

DOI:10.3969/j.issn.1001-4551.2015.01.023

基于 MELTAC-N 平台的核电厂安全级 DCS 环网研究与测试

王少威,汪富强,黎国民
(中广核工程有限公司,广东 深圳 518124)

摘要:针对工程实践中环网通讯相关问题的处理缺乏理论基础及国产化安全级 DCS 平台的开发缺乏成熟经验借鉴问题,对基于 MELTAC-N 平台核电厂安全级 DCS 环网的软硬件实现进行了研究。提出了安全级 DCS 环网双环网冗余设计、光切换开关设计等硬件设计方法,以及以 RPR 协议为基础,采用全数据收发策略的软件设计方法。在 CPR1000 安全级 DCS 平台上对安全级 DCS 环网的可靠性及实时性进行了评价,并进行了容错能力、响应时间及响应时间稳定性测试验证实验。结果表明,基于 MELTAC-N 平台安全级 DCS 环网软硬件设计具有较好的容错能力及响应时间稳定性。

关键词:安全级 DCS;环网;系统网络;链路容错;响应时间稳定性

中图分类号:TP23;TM918

文献标志码:A

文章编号:1001-4551(2015)01-0123-05

Research and test validation of data bus base on MELTAC-N safety DCS platform

WANG Shao-wei, WANG Fu-qiang, LI Guo-min
(China Nuclear Power Engineering Co., Ltd., Shenzhen 518124, China)

Abstract: Aiming at solving the problem of lacking theory for practice and reference for safety DCS platform localization research and development, the hardware and software design of data bus base on MELTAC-N safety DCS platform were investigated. A method of hardware design which include double circle and optical Switch function design and a method of software design which is full data transmission policy base on RPR protocol were presented. The reliability and real time performance were evaluated on the CPR1000 safety DCS platform, data link robust, response time and response time stability were tested. The results indicate that the hardware and software design of MELTAC-N safety DCS platform have excellent performance of data link robust, response time and response time stability.

Key words: 1E DCS; ring network data bus; bus system; robust of link; stability of response time

0 引 言

CPR1000 核电项目采用基于 MELTAC-N 平台的安全级 DCS 系统。安全级 DCS 平台承担着反应堆保护功能及专设安全动作功能,其功能的正确、可靠、稳定直接影响核电厂的运行效率及运行安全^[1]。

系统网络作为数据通路,承担着大量重要数据的柜间传输,犹如整个 DCS 系统的血脉,是 DCS 系统构

成、功能实现及系统稳定的基础^[2]。为了确保控制相关信息的及时传递,DCS 的系统网络必须满足实时性的要求,即在确定的时间限度内完成信息的传送。为了保障控制系统信息的稳定正确传递,DCS 的系统网络必需满足稳定性、可靠性的要求^[3-4]。

因此,本研究基于 MELTAC-N 平台安全级 DCS 环网的软硬件实现,介绍 MELTAC-N 平台安全级 DCS 环网的设计方法及特点。

1 CPR1000 安全级 DCS 平台网络系统简介

CPR1000 安全级 DCS 平台的系统网络由 4 组具有类似网络结构的环网组成,它们均为光纤双环网结构,分别为 safety system bus、safety bus train A、safety bus train B、HM data bus。其中 safety bus train A、safety bus train B 安全分级为 1E,safety system bus 及 HM data bus 安全分级为 NC^[5-6]。CPR1000 安全级 DCS 平台网络系统结构图如图 1 所示。由于 4 个环网实现原理相同,以下就以 safety bus train A 为例来进行说明。

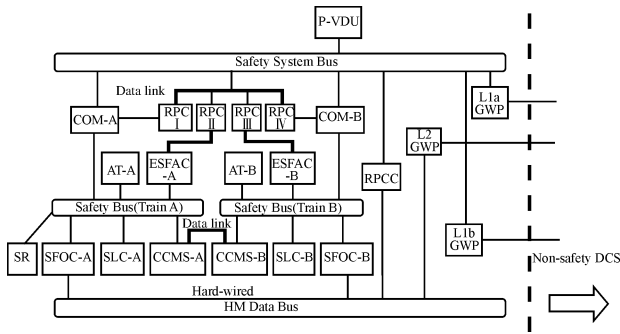


图 1 CPR1000 安全级 DCS 平台网络系统结构图

2 环网的硬件实现

2.1 双环网结构设计

为了保证部分通讯链路意外中断或故障而不可用的状态下,机柜间通讯不中断,必须提供冗余的通讯链路。双总线、环形或双重星形等网络拓扑结构被应用于 DCS 网络系统的设计中^[7]。CPR1000 安全级平台采用双环拓扑结构如图 2 所示。在双环结构中,存在内外两条独立物理链路的环路,内外环路数据的流向相反,每个节点均能与相邻节点互通数据。两条物理链路上的互为冗余,使得该形式的环网结构拥有了应对传输链路单一故障的能力。

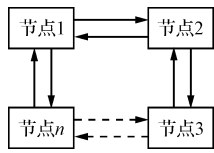


图 2 双环拓扑结构

CPR1000 安全级 DCS 平台各机柜以 CPU 为节点串接于环网上。环网上 CUP 节点的布置连接顺序除了需要考虑实际安装房间位置外,还需要考虑其布置顺序,以优化整个环网的数据传输性能及保障故障条件下数据的传输。

2.2 网络节点硬件配置

环网上各个机柜节点的硬件配置示意图如图 3 所示。环网上的各机柜通过 W-NET 网络接口板卡、光切换单元(Optical Switch)、光纤接线盒实现与环网的联通。

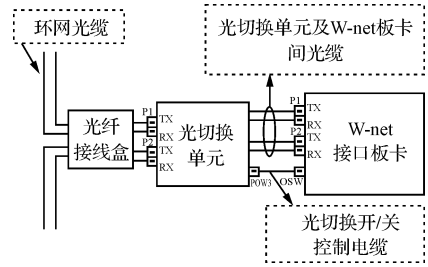


图 3 网络节点硬件配置

其中,W-NET 接口板卡为光纤接口通信卡件,它遵从 Futurebus + 总线标准;为了与系统 CPU 通信,它拥有双接口存储系统。双口 RAM 的实时区设计为两个大的区域,每一区域只允许一方写操作。即要么是 CPU 可读,通信控制器主写;要么是 CPU 主写,通信控制器可读,杜绝双方同时具备可写访问权限情况。两个模块的读写周期是完全独立而且异步的,不需要等待另一个放的读写操作完成,因此,任何一个确定的周期,CPU 和通信控制器的运行都不会被中断。通过双接口存储系统实现的 CPU 与通信控制器间的通讯,即使在通讯控制器故障的情况下也不会影响 CPU 正常运行,实现了通讯的功能隔离,这种功能隔离能够提高系统通讯的可靠性,环网的光电隔离及通讯隔离如图 4 所示。W-NET Card 使用 FPGA 作为该卡件的通信处理单元。W-NET Interface Card 的卡件面板上有 4 个光纤接口,一个 RS-232C 及 Ethernet 维护工具接口。值得注意的是,该卡件的 OSW 接口与 Optical Switch Unit 连接。

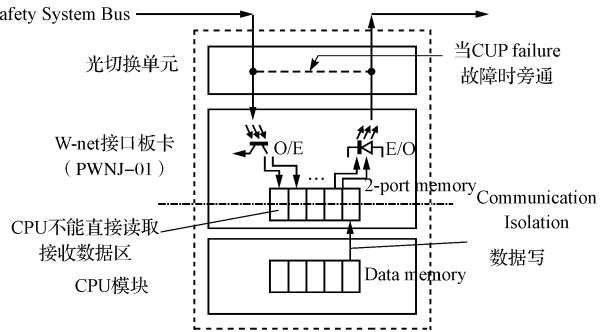


图 4 环网的光电隔离及通讯隔离

光切换单元是一种光纤回路切换设备。光纤回路切换大多数是通过光学切换来实现的。它所实现的功能是在 W-NET 接口板卡或节点机柜故障状态下,将该

节点从光纤环网中隔离、旁路,从而避免该失效的网络节点对整个光纤环网通讯的影响。光切换单元的切换操作由其 OSW 接口的输入信号控制。当 W-NET 卡件故障、失电或机柜 failure 的状态下,OSW 接口将失去对光切换单元模块的供电输入,光切换单元自动切换光回路,将故障节点从环网中旁路,从而保障环网链路的完整。环网节点故障前后环网链路状态如图 5 所示。

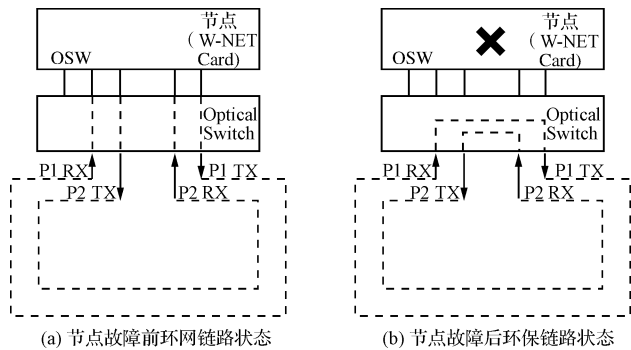


图 5 环网节点故障前后环网链路状态

3 环网的软件实现

3.1 RPR 协议

3.1.1 RPR 协议介绍

CPR1000 安全级 DCS 环网设计采用 RPR (Resilient Packet Ring, IEEE802.17) 协议完成环网传输控制及故障自愈。

RPR 为互逆双环拓扑结构,外环为 Outer Ring、内环为 Inner Ring^[8]。两个相邻 RPR 节点之间链路称为段 (Span),多个连续的段和其上的节点构成域 (Domain)。每个 RPR 节点都采用一个 48 位 MAC 地址作为地址标识。从 RPR 节点设备链路层来看,两对收发物理光接口只是一个链路层接口;从网络层来看,也只需要分配一个接口 IP 地址。环网带宽可以被不同的节点分段使用,整个环网的累积带宽大于单个链路的带宽容量。在非重叠区域的并发数据传输互不干扰;在重叠区域的并发数据传输,共同占用链路总带宽。每个节点均有以下 4 种数据操作功能:上环、转发、下环、剔除。

3.1.2 RPR 的自愈能力

RPR 技术的故障自愈能力非常强,能够实现很短时间内的故障保护切换。

在单环被切断的情况下,因为双环网传输物理链路上的冗余,环路数据仍然能够正常传输。

环网链路在故障的情况下,有两种保护方式:绕回

(Wrap) 保护方式和抄近 (Steering) 保护方式^[9],不同保护方式下的数据流向如图 6 所示。

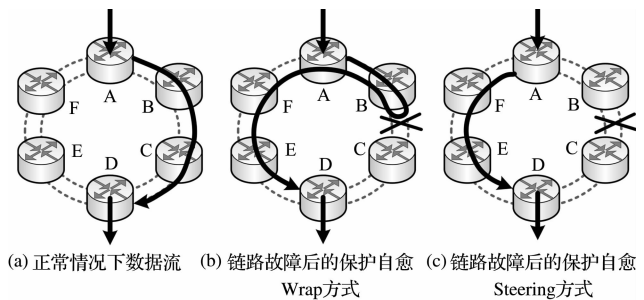


图 6 不同保护方式下的数据流向

绕回方式故障切换的恢复时间非常短 (50 ms 以内),但占用带宽较多。

抄近方式避免了带宽的浪费,但是由于需要重新收敛,恢复时间较长,可能会造成一些业务的中断。RPR 协议具有的这两种保护方式,使得 RPR 环网通讯拥有链路故障自愈能力,能够提高环网通讯的可靠性。

3.2 全数据收发设计

3.2.1 全数据收发简介

全数据收发指的是环网节点在每个数据收发周期内不对通讯点数据是否发现变化进行判断,而是将所有相关数据进行转发或接收。在环网上的通讯点数量较多的情况下,全数据收发的方式会增加环网的负荷,从而对环网的带宽、传输速率等性能提出了较高的要求。

3.2.2 全数据收发的优点

全数据收发能够一定程度上提升环网性能及可靠性。

通过采用全数据收发的模式,将使得该通讯网络在水平雪崩 (短时间内网络通讯点数据大量状态跳变) 的情况下,节点间数据通讯响应时间不会受到影响。理论上环网的通讯负荷与正常状态下一致,数据传输的响应时间也与正常状态下保持一致。

同时全数据收发的方式容许环网拥有较为简洁的数据筛选、数据更新、数据发送机制。一方面,简洁的通讯协议机制减小了用于通讯控制的数据,降低环网用于通讯控制的带宽;另一方面,更为简洁的通讯机制能够帮助降低通讯过程中数据传输出错的概率。

4 环网功能性能的测试验证

环网的功能性能的验证测试方法有很多种,本研究针对 MELTAC-N 平台安全级 DCS 环网软硬件设计特点,主要从容错能力、响应时间及响应时间稳定性两

个方面来进行验证。

4.1 容错能力验证

本研究模拟运行过程中环网可能碰到的各类故障情况,观测机柜间数据能否正确传递来验证环网的容错能力。

实验以 Safety Bus-Train A 为代表,选取安全逻辑机柜(SLC-A1)与安全显示柜(SFOC-A1)间的数据传输进行验证。在不同环网状态下,操作 NI 操作台上的安全操作显示单元(S-VDU,对应 SFOC-A1)ASG137VV 画面,发送 open 指令,检查安全逻辑柜是否能够正常执行 ASG137VV 的开启操作。

实验结果如表 1 所示。

表 1 环网不同链路故障下的实验结果

环网故障类型	故障模拟操作	ASG137VV 是否能正常操作
无故障	无	YES
单链路故障	拔掉 SFOC-A1 机柜 P1 Tx 端口光纤	YES
	拔掉 SFOC-A1 机柜 P1 Rx 端口光纤	YES
同网段双链路故障	同时拔掉 SFOC-A1 机柜 P1 Tx/Rx 端口光纤	YES
不同网段同一环网链路故障	同时拔掉 SFOC-A1 机柜 P1 Tx 及 P2 Rx	YES
不同网段内外环网链路故障	同时拔掉 SFOC-A1 机柜 P1 Tx 及 P2 Tx	NO
中间节点 Failure	Failure CCMS-A Subsystem-A CPU	YES
中间节点失电	CCMS-A 机柜整体断电	YES

实验结果验证了 CPR1000 安全级 DCS 环网的实现很好的保障了在某些链路故障及中间节点故障的情况下的数据传输,具有较好的链路容错能力。

4.2 响应时间及响应时间稳定性验证

为了验证安全级 DCS 环网响应时间及环网故障对于环网上信号传输响应时间的影响,本研究对环网故障前后安全专设响应时间进行测试,分析响应时间数据,对比环网故障前后安全专设响应时间的变化,从而实现对环网响应时间及响应时间稳定性的验证。

这里选取启动柴油机带载卸载安全专设工况为例进行验证,LHA 母线失电后,由厂用电切换到应急柴油发电机供电,并对设备进行甩负荷及重新加载负荷操作,LHA 母线失电信号通过 ESF-A 的 DI 点 LHA001

XUUV 输入,在强制的前置条件下,低压安注泵 RIS001PO 的开启指令由 ESF-A 通过 Safety Bus-Train A 传输给 SLC-A2,SLC-A2 通过 PIF 卡(优选接口卡)输出。信号的传输路径为 ESF-A、Safety Bus-Train A、SLC-A2。Safety Bus-Train A 作为信号路径上的关键段,其信号传输时间的变化对整个安全动作的响应时间会有明显的影响,因此通过对该安全动作响应时间的测量,能够较为清晰地展现 Safety Bus-Train A 环网不同状态下响应时间的变化。测试实验信息如表 2 所示。

表 2 响应时间实验信息

输入点	输出点	阶跃输入值	指标	前置条件
ESF-A: LHA001 XUUV	SLCA2: RIS001P- ORD	OFF → ON	550 ms or less	ESF-A: LHA041XG→ON; LHA004XA→ON; LHA041XB→ON; LHA007XA→ON

对该安全动作的响应时间进行拆解如图 7 所示。

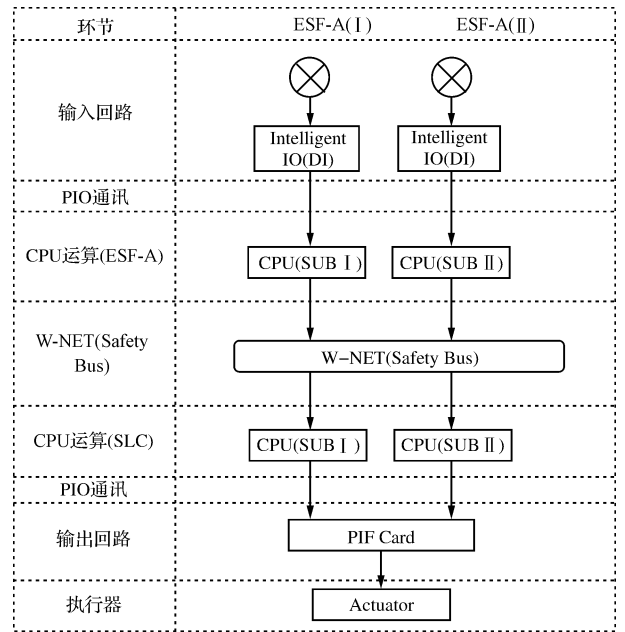


图 7 安全动作响应时间拆解

为了保证对环网故障对响应时间影响的准确分析,在测试验证过程中需尽量排除环网以外对响应时间影响的因素。因此实验中需采取以下措施:

- (1)单独进行该项测试,防止其他测试的影响。
- (2)消除 Safety Bus 环网各机柜报警,并保持各机柜状态正常。
- (3)实验过程中相关机柜 CPU 均不进行重启操作。

实验测试结果如表 3 所示。

表 3 响应时间测试结果

环网状态	响应时间/ms						均值/ms	均方差/ms
状态正常	161	157	164	154	138	...	154.8	9.064
单链路故障(拔掉 ESF-A I 系 P1 Tx 端口光纤)	200	187	171	173	174	...	181	11.045
同网段内外环链路故障(拔掉 ESF-A SUB I P1 Tx 及 P1 Rx 端口光纤)	162	191	159	171	193	...	175.2	14.288
环网上机柜 CPU Failure(ESF-COM-A SUB I Failure)	173	210	184	207	208	...	196.4	15.054
环网上机柜失电(ESF-COM-A 机柜断电)	176	167	194	184	177	..	179.6	9.002

根据表 3 中的数据可以看出,故障状态下,安全动作的响应时间平均值相较于正常状态均有所升高,其中在环网上机柜 CPU Failure(ESF-COM-A SUB I Failure)的情况下,安全动作响应均值时间变化最大,长达 41.6 ms。但鉴于专设安全动作响应时间的性能要求为小于 550 ms,故障条件下响应时间的变化仍处于可接受的范围,并未对安全动作的性能造成大的影响。

从响应时间的分布上看,在单链路故障,同网段内外环链路故障,链路上机柜 CPU failure 的 3 种故障条件下,响应时间均方差变大,时间分布更为分散。但总体来看影响较小。环网上机柜失电(ESF-COM-A 机柜断电)的情况下,响应时间均方差与正常状态下的情况基本一致。可见 Optical Switch 的切换保持了环网的结构完整,链路路径也未发生大的变化,保证了环网性能的稳定。

实验结果验证了在正常状态下,CPR1000 用安全级 DCS 环网具有良好的响应时间性能,即使在故障条件下,CPR1000 用安全级 DCS 环网响应时间未有大幅增加,仍有良好的响应速度及响应时间稳定性。

5 结束语

双环网结构、光切换模块的使用等硬件设计,结合上软件上 RPR 协议的使用及全数据收发策略,使得基于 MELTAC-N 平台安全级 DCS 环网具有较强的

链路容错能力及良好的时间响应速度及响应时间稳定性。

本研究及测试验证了其安全级 DCS 环网设计实现的有效性,能够增进对安全级 DCS 环网的了解,为工程实践中环网相关问题的处理提供了理论基础,同时也能够为国产化安全级 DCS 平台的开发提供有益的思路借鉴。

参考文献(References):

- [1] 郑伟智,李相建. CPR1000 保护系统设计研究[J]. 核动力工程,2012,33(6):21-26.
- [2] 郑扬帆. DCS 的通讯网络分析及提高可靠性方法[J]. 工业以太网与现场总线,2008(8):58-62.
- [3] 鄧永学,吕秀红,周爱平. 核电厂 DCS 可靠性讨论[J]. 自动化博览,2009(2):79-81.
- [4] 陈 龙. 核电站安全级 DCS 系统网络的基本设计准则[J]. 自动化博览,2013(1):78-81.
- [5] 苟国楷,黎国民,王群峰. 核电站安全分级对 DCS 系统设计影响分析[J]. 核动力工程,2011,32(5):23-28.
- [6] 腾国荣,李彦军,平建华,等. 核电站余热排出泵轴承体的受热分析[J]. 流体机械,2011,39(12):33-37.
- [7] 赵东升. 常见 DCS 通讯网络的结构特点及其比较[J]. 热电技术,2006(4):47-49.
- [8] IEEE 802.17a-2004,IEEE Standard for Local and Metropolitan Area Networks[C]. IEEE Computer Society, 2004:1-4.
- [9] 陶智勇. RPR 的网络保护及与 SDH 保护方式的互通[J]. 光通讯技术,2003(11):14-16.

[编辑:张 豪]

本文引用格式:

王少威,汪富强,黎国民. 基于 MELTAC-N 平台的核电厂安全级 DCS 环网研究与测试[J]. 机电工程,2015,32(1):123-127.

WANG Shao-wei, WANG Fu-qiang, LI Guo-min. Research and test validation of data bus base on MELTAC-N safety DCS platform[J]. Journal of Mechanical & Electrical Engineering, 2015,32(1):123-127.

《机电工程》杂志: <http://www.meem.com.cn>