工程总控中的工具，选择通讯站节点号，下装通讯站，即可用于控制的数据通信。

至此，通讯站组态下装完成，正常情况下通讯正常，数据上传L2层显示。

3 点表ComPoints.csv对上传数据的影响

当点表（ComPoints.csv）通讯数据地址连续时，进行请求和收发，分帧数据量较少，相反，如果通讯数据地址不连续，分帧数据量较大，导致上传数据延迟。

对于Modbus RTU协议而言，传输速率取决于双方协商的波特率。波特率表示每秒中传送的码元符号的个数，是衡量数据传送速率的指标。在CPR1000项目中，对不同的系统选取的波特率不同，一般为9600bps、19200bps、38400bps。

对于Modbus TCP协议以及IEC 60870-5-104协议而言，采用的是网络传输，传输速率取决于网络传输帧值的大小。网络传输帧值是在一定范围内浮动的，最大

的帧值是1518字节，最小的帧值是64个字节。但在实际应用中，帧的大小是数据量的多少，即设备每次能够传输的最大字节数是自动来确定的。

因为传输协议，传输速率在组态工程中已经确定，对数据上传的影响已经明确，因此，数据地址的连续与否，关系到分帧数据量的多少，数据量的多少将直接影响数据的传输时间长短和更新频率。

4 链路表LinkDef.csv数据对上传数据的影响

下文仅对Modbus RTU协议以及Modbus TCP协议中的相关参数进行说明。

对于Modbus RTU协议而言，在链路类型（LT），与上传时间相关的主要参数分别为：第7位读串口超时时间，读串口超时时间（通讯站发出请求召唤帧后，在超时时间内等待从站的回复，单位ms）；第8位读串口等待延迟时间，读串口等待延迟时间（通讯站判断到从站有回复数据后，在延迟时间后，再读串口数据，以保证读取完整的回复数据，单位ms）；第10位发送帧间间隔（通讯站在处理完第三方对上一帧的回复后延迟设置的时间间隔后发送下一帧数据，单位ms）；第12位读输入操作失败最多重复次数（一般设置为3次）；第13位写操作失败最多重复次数（一般设置为3次）；数据上传时间是上述参数时间累计之和。

对于Modbus TCP协议而言，在链路类型（LT），与上传时间相关的主要参数分别为：第4位超时时间（通讯站发出召唤或配置帧后，在超时时间内等待从站的回复，单位ms）；第6位最大帧长度（根据现场组态情况，自己定义，如第三方无特殊要求则应配置为259）；第7位发送帧间间隔；第8位读输入操作失败最多重复次数；第9位写操作失败最多重复次数。

影响通讯联络数据传输延迟的因素很多，如硬件、施工质量、传输协议等技术，软件组态等多种原因。下文仅就通讯链路参数导致的延迟讨论，通讯延迟的总时长主要由单个收发帧平均收发时间和收发帧数的乘积决定。因此，分析数据上传延迟问题，需要从上述数据中逐项分析，找到问题的根源，从而彻底将问题解决。

5 应用案例分析

5.1 Level2层显示和现场实时值存在明显偏差

问题描述：

2016年5月30日，在某核电站，2APA202PO泵运行期间，2APA205MV振动高报警（示值8.02，超过H1阈值7.1，维持1.5min左右），与就地不符，L2层刷新数据显示延迟。

问题分析：

分析逻辑组态震动高是第三方数据通过非安全级64号通讯站，上传到计算服务器进行数据处理，然后上传至L2层显示报警。逻辑组态如图2所示。

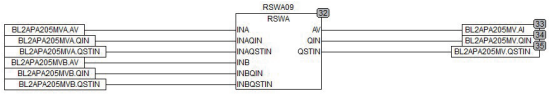

图2 BL2APA205MV报警组态截图

初步分析导致以上现象，有两种可能的原因：

（1）数据库点项参数配置异常，导致数据上传L2层显示迟缓；

（2）链路参数配置不合理，引起上传数据刷新延迟。

下文从以上两方面进行问题分析：

首先，分析BL2APA205MVA在ComPoints中点表的参数配置，通过比较分析，结合同类型其它点项分析，初步判断设置正常，如表4所示。

表4 BL2APA205MVA在ComPoints点表配置参数

通信点项名	站号	链路号	设备号	用户自定义数据	数据类型	数据长度	功能码	地址	输入输出类型	点类型
BL2APA205MVA.AI	64	0	2	0	5	4	4	538	0	0

分析BL2APA205MVA在ACI点表配置参数如表5所示。

表5 BL2APA205MVA在ACI点表配置参数

量程上限	量程下限	输入量量程上限	输入量量程下限	AV输出方式选择	超量程判断选择	超量程恢复死区	超量程限值%	超量程对质量影响	通讯写IO站允许	工程计算属性
20	0	16384	0	1	3	2.5	10	0	0	0

BL2APA205MVA在ACI点表配置参数（续）

历史库收集周期	质量坏输出替代值	质量坏替代	区域号	Retain属性	点名	站号	点说明	点相关图	量纲	输出格式	点类型
4	0	0	2	1	BL2APA205MVA	64	Bearing Vibration Main FWP		mm/s	%8.2f	ACI

BL2APA205MVA在ACI类型点表配置参数中没有异常。为了进一步定位问题的根源，提取报文分析成为解决该问题的唯一途径。

Modbus RTU通讯简介-数据帧结构、功能码、链路参数由64号通讯站报文分析可知:

在2016年05月30日22:05:53:099时刻，点021a（地址为：538），采集数据为19a9（6569），详见以下报文解析。

2016-05-30 Mon 22:05:53:081 (Main)SOCKET/COM 4 RECV 8 bytes: 02 04 02 1a 00 01 11 86

2016-05-30 Mon 22:05:53:099 (Main)SOCKET/COM 4 SEND 7 bytes: 02 04 02 19 a9 36 de

L2层显示=AV:=（AI-AIMD）×(MU-MD)/(AIMU-AIMD)+MD=6569/(16384-0)×(20-0)=8.018=8.02

由报文解析得知，在2016年05月30日22:05:57:179时刻开始打时标，详见下报文。

2016-05-30 Mon 22:05:57:179 (S)Test Information

由报文解析可见，在2016年05月30日22:07:18:731时刻地址538点项开始变位，采集数据为098f（2447），

L2层显示=AV:=（AI-AIMD）×(MU-MD)/(AIMU-AIMD)+MD=2447/(16384-0)×(20-0)=2.987=2.99

由报文解析得知，在2016年05月30日22:07:22:812时刻开始打时标，详见如下描述;

2016-05-30 Mon 22:07:22:812 (S)Test Information。

图3是事件记录的时序图。

由上述分析，可知两次之间数值采集时标之间差值，间隔长达1m25s，时间不符合现场显示要求，HMI画面的刷新频率在250ms左右，查看链路参数，发现LP链路参数区中的发送帧间间隔为1000s，经过和第三方厂家协商，设计院同意修改此参数，后将此参数修改为0，修改后显示符合现场要求。修改前链路参数

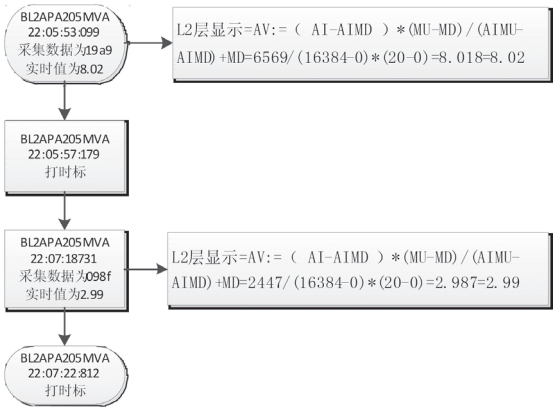

图3 BL2APA205MV报警时序图

如表6所示，修改后链路参数如表7所示。

表6 修改前链路参数配置

通信链路名	站号	链路号	链路类型	子链路类型	链路参数区
BL2DCS_VMS_01	64	0	1	VMSA	0'7'19200'8'2'N'3000'0'1000'5'255'3'3

表7 修改后链路参数配置

通信链路名	站号	链路号	链路类型	子链路类型	链路参数区
BL2DCS_VMS_01	64	0	1	VMSA	0'7'19200'8'2'N'3000'0'0'5'255'3'3

初步分析，链路参数在设计时，没有考虑现场运行人员的实际需求，对相应参数验证不充分，对每个参数的显示没有充分验证。

在现场调试过程中，必须对每一个通讯点的阀值进行测试，以保证在运行时显示正常，给运行人员提供可以信赖的实时数据以及报警。

5.2 通讯点表设备号引发通讯周期延长

问题描述:

2015年8月在某核电站现场调试人员发现，机组画面GME002YCD数据刷新时间约8s，但是在调试的其他三台机组相同画面刷新时间为2~3s，显示正常。

问题分析:

常规画面刷新的时长固定位250ms，通讯点值刷新时间实际反应的是和第三方通讯的周期长短有关。数据只要在通讯站采集到的数据有刷新，送到L2画面显示的周期都是固定不变的，不会导致较大的差异。

影响通讯站采集数据周期的因素有如下几项:

（1）链路参数的影响。某机组的#66通讯链路参数修改（0'1'57600'8'1'N'3000'500'0'10'255'3'3修改为0'1'57600'8'1'N'3000'200'0'0'255'3'3），减少了帧间间隔时间和读串口等待延迟时间后，通讯间各数据包的间隔时间和等待时间都减少，缩短了整个通讯的时间。

（2）数据量大小的影响。对异常机组数据与正常机组数据的66号站通讯站数据传输点数，以及每种功能码对应的数据量基本相当，因此该因素影响数据通讯的可能性极小。

（3）通讯数据地址是否连续的影响。只有通讯点的地址连续，数据才会按照连续地址打包，通讯数据包数量才最少，相应的通讯速率快，通讯时间最短，大大缩短了整个通讯周期时长。如地址不连续，则拆分的数据包就会增多，导致通讯时长明显增大。

按照因素（1）的分析，进行了修改下装，调整后没有明显的改观，排除因素（1）的影响。

因素（2）在对比过程中，数据大小基本一致，所以也排除。

最有可能的就是因素（3），下面重点对于因素（3）数据地址是否连续进行认真分析与研究。

采用两种方式，对现场点表进行了重新下装。首先，通过ftp命令登陆通讯站，利用put命令将点表和链路参数下传到通讯站MacsRTS目录下，重新启动主机，观察数据刷新频率没有任何变化。其次，在工程总控中，对数据库进行编译下装，重启通讯站主机，观察HMI画面显示刷新正常。

至此现场问题已经基本解决，初步定位为点表有异常。但是，问题的根源究竟在哪儿，需要作进一步分析和判断。

对经过工程总控编译下装后的点表，通过get命令提取后，和之前经过编译下装到现场通讯站的数据进行比对发现了问题。

对“ComPoints.csv”的点表进行比对分析发现，有6个点AA3CEX101KM9.DI、AA3CEX102KM9.DI、AA3CEX201KM9.DI、AA3CEX202KM9.DI、AA3CEX301KM9.DI、AA3CEX302KM9.DI的设备号“DN”虽都是2，但是在点表中的位置存在差异。如表8所示，为通过ftp命令直接put到通讯站的数据；如表9所示，为通过编译后下装到通讯站的数据。

表8 为通过ftp命令直接put到通讯站的数据

通信点项名	（站号，链路号，设备号，自定义数据，数据类型，数据长度，功能码，地址，输入输出类型，点类型）									
AA3GGR314MT9.DI	66	0	3	0	4	1	4	1023.4	0	1
AA3CEX101KM9.DI	66	0	2	0	4	1	4	1023.5	0	1
AA3GGR321MT3.DI	66	0	3	0	4	1	4	1024	0	1
…	…	…	…	…	…	…	…	…	…	…
AA3GGR321MT9.DI	66	0	3	0	4	1	4	1024.4	0	1
AA3CEX102KM9.DI	66	0	2	0	4	1	4	1024.5	0	1
AA3GGR322MT3.DI	66	0	3	0	4	1	4	1025	0	1
…	…	…	…	…	…	…	…	…	…	…
AA3GGR322MT9.DI	66	0	3	0	4	1	4	1025.4	0	1
AA3CEX201KM9.DI	66	0	2	0	4	1	4	1025.5	0	1
AA3GGR323MT3.DI	66	0	3	0	4	1	4	1026	0	1
…	…	…	…	…	…	…	…	…	…	…
AA3GGR323MT9.DI	66	0	3	0	4	1	4	1026.4	0	1
AA3CEX202KM9.DI	66	0	2	0	4	1	4	1026.5	0	1
AA3GGR324MT3.DI	66	0	3	0	4	1	4	1027	0	1
…	…	…	…	…	…	…	…	…	…	…
AA3GGR324MT9.DI	66	0	3	0	4	1	4	1027.4	0	1
AA3CEX301KM9.DI	66	0	2	0	4	1	4	1027.5	0	1
AA3GGR325MT3.DI	66	0	3	0	4	1	4	1028	0	1
…	…	…	…	…	…	…	…	…	…	…
AA3GGR325MT9.DI	66	0	3	0	4	1	4	1028.4	0	1
AA3CEX302KM9.DI	66	0	2	0	4	1	4	1028.5	0	1

表9 为通过编译后下装到通讯站的数据

通信点项名	（站号，链路号，设备号，自定义数据，数据类型，数据长度，功能码，地址，输入输出类型，点类型）									
AA2GME544MV9.DI	66	0	2	0	4	1	4	1022.5	0	1
AA2CEX101KM9.DI	66	0	2	0	4	1	4	1023.5	0	1
AA2CEX102KM9.DI	66	0	2	0	4	1	4	1024.5	0	1
AA2CEX201KM9.DI	66	0	2	0	4	1	4	1025.5	0	1
AA2CEX202KM9.DI	66	0	2	0	4	1	4	1026.5	0	1
AA2CEX301KM9.DI	66	0	2	0	4	1	4	1027.5	0	1
AA2CEX302KM9.DI	66	0	2	0	4	1	4	1028.5	0	1
AA2GSE999MP.AI	66	0	3	0	14	4	4	0	0	1

从表8可以得出，现场调试人员在执行DEN变更过程中，直接在“ComPoints.csv”中进行修改，将这6个点的设备号由3变为2，但未对其点表所在位置进行调整，导致系统通讯设备号（DN）、地址（AD）不连续，设备号2和3之间交替重复，因此数据包增多，从而延长了通讯的采集周期。

正确的操作步骤应该是，在MACS6.2.0平台中的工程总控对通讯点表ComPoints进行修改，如图4所示，然后编译，工程重新生成通讯点表“ComPoints.csv”、“LinkDef.csv”，新的通讯点表在编译过程中位置调整遵从如下规则：COMTAG编译生成ComPoints.csv文件时，是按照输入输出类型（IOT）->站号(SN)->链路号（LN）->设备号（DN）->功能码（FC）->地址（AD）优先顺序排列的。

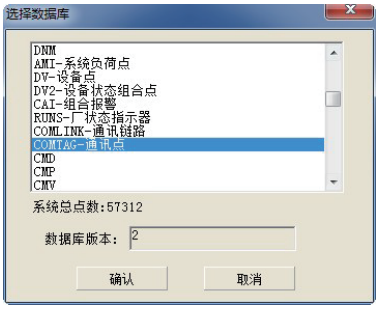

图4 在数据库中添加通讯点

这样就确保设备号顺序排列、地址连续，下装配置文件到对应通讯站后，有关点项才可以正常通讯。

5 对今后工作的借鉴与启发

（1）通讯站通讯点表中任意参数的修改，都要遵循常规修改方法。在工程总控中修改后，需要编译工程总控，生成新的通讯点表配置文件，然后在现场条件允许时，下装到通讯站，重启后生效。

（2）由于受现场条件约束，特殊情况需要特殊处理，但是必须要保证“设备号顺序排列”、“地址连续”两点原则。如有个别点的设备号有变动，但是，现场不满足编译的条件时，则需要以文本方式打开（非Excel方式打开），修改设备号后，并将该行剪切到相同设备号的位置，并且保证地址由小到大顺序排列。

（3）在平台设计过程中，是否有必要考虑一下，在裁剪Linux系统时删除put命令功能，防止通过put命令将点表和链路参数下装到通讯站，仅保留get命令功能，从而保证了下装的唯一途径是通过工程编译后下装，其它途径全部通过技术方式禁用。

6 结束语

本文结合在CPR1000项目实施调试第三方通讯站过程中遇到的棘手疑难问题，认真分析问题、剖析根源，最终找到了解决该问题的方法。在核电调试和运行过程中，进行优化和完善，不断在管理和技术上探索有利于项目实施的方法和举措，为后续同类型机组及华龙一号的调试和运行提供技术支持。AP

作者简介：

迟宗岭（1977-），男，山东茌平人，大专，工程师，现就职于北京广利核系统工程有限公司，主要从事核非安全级数字化仪控系统研究工作。

参考文献：

[1] Sumitabba Das. UNIX Concepts and Applications Fourth Edition[M]. 北京：清华大学出版社, 2006.

[2] 王刚, 等.Linux 命令、编辑器与Shell编程[M]. 北京：清华大学出版社, 2012.

[3] James Pyles, Jeffrey L. Carrell, Ed Tittel. TCP/IP协议原理与应用[M]. 北京：清华大学出版社, 2018.